intro

«Ноа, ты живой» – спросил Добрянский, заметив краем глаза, что я потихоньку сполз на клаву и, по всей видимости, отключился.

Не знаю, можно ли классифицировать то состояние, в котором я находился по шкале живой/полумертвый/мертвый, но спать хотелось очень сильно. Еще бы – уже вторые сутки подряд мы пытались разобраться, откуда вообще взялись эти проклятые протоколы? Дело в том, что когда мы рассказываем в журнале о каком-нибудь сложном, запутанном протоколе, всегда пытаемся провести какие-то аналогии с реалом, чтоб легче было понимать. Но фишка в том, что когда ты, наконец, понимаешь, что такое протокол, начинаешь примерять его к реальным ситуациям, и получается, что очень многое в реале – это тоже протокол!

Мы шли с Донором по улице, и он уже собирался что-то сказать – даже начал фразу… Но тут я вспомнил, что-то очень важное, приоритет чего был значительно выше, чем приоритет того, что хотел сказать Дон. Естественно, я его прервал (но где-то у себя в стеке все же сохранил запись о том, что Донор хотел мне что-то сказать). Когда мы обсудили это «важное», я извлек из стека скинутый туда дамп и попросил Донора продолжить передачу перерванных данных. Но тут оказалось, что он уже не помнит, о чем хотел заговорить. На это я ему ответил фразой «Данные были утеряны, связь будет оборвана», на что мы оба улыбнулись, согласились, что общаемся по протоколу без гарантированной доставки данных, и договорились в следующий раз, когда кто-то кого-то будет прерывать по более важным вопросам, скидывать в стек не просто информацию об оборванном сеансе связи, но и уже частично полученные данные, чтоб можно было потом по логам восстановить передачу утерянных данных.

Вот и думай теперь: сетевые протоколы были специально созданы по образу и подобию протоколов из реала, которые мы ежедневно юзаем во время общения, принятия пищи и всего остального. Но, черт возьми, кто придумал эти самые протоколы из реала, к которым все уже привыкли и почти не замечают????!!!!

Как ты, наверное, уже понял, в этом номере Спеца, тебя ожидает огромная куча протоколов, тория и практика по сканированию сетей и машин, обзоры самых рулезных сканеров, куча советов и многое-многое другое. Мы просто в очередной раз взяли одну из тем по взлому и разложили ее для тебя по полочкам. Наслаждайся :).

n0ah

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.

ЧТО ТАКОЕ СКАНИРОВАНИЕ?

СКАНИРОВАНИЕ НА ПАЛЬЦАХ

Donor (donor@real.xakep.ru)

СЕГОДНЯ МЫ РАЗИНУЛИ ПАСТЬ НА ОЧЕНЬ ВАЖНУЮ ТЕМУ – «СКАНИРОВАНИЕ». И ЕСЛИ ПРИ СЛОВАХ: «Я СКАНЮ СЕТЬ» У ТЕБЯ В МОЗГУ ВСПЛЫВАЕТ КАРТИНКА ПАЧКИ ПРОВОДОВ, ЗАСУНУТЫХ В ПЛАНШЕТКУ ОТ ХУЙЛЕТ ПУКЕРТ, СРОЧНО ВТЫКАЙ, О ЧЕМ РЕЧЬ. ДЛЯ ЭТОГО Я РАЗЛОЖУ ПЕРЕД ТОБОЙ ТЕМУ НА ВЕЕРЕ ИЗ ПАЛЬЦЕВ :).

СКАНИРОВАНИЕ - ЭТО РАЗВЕДКА

Сканирование – это один из важнейших методов в бардачке хаксора. Представь себе, что ты решил заняться телефонным хулиганством. Чтобы получить клевый пранк, тебе нужно найти самую крикливую старушку в районе. Но ты же не знаешь номера телефонов старушек твоего района, поэтому не к кому применять своего другана, умеющего говорить разными голосами. Значит, нужна разведка. Ты составляешь список телефонных номеров своего района и обзваниваешь один за другим все номера. Как только ты услышал голос, ты определяешь, старушка или нет и ставишь соответствующий значок рядом с соответствующим номером телефона. Помаявшись недельку, ты составишь более-менее полную базу телефонов старушек твоего района.

Аналогично в хаке. У тебя есть какая-то сетка, которую жуть как хочется приласкать. Нужно выяснить, что там в этой сетке есть (какие тачки, сколько, на каких осях, чем занимаются), прежде чем картинно раскладывать рут-киты. То есть, твой район – это целевая сетка, телефоны – это IP-адреса машин, старушки – это машины, а сканер – это ты, амиго :). Ты «обзваниваешь» все айпишники и выясняешь, сидит ли там старушка или номер вообще отключен за неуплату. Составив список IP-адресов реально существующих и работающих машин уже можно что-то хачить.

Кстати, когда-то хакеры действительно сканировали телефонную сеть! Ведь интернета, как такового, еще не было, а были отдельные маленькие сетки, и чтобы подключиться к такой сетке, а уж тем более похачить, нужно было знать номер телефона сервака. Вот, хацкерские проги и звонили по всем номерам, слушая, ответит на том конце модем или злющая старушка.

СКАНИРОВАНИЕ - ЭТО ПЕРЕБОР

Да, разведку ты производишь наугад. То есть, ты звонишь на первый номер, потом на второй или на десятый, двадцатый, тридцатый и так далее. Это уж как ты захочешь перебирать номера. Все, где есть перебор можно назвать сканированием. Планшетный сканер подряд одну за другой считывает строчки с бумаги, луч в трубке монитора подряд одну за другой зажигает точки люминофора на экране, взломщик одну за другой втыкает отмычки в замок – все они сканируют.

Сканирование в хаке – тоже перебор. Кул хака в поисках необходимого один за другим перебирает адреса машин и номера портов на них.

СКАНИРУЕМ УМНО!

Можно неделями тупо сканировать все телефонные номера в ожидании вожделенного старческого «Алле!», а можно прикинуть, в каком доме живет больше всего старушек, и на какие цифры начинаются номера в этом доме, тогда старушки нароются гораздо быстрее.

Так же при хаке - можно сканировать сперва стандартные адреса и порты, а только потом, если понадобится, все остальные.

АДРЕС

Теперь, когда мы разобрались, что такое сканирование, давай воткнем, что сканируем. Когда мы хулиганим по телефону, мы сканируем (перебираем) номера телефонов. Так же, когда мы хачим, мы сканируем (перебираем) IP-адреса и порты. IP-адрес машины – это то же, что и номер телефона старушки. Просто телефону нельзя приказать: «Клавдию Ивановну мне!», а компу можно. Пишешь «www.sex.com», а железка сама узнает «номер телефона» соответствующего сервака и «звонит» ему.

В одной сетке IP-адреса начинаются с одних и тех же цифр, как номера телефонов в твоем районе. Поэтому чтобы взломать какой-то сервер, не нужно сканить весь инет, достаточно посканить диапазон IP'шников. Хотя, если кто-то получает от этого определенное извращенное удовольствие...

ПОРТ

Сервер сам по себе ничего не умеет, как телефон сам по себе не умеет отвечать тебе на твой бред. На твой бред тебе отвечает старушка. Таким образом, она, сама этого не зная, удовлетворяет твои извращенные фантазии, то есть предоставляет тебе сервис. На серваке сервис (на-

пример, в виде порнушной картинки) тебе предоставляет программа.

Теперь представь, что в квартире вместе со старушкой живут: немой старичок, шизанутая внучка, кастрированная жучка, лысая кошка и чумная мышка. А тебе нужна именно старушка. Так как до нее достучаться? Правильно, крикнуть: «Бабку мне к телефону!» или набрать ее внутренний номер, если это хай-тек старушка :). То есть: 555-55-55:Клавдию Ивановну. Вот и на серваке каждая программа имеет так называемый порт. Чтобы получить порнушную картинку с www.sex.com, нужно «позвонить» по соответствующему IP-адресу и попросить в «окошке» с номером 80 порнушную картинку. Выглядит это так: 192.61.231.111:80 (номер и порт). Если попросить картинку в другом окошке, то тебя пошлют далеко и надолго.

Откуда я (или Ыгсплорер) знаю, что нужно просить в 80-м окошке? Да оттуда, что это стандартный порт! Вот зачем Спец постоянно публикует для тебя список стандартных портов.

Таким образом, хацкер может выяснить, какие проги запущены на серваке, ткнувшись в определенные стандартные порты, так же легко, как ты можешь выяснить, живет ли по этому телефонному номеру Клавдия Ивановна. А зная, какой конкретный софт трудится на серваке, легко выяснить его баги и найти эксплоиты для него.

ЧТО ТАКОЕ СКАНЕР?

Хацкер, конечно, мог набирать ручками номера телефонов и слушать, засвистит ли на другом конце модем или нет, но так и сдохнуть недолго. Поэтому умный хакер поручал звонить, слушать и отмечать в списке компу. Прога, которая это делала, - один из примеров сканера.

То же самое и сейчас. Это, конечно, дико круто – формировать запросы к серваку ручками, но намонстрячить несколько сотен тысяч запросов вручную – увольте! Для этого существует огромное количество прог, которые ты без труда отыщешь в инете.

Современный сканер постепенно «звонится» на все IP-адреса из диапазона, заданного юзером, то есть берет с бумажки один за другим оставленные ему тобой номера телефонов и шлет определенные запросы на все или часть портов, то есть последовательно спрашивает: «А Таню можно? А Лену Можно? А Вику можно?..». И так для каждого IP-адреса (номера телефона).

Современный сканер – это довольно продвинутая прога, чем-то напоминающая антивирус. Сканер не просто «стучится» по адресам и портам, но и получает информацию о прогах, запущенных на серваке, сравнивает их названия и версии со своей внутренней базой данных и выдает отчет о найденных дырках (это уже не сканер, а анализатор уязвимостей. хотя, анализатор уязвимостей тоже занимается сканированием :) – прим. ред.). При этом он еще шифруется, чтобы админ сервака не просек, что его сканят.

Часто, достаточно запустить сканнер, найти в поисковике эксплоит (прогу-ломалку), чье название берется из отчета, запустить ее, и ты уже хацкер. Правда, в голове от этого не прибавится, так как «сломал» сервак не ты, а чел, написавший сканер и эксплоит.

КАК РАБОТАЕТ СКАНЕР

Итак, юзер ввел диапазон IP-адресов (листочек с телефонами) и диапазон портов (предполагаемые жильцы квартиры) и запустил прогу. Сканер берет первый IP-адрес из списка и посылает по нему, допустим, запрос Hallo! aka «Алле!». Приходит ответ – значит, по этому IP есть живая тачка. Йоу! Начинаем дрючить порты. Например, посылаем запрос на 80-й порт и слушаем. Пошли ответные пакеты aka упакованная информация – значит, порт живой. Далее сканер дрючит порт хитрыми запросами и выясняет название программы, которая откликается по этому порту, ее версию, требуется ли пароль и так далее. Потом сверяется со своей базой данных и дает заключение о наличии дырищи. Если ответы не приходят, то сканер стучится по следующему IP'шнику или порту и так, пока не переберет весь диапазон. В конце концов хацкер получает вполне удобоваримый отчет о живых тачках, открытых портах и найденных уязвимостях. То есть бабку нашли :).

Итак, ты понял, что сканирование сети – это поиск реальных живых машин и соответственно их IP'шников среди всех IP-адресов этой самой сети, то есть ищем телефоны, а сканирование портов – это опрос и анализ портов на каждой из живых машин этой сети, то есть опрашиваем всех жильцов квартир по найденным телефонам.

ЧТО ДАЕТ СКАНИРОВАНИЕ

Сканирование позволяет хаксору нарыть инфу о том, как построена сеть, какие тачки есть в этой сети, какие функции они выполняют и какие дырки в запущенном на них софте, возможно, есть. Это дает возможность нарыть дополнительную инфу о тачке, которую собственно хочет похачить хацкер, продумать обходные пути, вломиться на тачку не напрямую, а через соседнюю по сети машину и так далее.

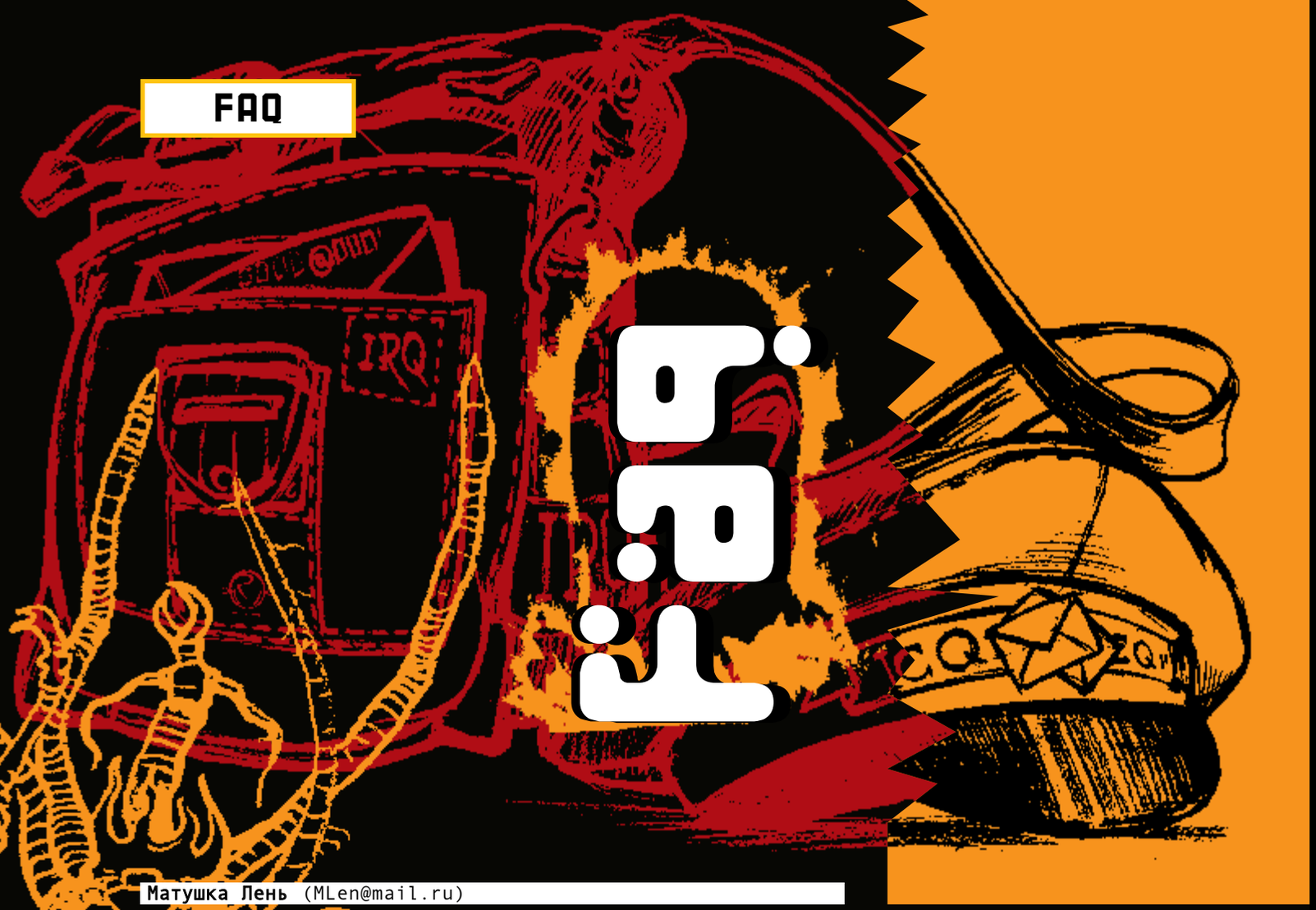
То есть, допустим, злобный внучок целевой старушки не завет свою бабку к телефону, потому что он, видите ли, нас не знает. Мы сканируем другие номера телефонов, предположительно относящиеся к этому же подъезду и находи другую старушку – соседку целевой бабки. Соседка оказывается уязвимой для молодых обходительных хацкеров и выбалтывает нам много личной инфы про целевую бабку. Теперь мы уже звоним целевой бабке и говорим внучку, что мы – Кузьма Петрович и работали вместе с целевой бабкой на Рязанской ТЭЦ. Внучок сомневается, но бабку зовет. Вуаля!

Далее сканер дрючит порт хитрыми запросами и выясняет название программы, которая откликается по этому порту, ее версию, требуется ли пароль и так далее. Потом сверяется со своей базой данных и дает заключение о наличии дырищи.

ВПИТЫВАЙ!

Итак, ты воткнул, что сканирование – это сбор важной развединформации о хакаемой тачке. Без него и хака-то не получится. Сканер сканирует сеть на наличие в ней живых машин и найденные машина на наличие открытых портов, а также на наличие уязвимого aka дырявого софта, висящего на этих портах. Сканирование всей сети позволяет нарыть дополнительную инфу о хакаемой тачке, а также нарыть обходные пути.

Так что, сканирование – это важно. Читай Спец внимательно!



FAQ

Матушка Лень (MLen@mail.ru)

Что такое SAP?

Service Access Point - точка доступа к услуге (ТДС). В прошлых номерах Спеца я уже рассказывал тебе о схеме клиент-сервер. Сервер - предоставляет услуги, а клиент их потребляет. Услуг в Интернете бывает множество, это услуги по передаче почты, услуги доступа к веб-страничкам, услуги поиска и так далее...

Одним словом, глобальная сеть похожа на огромный универсам с кучей отделов, и в каждом отделе тебе могут предоставить массу услуг. По отделам бродят миллионы клиентов и пользуются услугами.

Чтобы клиенту оказали услугу, он должен ее потребовать. То есть нужно нагрянуть в какой-нибудь отдел (на сервер) и обратиться к ответственному лицу (продавщице, например). Это лицо и есть твоя точка доступа к услуге. Через продавщицу ты сможешь воспользоваться возможностью попить сока у себя в квартале. Только не грози при этом южному централу :)!

На самом деле ТДС - очень широкое понятие, ведь услуги могут предоставлять не только серверы, но и еще куча устройств. Например, розетка твоего телефона - точка доступа к услуге голосовой связи! IP-адрес тоже в каком-то смысле точка доступа к услуге передачи данных по сети. А MAC-адрес твоей сетевой карты - точка доступа к передаче данных по физической среде.

Кто оказывает услуги?

Мы с тобой договорились, что сервер - это отдел во всемирном универсаме (Интернет). До отдела (сервера) ты можешь добраться, зная его IP-адрес. А чтобы получить нужную услугу, нужно обратиться к нужной продавщице. Понятно, что продаваловка лишь часть какого-то мегамеханизма, скрытого от твоих глаз. Где-то там, в закрытой части отдела, кишат грузчики, уборщицы, рабочие, даже целые заводы. Это все софт, который стоит на сервере. Эти программы фунциклируют на сервере и оказывают тебе услуги, но ты получишь их только через маленькое окошко - продавщицу!

Что такое порт?

Это точка доступа к софту на сервере, который оказывает тебе услуги. В любом отделе (сервере) много продавщиц: одна торгует вебом, другая почту принимает, третья телом приторговывает ;). Собственно, на каждом сервере есть стандартный набор

портов, на которых висят стандартные услуги. Порты различаются по номерам.
Не надо путать их с параллельными портами, com-портами, морскими и аэропортами! Хотя суть одна.

Что такое socket?

Socket переводится как розетка (гнездо, в которое втыкают вилку). Его часто путают с портом, но они отличаются. Сокет - это способ найти во всемирном универсаме именно ту услугу и именно ту продавщицу, которые нам с тобой нужны. Сокет - это уникальный IP-адрес и адрес порта. То есть мы точно знаем IP-номер отдела и номер продавщицы, которая в этом отделе торгует уникальными бананасами. Больше таких во всей сети не сыскать!
Хотя, если ты перепутаешь порт и сокет, большой ошибки не будет. Это сходные понятия, все зависит от того, в каком контексте о них говорят.

Я забыл, что такое IP?

Internet Protocol - Интернет протокол. По этому протоколу передают данные по сети Интернет, он хорош тем, что его понимают почти все операционные системы мира. Каждый пакет этого протокола содержит глобальный адрес. По этому адресу можно связаться с любым компьютером в сети. Поэтому этот адрес называют IP-адресом или айпишником.

Я забыл, что такое TCP/IP?

Transport Control Protocol/Internet Protocol - транспортный протокол с контролем доставки/Интернет протокол. Вокруг TCP/IP и крутится все сканирование портов. Почему? Да потому, что это главный транспорт в Интернете. IP отвечает за адрес и выбор маршрута, за связь между двумя железками, за то, чтобы покупатель дошел до нужного отдела в глобальном универсаме. TCP - отвечает за надежную связь между двумя софтинами. Чтобы информация из одной программы попала в другую, то есть чтобы покупатель нашел себе нужную продавщицу и с ней договорился.

Зачем нужны порты с сокетами?

На самом деле, портом можно назвать не только продавщицу, но и покупателя. Они как вилка с розеткой. Чтобы семья покупателя могла передать заказ на определенный склад отдела, нужны продавщица и покупатель. По айпишнику можно найти нужную железку (сервер) в Интернете, а по сокету ты найдешь нужную софтину в Интернете. Сокет состоит из адреса железки (айпишника), на которой стоит софтина, и адреса порта (программного шлюза), на котором висит софтина.
Интрига в том, что ты можешь сам придумать две программы, которые повесятся на свободные порты на двух разных тачках и будут общаться между собой через Интернет. Бывают и стандартные порты, на которых висят стандартные приложения. Чтобы хорошо сканить и хорошо защищаться, хакер должен их себе представлять.

Какие бывают порты?

P-адрес прописывается в заголовке пакета IP-протокола. IP переносит на своем горбу TCP. В заголовке TCP прописывается адрес порта. TCP на себе тащит самые главные интернетовские протоколы. Эти протоколы умеют распознавать приложения, которые висят на портах.
Адрес порта 16-битный, это значит, что портов может быть около 65 тысяч! Под стандартные приложения отведена первая тысяча портов (с первого по тысячный порты. Все, что больше, - для динамического выделения. То есть если портов не хватает - можно брать оттуда! Представляешь, какой штат продавщиц?
Обычно все лишние порты закрывают, чтобы хакеры не лезли, оставляют только необходимые для предоставления серваком услуг.

FAQ

Что такое порт HTTP?

HyperText Transfer Protocol отвечает за передачу WEB-страничек в виде HTML. По этому протоколу разговаривают Web-сервер и Web-браузер. Они оба по умолчанию закреплены за портом 80. Если ты заблокировал этот порт, то странички смотреть не сможешь. Если ты админ, то это отличный способ разрешить юзерам доступ только к почте. Нечего порнуху качать!

Зачем нужен порт DNS?

На 52 порту тусуется протокол службы имен доменов (Domain Name Service). Эта продавщица оказывает справочные услуги. В ответ на имя странички в Интернете она говорит тебе ее IP-адрес. Без этого порта у тебя не будут работать имена страничек.

Где живут POP3 и SMTP?

Post Office Protocol ver. 3 - протокол почтового отделения - нужен для получения почты, ее нам отдает продавщица под счастливым номером 110. Simple Mail Transfer Protocol (простой протокол для отправки почты) предоставляет барышня с биркой 25. К этим дяфчонкам можно зателнетиться (по протоколу Telnet) и начать ими понукать. Если хакер нашел на малоизвестном сервере открытый порт SMTP, он может начать с него спамить мирных пользователей или даже крошить их мыльными бомбами!

Где живут ICQ и IRC?

Тетя Ася с тетей Ирой живут под номером 4000 и где-то в районе 6,5 тысяч. Это не стандартные программы, поэтому их номера переваливают за тысячу. Хотя можно извернуться и настроить их через 80-й порт, если админ закрыл все остальные порты и не пускает нас к Аське с Ирокой, педе... э-э-э-э... паразит!

Что такое удаленное администрирование?

Напомню, что обычное администрирование - это полный контроль над компьютером или какой-то его частью. То есть если ты можешь творить с какой-то программой все, что захочешь, значит - ты администратор. А что можно хотеть? Достаточно иметь полный доступ ко всем файлам: читать, записывать, удалять, изменять и запускать их. Хотя еще можно управлять разными устройствами: микрофоном, выезжающей крышкой сюдюка, принтером, включением/отключением компа.
Удаленное администрирование - администрирование через сеть. В этом случае все то же можешь делать с чужим компьютером через Интернет со своей домашней тачки. Но вот проблема: многие протоколы Интернета сделаны так, чтобы исключить такую возможность, поэтому приходится изгаляться.
Главная задача хакера стать удаленным администратором чужого компьютера, для того-то он и сканирует порты.

Что такое троян?

Это программа удаленного администрирования. Троян решает большинство проблем хакера. Главное впарить эту софтину пользователю или админу. Когда троян поселился на компьютере жертвы, он может запускать программы, работать с файлами, может полностью переколбасить чужой компьютер. Троянец вешается на какой-то порт, через который общается со своим хозяином. Обычно троянца засылают для того, чтобы украсть пароли, базы данных, удалить логи или просто поиздеваться. Иногда трояны встроены в вирусы, умеют размножаться и заражать безобидные программы. При этом инфекция передается через дискетки, по электронной почте, вместе с «полезными» программами из Интернета. Часто троянскими конями заражены хакерские

программы. Будь осторожен, когда качаешь злобные проги с чьей-то домашней странички!
Подкожный поразит (троян) может превратить безобидную продавщицу (порт) в коварного монстра, который ворует товар (ресурсы чужого компьютера) и отдает его знакомому малолетнему преступнику (хакеру), с которым состоит в интимной связи (по TCP/IP)!

Как определить наличие трояна?

Как обычный вирус трояна можно отловить антивирусом. Только злые троянские лошади постоянно мутируют, и антивирус может не узнать мутанта. Для того чтобы надежно защититься, тебе понадобится самая свежая вирусная база, с тепленькими сигнатурами.
Если троянец уже поселился на твоей машине, то ты увидишь, как он ломится в порты для того, чтобы связаться со своим хозяином. Разглядеть эту активность можно с помощью файрволла, он же поможет тебе заблокировать троянца. Но лошади тоже не дураки, научились ломиться по жизненно важным для тебя портам, которые закрыть нельзя. Например, по 80-ому порту, через который грузятся веб-странички. Еще важно, где в твоей системе встроился файрволл, а где троян. Реально написать очень умную лошадь, которая закопается в драйвер сетевого адаптера. В таком случае никакой файрволл коня не достанет.

Что такое Firewall?

Это такая программа, которая следит за состоянием портов. То есть это охранник магазина, который приглядывает за продавщицами, чтобы к ним никто особо не приставал. Иногда огненная стена сильно обламывает хакерские затеи по сканированию портов. Порты, прикрытые файрволлом, могут вообще не отвечать на ping и другие хакерские попытки соединиться. Подробнее об этих замечательных программах и о том, как с ними бороться, читай в следующем номере!

Что такое сигнатура?

Это цифровой отпечаток данных. Что-то типа отпечатков пальцев. Чтобы узнать человека, не нужно изучать его целиком, достаточно маленького отпечатка пальца. Так же и с данными. Каждый кусок цифровой инфы может иметь свою уникальную сигнатуру в несколько байт. При этом неважно, сколько этот кусок весит: гигабайт или 64 байта. Какой это кусок: кусок текста, кусок звукового файла, кусок картинки или кусок кода, тоже неважно. Обычно с живого вируса снимают отпечатки пальцев (сигнатуру) и сохраняют их в вирусной базе. Сигнатуры очень маленькие, поэтому в один файл вирусной базы влезает информация о тысячах новых вирусов. Этот файл легко рассылать через Интернет из-за небольших размеров. Очень удобно то, что даже если вирус встроился в какую-то программу, антивирус все равно быстро узнает его сигнатуру. Но вирусы тоже не идиоты (особенно трояны): они мутируют, перестраивают свой код или рождаются новые - науке не известные. Поэтому свежих троянов антивирус может пропустить!

Что такое NetBIOS?

Network Basic Input/Output System - базовая сетевая система ввода-вывода. Это достаточно древний протокол, придуманный IBM. Его поддерживает Novell и Microsoft. Фактически это протокол удаленного администрирования, потому что он позволяет сделать твои диски и твои принтеры общими для всех пользователей сети. Этот протокол используется во многих локальных сетях для того чтобы можно было легко обмениваться файлами и печатать на чужом принтере. Он крайне прост и очень слабо защищен, пароли доступа к чужому диску подбираются влегкую. Поэтому всем администраторам советуют отключать этот протокол на машинах, подключенных к Инету.

Что такое NetBIOS via TCP/IP

А вот здесь кроется самая главная прелесть. Дело в том, что с NetBIOS можно работать через TCP/IP. То есть тисипи

умеет передавать пакеты нетбиоса. Представляешь, какое западло? В Windows 95, 98, NT модуль NetBIOS висит на 135-139 портах, а в Windows2000 на 445-м. Многим пользователям этот протокол не нужен, просто виндовс включает его по умолчанию, а некоторым любителям локалки без него просто не обойтись (чтобы юзать чужие принтеры и файлы). Поэтому хакеры прежде всего сканируют компьютер на наличие NetBIOS. Для этого они сначала пингуют нетбиосовские порты, а потом пытаются установить нетбиосовскую сессию. Это значит, что скоро хакер будет удаленно администрировать чей-то компьютер даже без помощи трояна.

Как спастись от NetBIOS?

Если тебе не нужен этот протокол, то нечего его устанавливать. Если он уже установился самостоятельно в «Свойствах сети» на «Контрольной панели» твоего Windows, его можно удалить. Ну а если у тебя локальная сеть и без него не обойтись, то нужно отключить NetBIOS через TCP/IP. Тогда тебя хакнуть смогут только другие пользователи локалки. 139-порт - любимый порт для нюков и прочей хакерской гадости, поэтому полезно закрывать его файрволлом или в реестре. Есть множество программ и заплаток, которые закрывают этот порт для безопасности.

Что такое Nuke?

Нюк - это атака на отказ услуги (Denial Of Service). То есть это когда мы даем продавщице такой запрос, от которого она падает в обморок и роняет за собой весь отдел с другими продавщицами. Когда хакер сканирует порты пользователя или сервера, он обязательно проверяет их на возможность нюка. Ведь можно завалить сервер или выкинуть врага из сети. Раньше все давали неправильные инструкции NetBIOS по 139 порту, после чего он вешал всю систему и зажигал синий экран Windows. Сейчас все поприкрывали этот порт, поэтому можно открыть множество полувинчатых TCP соединений. Толпа из тысячи человек накидывается с вопросами на продавщицу, и та сходит с ума. Это называется SYN flood.

Что такое логи?

Log-файлы - самая стремная часть сканирования. Дело в том, что любое обращение к порту, попытка установить сеанс связи фиксируются в специальном файле. Поэтому, если хакер решил посканить порты на каком-то сервере, то времени у него не много. Админ очень быстро заметит в логах, что кто-то перебирает порты, и решит, что его хакают. Поэтому хакеру нужно скорее ломать сервер и стирать логи. Ну и, конечно, нужно скрывать свой настоящий адрес, чтобы не сели на хвост спецслужбы. Ведь по реальному IP очень легко найти реального человека из Интернета. Ведь IP обязательно зарегистрирован на конкретную организацию. Это значит, что если хакер засветил IP своего провайдера при сканировании, то туда придут спецслужбы. Следователи глянут логи и найдут хацорский номер телефона (сейчас на любом модеме стоит определитель) или IP-адрес, на который зарегистрирован хакерский компьютер. Через 15 минут они вламываются в гости и отбирают у хацкера комп. Кстати, не вздумай сканить своего провайдера. Провайдеры очень не любят, когда к ним ломятся во все порты с их же айпишника. Обычно такого пользователя сразу удаляют из базы и закрывают с его телефона доступ навсегда.

Что такое анонимный Proxy?

Proxy переводится как представитель. Это сервер, который лазит в Инете по заданию хакера, но под своим айпишником, то есть во всех логах остается айпишник прокси, а не хакера. Поэтому вредитель может сидеть в Москве, а спецслужбы будут лазить в Париже. Конечно, каждый анонимный прокси ведет логи, по которым можно вычислить злоумышленника. Поэтому хакеры используют целую цепочку из анонимщиков, которая постоянно меняется. Для того чтобы расследовать хак по логам, людям в черном придется съездить в Одессу, Нью-Йорк, Улан-Батор и Гонконг. Конечно, у хакеров все тормозит, зато все анонимно. Но как ни странно, проказников все равно постоянно ловят.

Так в чем же заключается сканирование портов?

Сканирование портов - это самый настоящий перебор. Мы зашли в отдел и перебираем продавщиц на стойкость, может какая-то из них отдастся бесплатно? Еще мы можем перебирать отделы, вдруг в каком-то много лишних продавщиц торчат с голыми задницами? В том-то и заключается сканирование, что мы тыркаемся по нескольким айпишникам, по нескольким портам - куда войдет.
Знай, тупой перепихон всегда вреден! Намного полезнее долбиться в определенные IP, по определенным портам. Порты проверяют стандартные, типа 139-ого. IP чешут какой-нибудь организации, провайдера или конкретного пользователя.

Откуда берут IP для сканирования?

Чтобы просканировать сервер, на котором висит вражеская страничка, хакер вводит в программу-сканер его IP или его DNS. IP, как ты понял, определяют по DNS, то есть по имени сервера. Сканер начинает перебирать порты на сервере и пытаться подконнектиться к каждому.
IP конкретного пользователя берут из чата, Аськи, Ирки или мыла. Если хакер хочет украсть пароли для выхода в Инет модемных юзеров, то он перебирает адреса провайдера. Если ты сидишь на модеме и твоя тачка не защищена, значит - скоро ты станешь чьим-то халявным Инетом, если еще не стал.

COVER STORY

10 (23)

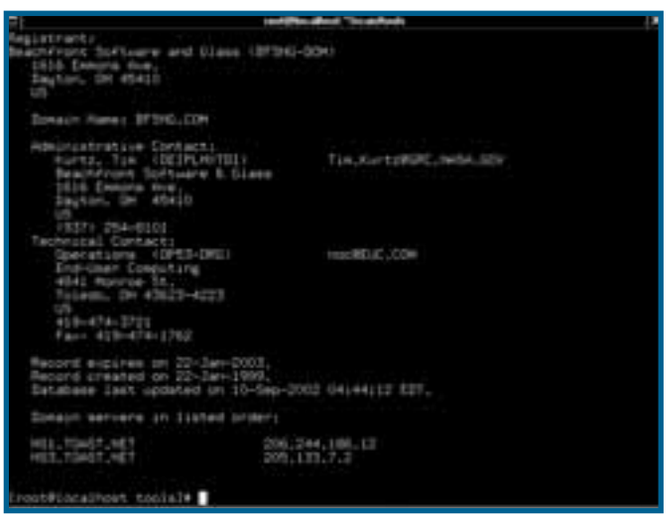
WHO IS?

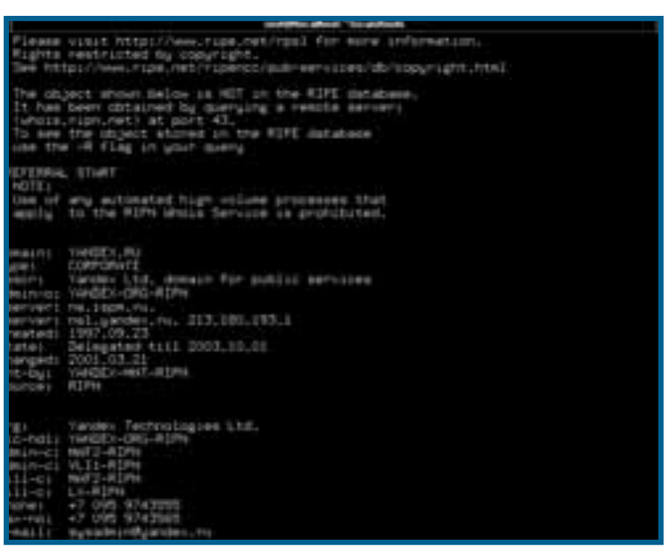
наводим справки

Все считают, что сканирование – это то, с чего начинается любой хак. На самом деле сканированию предшествует еще один этап – сбор информации. Прежде чем перейти к взлому, надо просканировать цель и выяснить, что это вообще такое. Точно так же, прежде чем перейти к сканированию, надо сначала собрать всю доступную информацию о цели. Мощнейшим источником информации о целевой системе является сервис whois.

mopy (mopy@xakep.ru)

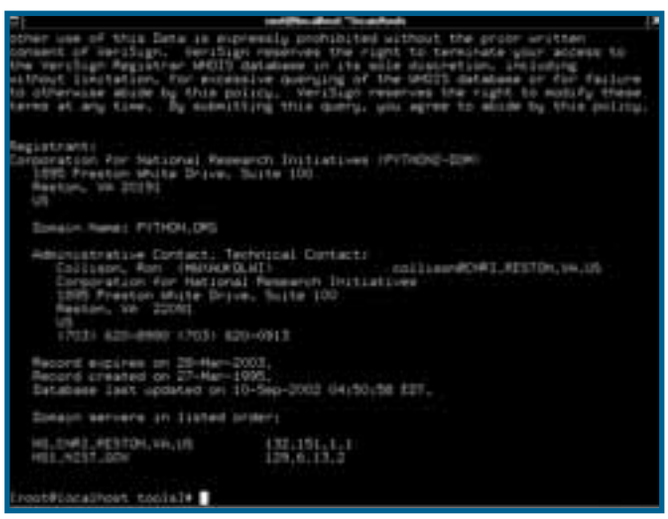
Сервис whois - это универсальный источник информации об отдельных персонах, организациях, сетях и доменах. В базах данных whois хранится информация на все организации, которые имеют выделенные диапазоны IP-адресов и/или владеют доменными именами. Вполне естественно, что чаще всего сервера whois поддерживают конторы, которые занимаются раздачей выделенных диапазонов IP-адресов и доменов. В Росси такая контора называется РосНИИРОС (Российский Научно-Исследовательский Институт Развития Общественных Сетей) и базируется по адресу www.ripn.net.





Изначально доступ к сервису whois осуществлялся при помощи одноименной клиентской программы (она имеется в nix'ах – попробуй выполнить команду «whois» в окне терминала), но сейчас все чаще появляются web-интерфейсы для работы с whois-серваками. Такая штука есть и у РосНИИРОС: http://www.ripn.net:8080/nic/whois/index.html.

Для того чтобы понять, как работать с whois-серверами и какая нам от этого польза, надо сначала выяснить, что представляют собой эти самые whois-сервера. Whois-сервак –



это база данных, содержащая в себе записи об организациях, имеющих выделенные диапазоны IP'шников и/или доменные имена, о системных администраторах этих организаций, о сетевых адресах и о доменных именах. Согласно RFC1834, база данных whois может содержать три типа записей: записи о людях (это в основном системные администраторы контор, имеющих выделенный диапазон IP и/или домен), записи о хостах и записи о доменах. Из чего состоят эти записи можно посмотреть в табличке (описание полей каждого типа записи переводил с англицкого сам, так что не обессудь ;)).
Если ты поглядел на табличку, то должен уже представить себе, какого рода информацию можно выудить из whois-сервера :). Давай теперь разберемся, какая хацкеру от всего этого польза.

1. Зная только имя домена, можно получить информацию о диапазоне адресов, принадлежащем владельцу домена (сразу становится понятно, что надо сканить :)).
2. Зная только один IP, можно узнать весь диапазон адресов из той же сети, а также имена доменов, принадлежащих организации-владельцу этого диапазона адресов.

Individual records/Записи о людях

ПОЛЕ	ОПИСАНИЕ ПОЛЯ	СТАТУС
Name	Имя индивида	обязательное
Organization	Название организации	обязательное
Organization-type	Тип организации (учебная, коммерческая, исследовательская)	необязательное
Work-telephone	Рабочий телефон	необязательное
Fax-telephone	Номер факса	необязательное
Work-address	Рабочий почтовый адрес	необязательное
Title	Должность	необязательное
Department	Подразделение	необязательное
Email-address	Мыло	необязательное
Handle	Уникальный идентификатор записи на локальном сервере	обязательное
Last-record-update	Дата последнего обновления записи	обязательное
Home-telephone	Домашний телефон	необязательное
Home-address	Домашний почтовый адрес	необязательное

Host records/Записи о хостах

ПОЛЕ	ОПИСАНИЕ ПОЛЯ	СТАТУС
Hostname	Доменное имя	обязательное
IPAddress	IP'шник	обязательное
Sysadmin-name	Имя сисадмина	необязательное
Sysadmin-phone	Номер телефона сисадмина	необязательное
Sysadmin-address	Адрес сисадмина	необязательное
Sysadmin-email	Мыло сисадмина	необязательное
Machine-type	Тип машины	необязательное
OS	ОСь	необязательное
MX	Почтовый шлюз	необязательное
Last-update	Дата последнего обновления	необязательное
Info	Ссылка на источник дополнительной информации	необязательное

Domain records/Записи о доменах

ПОЛЕ	ОПИСАНИЕ ПОЛЯ	СТАТУС
Domain-name	Доменное имя	обязательное
Network-address	IP, привязанный к этому домену	обязательное
Admin-name	Имя представителя административной службы организации, владеющей доменом	обязательное
Admin-address	Почтовый адрес представителя административной службы организации, владеющей доменом	обязательное
Admin-telephone	Телефонный номер представителя административной службы организации, владеющей доменом	обязательное
Admin-email	Мыло представителя административной службы организации, владеющей доменом	обязательное
Tech-name	Имя представителя технической службы организации, владеющей доменом	обязательное
Tech-address	Почтовый адрес представителя технической службы организации, владеющей доменом	обязательное
Tech-telephone	Телефонный номер представителя технической службы организации, владеющей доменом	обязательное
Tech-email	Мыло представителя технической службы организации, владеющей доменом	обязательное
Nameservers	Первичные DNS для этого домена	необязательное
Last-update	Дата последнего обновления записи	обязательное

3. Зная только один домен, принадлежащий организации, можно узнать имена всех ее доменов.
4. Зная только одно имя домена или один IP, можно узнать организацию, выяснить имя ее админа, потом найти все организации, в записях которых прописан этот же админ, и предположить, что это, скорее всего, связанные между собой организации, стало быть и их компьютерные сети могут быть связаны между собой. А потом получить диапазоны адресов всех этих организации ;) (заметь, уже второй раз становится понятно, что надо сканировать).

О, как! Применив немного смекалки, из whois можно вытащить огромное количество полезной информации о диапазонах адресов, о доменах, о DNS-серверах и тд. Только после этого можно приступать к сканированию, а уж потом – если повезет - и к взлому.

КОЛЛЕКЦИЯ ОТПЕЧАТКОВ

OS fingerprints - определение ОС удаленной системы

DarkSergeant (DarkSergeant@inbox.ru)

ОТПЕЧАТКИ

Для того чтобы отличить одного перца (например, тебя) от другого (например, от твоего соседа) хранители правопорядка и остальные большие братья применяет разные отпечатки: отпечатки пальцев, отпечатки радужки глаза, отпечаток лица (фотографию или фоторобот). Кроме отпечатков также применяются приметы (вес, рост, возраст, форма и расположение лица, носа, ушей, глаз), где у тебя какие шрамы и наколки находятся. Челы из органов также могут тебя узнать по жестам, походке, манере разговора, словарному запасу, почерку, голосу.

ЗАЧЕМ ОНО ТЕБЕ НАДО?

Для того чтобы ни в чем не отставать от спецслужб, хацкеры планеты тоже завели себе базу отпечатков, только они коллекционируют отпечатки не на перцев, а на операционные системы. Ведь не определив, какая ОСь стоит на серваке, никак нельзя перейти ближе к телу ;). Определение удаленной OS – это одна из первейших задач сканирования!

КАКОЙ ОТПЕЧАТОК ЛУЧШЕ? ТВОЕГО УХА ИЛИ ТВОЕГО ГЛАЗА?

Давай с тобой немного подумаем, почему для опознания нас с тобой в основном используют отпечатки пальцев и фотоморды, а не форму носа или размеры ушей? Потому что данные способы характеризуются высокими показателями аутентичности, уникальности, быстрым съемом информации, сложностью подделки. В переводе на русский означает: твои отпечатки пальцев легко получить (Раз! – и твои пальца в чернильнице, Два! – пальцы прижаты к бумажке, Три! – они уже в ГБ'шной базе). Такие как у тебя отпечатки только у тебя одного, отпечатки пальцев сложно подделать (если уж нашли твои отпечатки в квартире, где деньги лежали, то уже не отвертишься :)).

«БЕЛЫЕ» И «ЧЕРНЫЕ» ЯЩИКИ

К сожалению, любая программа (а ОС – как никак, тоже программа) является «белым ящиком», в отличие, от человека – который «черный ящик». Выражение «черный ящик» означает, что мы видим данный «ящик» только снаружи и не знаем, как данный «ящик» устроен изнутри. Выражение «белый ящик» – наоборот – означает, что мы видим, как устроен данный «ящик» и поэтому можем легко поменять его внутреннее устройство, что хорошо видно на примере open source софта, который можно в любой момент изменить и собрать версию под себя. А как бы было хорошо, если бы люди тоже были бы «белыми ящиками»! Люди, то ладно, а вот перчинки точно должны создаваться под ярлыком open source. Представляешь, какая лафа была бы! Берешь и патчишь Леночку из соседнего подъезда, и вот она уже с тебя глаз не сводит и делает, что ты ей скажешь. Или меняешь код своей герлы, чтобы она за пивом с утра бегала, а не ругалась вечером, когда ты из клуба возвращаешься в три часа ночи. (Ой. Что-то я от темы отвлекся. Сейчас редактор возьмет большие ножницы и будет выстригать из статьи лишнее.) Возвращаемся к баранам, то бишь, к «ящикам». Как я уже говорил, операционная система является «белым ящиком» и поэтому злобный админ может легко подменить большинство отпечатков оставляемых ОС'ой, поэтому не останавливайся на одном способе. Используй все способы, которые знаешь, а потом уже в спокойной обстановке фильтруй полученную инфу. Относись к полученным результатам с изрядной толикой недоверия.

ТЕХНИЧЕСКАЯ ИНФА

Заканчиваю гнать не по теме и перехожу сразу к способам удаленного определения осей. Так как место, предоставляемое под статью не резиновое, рассмотрю только базовые идеи удаленного определения ОС'ей, а также те способы, которые легко воспроизвести своими руками. За более полной информацией, как всегда посылаю на три буквы (www, а не то что ты там подумал), а если конкретнее, то на void.ru, insecure.org, ya.ru, google.com (ключевые слова – «OS detection», «OS fingerprints», «удаленное определение операционной системы»).

TCP/IP/UDP/ICMP РАЗЛИЧИЯ

Если мы посмотрим на операционную систему снаружи (из сети), то мы увидим «черный ящик» из которого «торчат» различные порты, через которые уже можно получить доступ к внутренностям (различным сетевым службам) ОСы. Для того чтобы отличить одну ОС от другой, можно посмотреть как в исследуемой операционке реализуется работа портов. Как порты отвечают на различные запросы, как они реагируют на правильные и неправильные данные.

TTL. Простейшую проверку можно сделать и руками, набрав команду ping <host> и посмотрев какой номер TTL выдается в ответ. Так номер 128 обычно использует Windows старших версий, 64 – Linux 2.0.x (255 - Linux 2.4.x), 32 – Windows 95. Более полную и новую табличку смотри опять же в инете. Продвинутые сканеры конечно на одном только TTL не останавливаются, смотря также и другие особенности.

FIN-исследование. На любой открытый порт сервера посылается FIN-пакет (TCP-пакет на завершение соединения). В соответствии с RFC 793 сервер должен ответить на такой пакет RST-пакетом, однако некоторые ОС типа Windows, BSDI, CISCO, HP/UX, MVS и IRIX не посылают ничего в ответ.

BOGUS-исследование. Посылается SYN-пакет с установленным в TCP-заголовке неиспользуемым «флагом» BOGUS. «Флаг» BOGUS не является настоящим флагом. На самом деле этот термин подразумевает установку бит в поле Reserved заголовка TCP-пакета как 1000000. ОС Linux до 2.0.35 сохраняет в ответе этот «флаг». Некоторые ОС обрывают соединение при получении такого пакета.

Закон изменения ISN. Посылается SYN-пакет с запросом на соединение. Сервер, получив запрос на соединение, записывает в поле ISS ответа — свой собственный ISN, и отправляет пакет обратно. Эта операция повторяется несколько раз для нарабатывания статистики. Возможны следующие зависимости: Закон «постоянного приращения» (поле ISN увеличивается с каждым запросом на постоянную величину) – старые версии UNIX'а. Закон «случайных приращений» (приращения ISN носит случайный характер) – новые версии Solaris, IRIX, FreeBSD, DigitalUnix, Cray. Закон «время-зависимых приращений» (ISN периодически во времени увеличивается на не-

большую величину) – Windows. Закон «постоянный» (значение ISN не меняется) – железки: концентраторы 3Com, Apple LaserWriter.

Поле Window из TCP-пакета. Смотрится значение поля Window в серверных TCP-пакетах. У ОС AIX – это значение 0x3F25; Windows, OpenBSD и FreeBSD – 0x402E.

Поле ACK из TCP-пакета. На закрытый TCP-порт отправляется FIN|PSH|URG-пакет с известным значением ISN в поле ISS. Большинство ОС скопируют значение ISN, прибывшее в ISS, в поле ACK ответа. Однако ОС Windows и некоторые сетевые принтеры отправят в поле ACK ответа ISN+1. Если же послать SYN|FIN|PSH|URG-пакет, поведение Windows предсказать трудно. Иногда эта ОС отправляет в поле ACK ответа прибывший ISN, иногда — ISN+1, иногда — по всей видимости, случайное значение. Остается только догадываться, какой код написала Microsoft для обработки подобной ситуации.

Скорость генерации ICMP-пакетов. Стандарт RFC 1812 рекомендует ограничивать количество отправляемых ICMP-сообщений об ошибках. Так Linux, следуя данной рекомендации, позволяет только до 80 сообщений в 4 секунды с простоем в четверть секунды, если это значение было превышено. Замечу, что проведение данного теста требует много времени и создает большую нагрузку на канал.

Этот список можно продолжать и продолжать, но давай в этой маленькой статье рассмотрим и другие способы.

СЕТЕВЫЕ СЛУЖБЫ

Если мы посмотрим, какие службы «торчат» из исследуемой осы, то мы можем с большой вероятностью угадать тип ОСи, стоящей на компе. Так понятно, что служба identd/auth (113) работает обычно только на nix'ах. Для ручной проверки запускаем любой сканер сетевых служб и смотрим результаты. А дальше чешем репу и пытаемся вычислить операционку на основе этих результатов.

СТАНДАРТНЫЕ СЕТЕВЫЕ СЛУЖБЫ

На рабочем сервер всегда запущена куча стандартных служб (сервер же не только комнату обогревает, он еще и делает что-то полезное). Так почти всегда на сервере можно найти http, ftp, smtp и pop3 сервер. Если мы узнаем, какие программы используются для обслуживания этих сервером, то мы опять же легко вычислим тип операционной системы. Так если мы обнаружили, что на сервере стоит IIS, то ОС, скорее всего, винды, а sendmail, скорее, крутится под nix'ом. Также у многих служб можно просто спросить версию операционной системы. Даже если версию ОС мы не узнали, а узнали только версию http-сервера, то этого может быть вполне достаточно для запуска exploit'а.

HTTP

Простейший ручной способ для получения инфы по http-серверу – telnet <host> 80, далее HTTP / GET/1.0{Enter}, в первых строчках ответа будет название http-сервера.

FTP

Для получения инфы от ftp – telnet <host> 21, в ответе от сервера будет названия FTP-сервера, далее залогинившись и набрав команду SYST можно узнать версию операционной системы (но большинство nix уже давно возвращает липовую версию, обычно это - UNIX Type: L8 ;).

SMTP/POP3

telnet <host> smtp, в ответе опять же присутствует название smtp-сервера. Все то же самое и для pop3-сервера: telnet <host> pop3. У nix'овых серверов можно также запросить инфу у identd/auth-сервиса.

Сразу предупреждаю, что все эти простейшие способы известны давно и поэтому админы (особенно nix'овые) сразу меняют данные заголовки на что-нибудь непотребное. Кроме выше перечисленных прямых методов можно использовать косвенные: какие фичи поддерживаются данными программами, файлы с какими расширениями используются, есть/нет шифрование/архива-

ция трафика, какие методы используются для идентификации пользователя и т.д. Ручные способы: меняем регистр запроса (вместо <host>/index.htm пишем <host>/Index.htm), если все прошло без ошибок – значит сервер Windows, иначе - nix, то же самое можно проделать и на ftp. Также можно посмотреть, файлы с каким расширением использует http-сервер для генерации страничек, так расширение asp/aspx с головой выдает Windows, а cgi/bin чаще используется под nix-ами (ну это уже совсем примерно, сойдет разве что для проверки и подтверждения уже определенной ОС – прим. ред.).

Из экзотики стоит упомянуть, что все то же самое можно делать и для менее популярных сервисов (печать, DNS). Для точного определения ОС из семейства Windows можно посмотреть, какие команды из семейства WNet* поддерживаются удаленным сервером.

THE END

На этом уважаемые слушатели наша передача завершается. Напоследок приведу только небольшой список программ, который стоит использовать в нелегком деле коллекционирования вражеских скальпов, то бишь - отпечатков.

Готовые программы/службы для определения ОС-ей:

NetCraft (www.netcraft.com) - сайт, выдает на какой операционке бегает вражий сервак.
Void (void.ru) - кроме ОС-ы сервека, еще выдают инфу по запущенным сервисам.
Nmap (www.insecure.org) - классика, одна из самых мощных программ для определения удаленной операционной системы.
Xprobe (www.sys-security.com) - программа, меняя мощная чем nmap, но тоже интересная.
Passive OS Detection tool (lcamtuf.coredump.cx) – небольшая программа, показывающая идею пассивного (без забрасывания сервера кучей пакетов) определения Оси.
Retina Network Security Scanner (www.eeye.com) - буржуйский коммерческий монстр
ShadowSecurityScanner (www.safety-lab.com) - русская коммерческая программа (регистрация для студентов стоит всего 210 р).
WinFingerprint (winfingerprint.sourceforge.net) – программа для точного удаленного определения версии windows'а.
Snort (www.snort.org) - сниффер с удобным просмотром TTL, Window Size и т.д. из TCP/IP пакета.

SCAN-ЛОГИ

Ну что стоит настоящему хакеру быстренько налабать программку простейшего сканера портов? Лень? Ну вот и нам тоже ЛЕНЬ! Поэтому как настоящие разленившиеся раздолбаи мы заходим по адресу: http://cs.baylor.edu/~donahoo/NIUNet/portscan.html и качаем оттуда файл scan.c с готовым сканером. Еще нам понадобиться файл listofports.dat с описанием портов (брать там же).

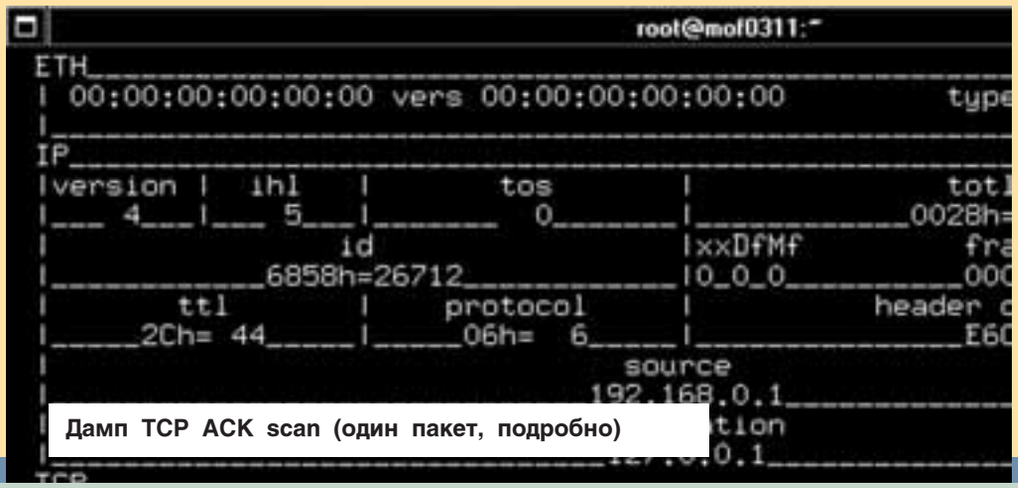
изучаем трассировки сканов

Мопи (mopy@xakep.ru)

Однажды, в Спеце по DoS-атакам, мы уже публиковали логи «подозрительной» сетевой активности. Хоть это и достаточно «скучный» материал, мне пришло очень много писем с просьбами рассказать, как мы делаем эти самые логи, откуда их выдираем. Млин, очень просто мы их делаем – запускаем на своей тачке сниффак и начинаем делать с ней то, логи чего хотим получить. В прошлый раз мы травили несчастный комп DoS-атаками, а в этот раз просто сканили, применяя разные типы сканированя. Сканили опять же со своей тачки, но с заспуфеным IP (для наглядности). Так что ничего особого в этом нет – все просто! Достаточно сложно как раз научиться читать логи. Ну, не то чтобы уж очень сложно – мозговой активности там никакой не надо – просто долго и нудно. Надо обладать нехилым терпением, чтоб сидеть и сравнивать все эти трассировки, подмечать какие-нибудь характерные для атак моменты и тд. Если тебя это не пугает, можешь попробовать повникать в эти логи сканов. А если пугает... – если пугает, тогда продолжай читать Спец, а к этим штукам вернешься, когда поймешь, что это на самом деле не тук уж и все гиморно ;).

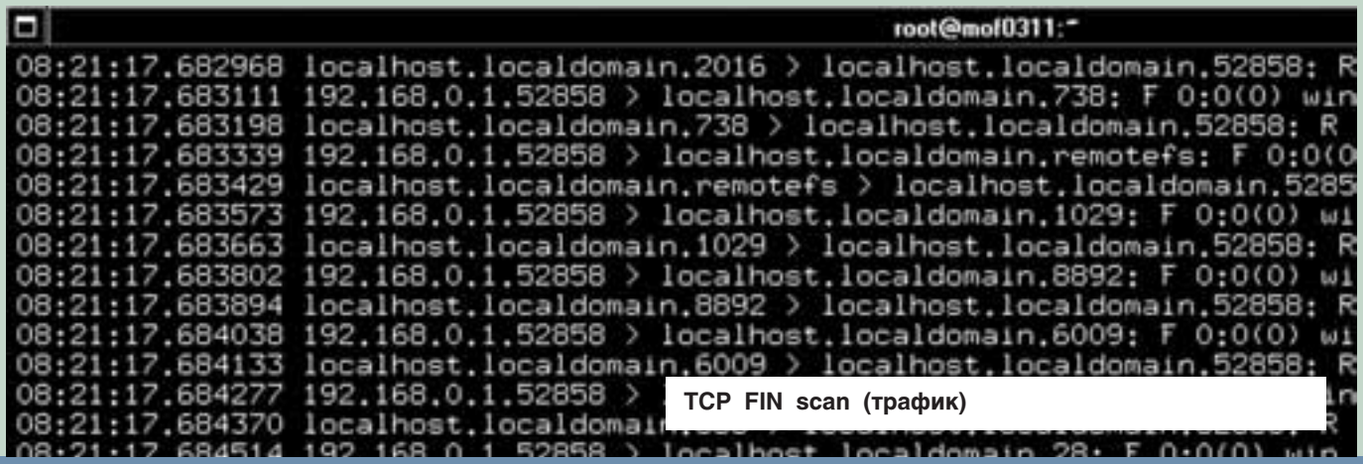
```
root@mol0311:~
08:47:40.468276 192.168.0.1.37308 > localhost.localdomain.2035: . ack 24525
08:47:40.468353 localhost.localdomain.2035 > localhost.localdomain.37308: R
F)
08:47:40.468492 192.168.0.1.37308 > localhost.localdomain.65301: . ack 2452
08:47:40.468570 localhost.localdomain.65301 > localhost.localdomain.37308:
DF)
08:47:40.468702 192.168.0.1.37308 > localhost.localdomain.32771: . ack 2452
08:47:40.468782 localhost.localdomain.32771 > localhost.localdomain.37308:
DF)
08:47:40.468917 192.168.0.1.37308 > localhost.localdomain.570: . ack 245250
08:47:40.468997 localhost.localdomain.570 > localhost.localdomain.37308: R
)
08:47:40.469138 192.168.0.1.37308 > localhost.localdomain.991: . ack 245250
08:47:40.469224 localhost.localdomain.991 > localhost.localdomain.37308: R
)
08:47:40.469359 192.168.0.1.37308 >
08:47:40.469447 localhost.localdomain.180 > localhost.localdomain.37308: R
```

Дамп TCP ACK scan (трафик)

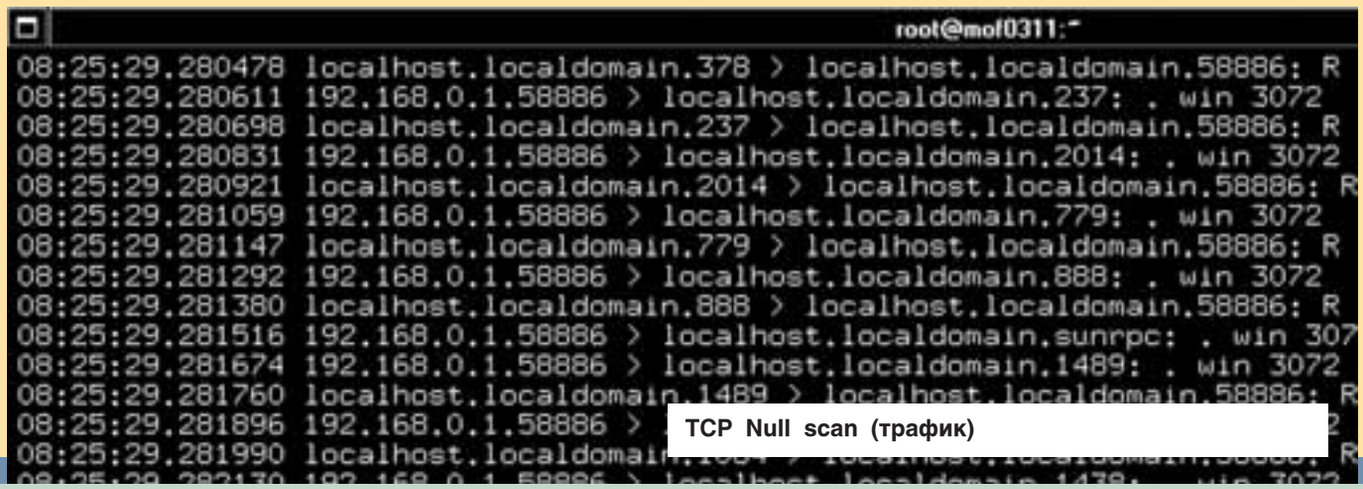

root@mof0311:~
ETH
00:00:00:00:00:00 vers 00:00:00:00:00:00
IP
version
ihl
tos
id
6858h=26712
ttl
protocol
2Ch= 44
06h= 6
source
192.168.0.1
Дамп TCP ACK scan (один пакет, подробно)


root@mof0311:~
08:57:40.565075 localhost.localdomain.45485 > localhost.localdomain.1002: S
7 <mss 16396,sackOK,timestamp 1478356 0,nop,wscale 0> (DF)
08:57:40.565174 localhost.localdomain.1002 > localhost.localdomain.45485: R
08:57:40.565933 localhost.localdomain.45486 > localhost.localdomain.690: S
<mss 16396,sackOK,timestamp 1478357 0,nop,wscale 0> (DF)
08:57:40.566036 localhost.localdomain.690 > localhost.localdomain.45486: R
08:57:40.566762 localhost.localdomain.45487 > localhost.localdomain.3900: S
7 <mss 16396,sackOK,timestamp 1478357 0,nop,wscale 0> (DF)
08:57:40.566857 localhost.localdomain.3900 > localhost.localdomain.45487: R
08:57:40.567586 localhost.localdomain.45488 > localhost.localdomain.2: S 40
mss 16396,sackOK,timestamp 1478357 0,nop,wscale 0> (DF)
08:57:40.567685 localhost.localdomain.2 > localhost.localdomain.45488: R 0:
08:57:40.568409 localhost.localdomain
7 <mss 16396,sackOK,timestamp 1478357
TCP connect scan (трафик)

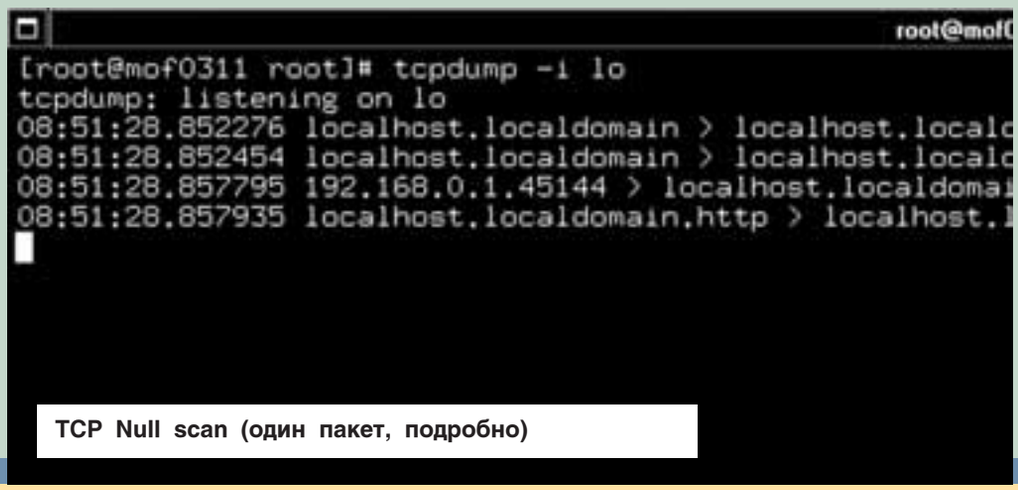

root@mof0311:~
ETH
00:00:00:00:00:00 vers 00:00:00:00:00:00
IP
version
ihl
tos
id
B676h=46710
ttl
protocol
40h= 64
06h= 6
source
127.0.0.1
TCP connect scan (один пакет, подробно)


root@mof0311:~
08:21:17.682968 localhost.localdomain.2016 > localhost.localdomain.52858: R
08:21:17.683111 192.168.0.1.52858 > localhost.localdomain.738: F 0:0(0) win
08:21:17.683198 localhost.localdomain.738 > localhost.localdomain.52858: R
08:21:17.683339 192.168.0.1.52858 > localhost.localdomain.remotefs: F 0:0(0
08:21:17.683429 localhost.localdomain.remotefs > localhost.localdomain.5285
08:21:17.683573 192.168.0.1.52858 > localhost.localdomain.1029: F 0:0(0) wi
08:21:17.683663 localhost.localdomain.1029 > localhost.localdomain.52858: R
08:21:17.683802 192.168.0.1.52858 > localhost.localdomain.8892: F 0:0(0) wi
08:21:17.683894 localhost.localdomain.8892 > localhost.localdomain.52858: R
08:21:17.684038 192.168.0.1.52858 > localhost.localdomain.6009: F 0:0(0) wi
08:21:17.684133 localhost.localdomain.6009 > localhost.localdomain.52858: R
08:21:17.684277 192.168.0.1.52858 >
08:21:17.684370 localhost.localdomain
TCP FIN scan (трафик)

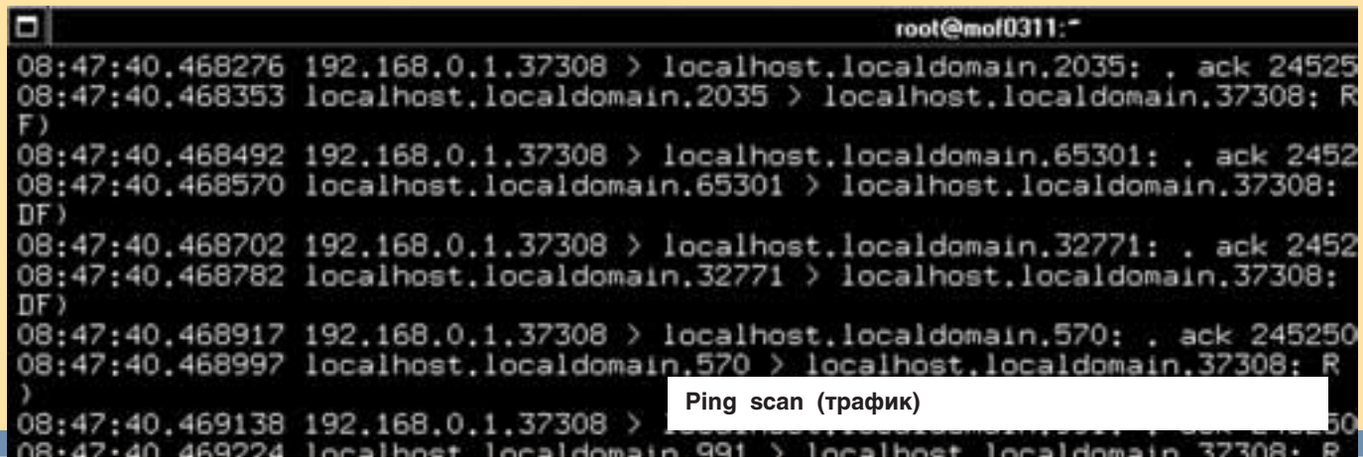
TCP FIN scan (один пакет, подробно)



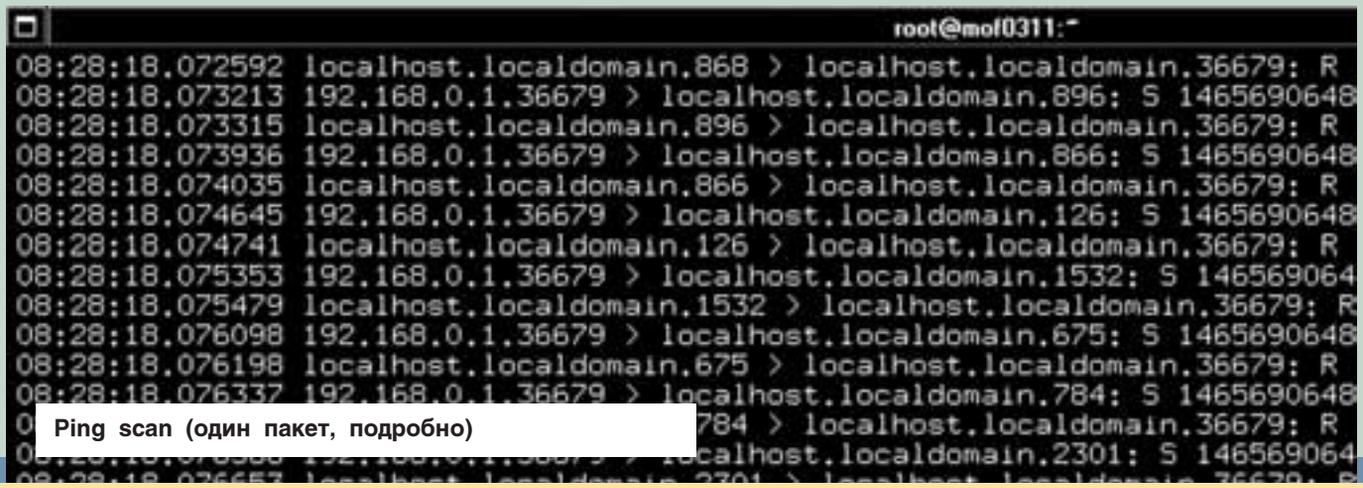
TCP Null scan (трафик)

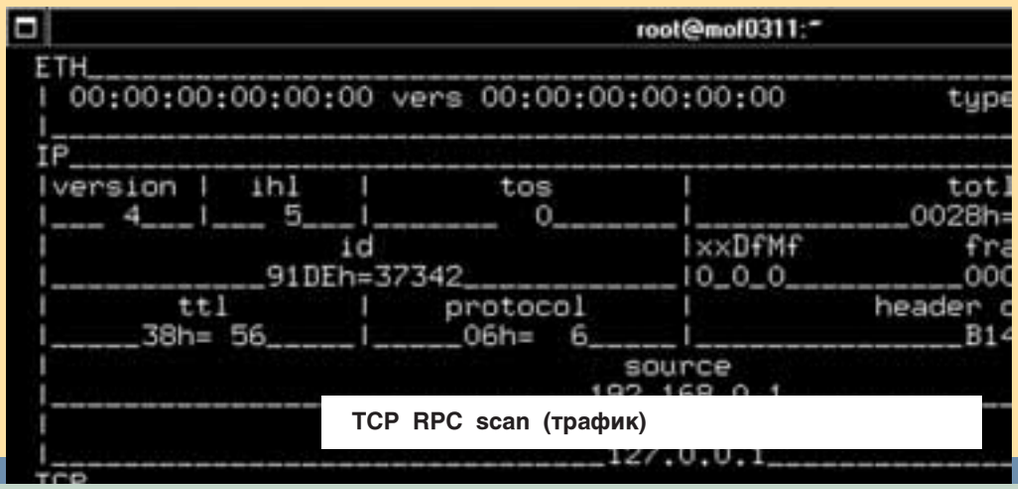


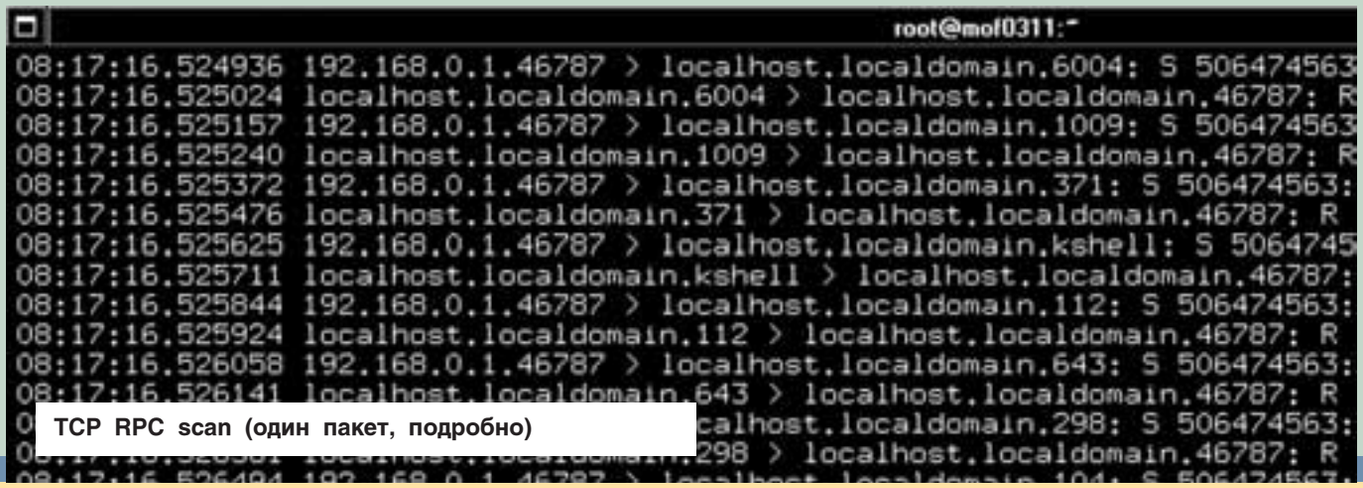
TCP Null scan (один пакет, подробно)



Ping scan (трафик)


root@mof0311:~
08:28:18.072592 localhost.localdomain.868 > localhost.localdomain.36679: R
08:28:18.073213 192.168.0.1.36679 > localhost.localdomain.896: S 1465690648
08:28:18.073315 localhost.localdomain.896 > localhost.localdomain.36679: R
08:28:18.073936 192.168.0.1.36679 > localhost.localdomain.866: S 1465690648
08:28:18.074035 localhost.localdomain.866 > localhost.localdomain.36679: R
08:28:18.074645 192.168.0.1.36679 > localhost.localdomain.126: S 1465690648
08:28:18.074741 localhost.localdomain.126 > localhost.localdomain.36679: R
08:28:18.075353 192.168.0.1.36679 > localhost.localdomain.1532: S 146569064
08:28:18.075479 localhost.localdomain.1532 > localhost.localdomain.36679: R
08:28:18.076098 192.168.0.1.36679 > localhost.localdomain.675: S 1465690648
08:28:18.076198 localhost.localdomain.675 > localhost.localdomain.36679: R
08:28:18.076337 192.168.0.1.36679 > localhost.localdomain.784: S 1465690648
784 > localhost.localdomain.36679: R
Ping scan (один пакет, подробно)
localhost.localdomain.2301: S 146569064


root@mof0311:~
ETH
00:00:00:00:00:00 vers 00:00:00:00:00:00
IP
version | ihl | tos
4 | 5 | 0
id
91DEh=37342
ttl | protocol
38h= 56 | 06h= 6
source
127.0.0.1
TCP RPC scan (трафик)


root@mof0311:~
08:17:16.524936 192.168.0.1.46787 > localhost.localdomain.6004: S 506474563
08:17:16.525024 localhost.localdomain.6004 > localhost.localdomain.46787: R
08:17:16.525157 192.168.0.1.46787 > localhost.localdomain.1009: S 506474563
08:17:16.525240 localhost.localdomain.1009 > localhost.localdomain.46787: R
08:17:16.525372 192.168.0.1.46787 > localhost.localdomain.371: S 506474563:
08:17:16.525476 localhost.localdomain.371 > localhost.localdomain.46787: R
08:17:16.525625 192.168.0.1.46787 > localhost.localdomain.kshell: S 5064745
08:17:16.525711 localhost.localdomain.kshell > localhost.localdomain.46787:
08:17:16.525844 192.168.0.1.46787 > localhost.localdomain.112: S 506474563:
08:17:16.525924 localhost.localdomain.112 > localhost.localdomain.46787: R
08:17:16.526058 192.168.0.1.46787 > localhost.localdomain.643: S 506474563:
643 > localhost.localdomain.46787: R
TCP RPC scan (один пакет, подробно)
298 > localhost.localdomain.46787: R


root@mof0311:~
ETH
00:00:00:00:00:00 vers 00:00:00:00:00:00
IP
version | ihl | tos
4 | 5 | 0
id
B1B6h=45494
ttl | protocol
34h= 52 | 06h= 6
192.168.0.1
TCP SYN scan (трафик)

ПОЖМЕМ ДРУГ ДРУГУ РУКИ!

разбор методов сканирования

Ты, наверное, как истинный кул хацкер, не можешь недооценить полезность и рулезность исследования системы методом сканирования портов с целью выявления уязвимых мест. А сканировать, не зная самих методов сканирования, - это fo lamaz. Так что давай не будем уподобляться этим животным, дающим столь ценную шерсть, и разберемся с этим вопросом.

stix (f3x@hotmail.ru)

Перед рассмотрением всего, что пойдет ниже, хотелось бы отправить читателя, то есть тебя, поглядеть на опус о TCP - RFC 793, который непосредственно касается рассматриваемой нами темы. Но я же понимаю, что у тебя нет на это времени, и попробую растолковать все на пальцах :).

Итак, первое, что ты должен понять, это механизм установления TCP-соединения, который состоит из трех фаз, этапов, ступеней - короче, неважно. Комп, устанавливающий соединение, сначала посылает TCP-пакет с установленным флагом SYN, после чего принимающий комп (адресат) посылает в ответ TCP-пакет с установленными флагами SYN и ACK, если порт открыт, и - второй вариант развития данного действа - если порт не активен (закрыт), происходит разрыв соединения с помощью TCP-пакета с установленным флагом RST, который отсылает адресат. Третья фаза заключается в следующем: после получения от адресата TCP-пакета с установленными флагами SYN и ACK в ответ на этот пакет отсылает TCP-пакет с установленным флагом ACK (само собой, все эти пакеты имеют соответствующие номера последовательностей sequence numbers (отвечающих за правильность принятия) и номера подтверждений acknowledge numbers (отвечающих за успешное принятие пакетов). После всего этого соединение считается установленным. Данная процедура имеет, как уже было замечено выше, свое название: «трехуровневое рукопожатие» или «трехфазное рукопожатие», или, короче, просто handshake, то есть рукопожатие.

С процедуры установления соединения (рукопожатия) начинается любой сеанс обмена данными между удаленными компами. Необходимо также ввести ясность в понятие флага (SYN, ACK, RST). Что это за байдень такая?

Любой TCP-пакет состоит из некоторого строго определенного набора полей разной длины, заполняющихся некоторым значением (или 1, или 0), так вот, флаг SYN - это флаг или поле, значение которого установлено в 1, т. е. активировано. Пакет, установленный с флагом SYN, инициирует соединение. Флаг ACK используется для подтверждения успешного принятого пакета, флаг RST - отвечает за сброс соединения. Существуют определенные законы, по которым данным флагам назначаются значения. Они назначаются исходя из ситуации и условий - это означает, что нельзя сформировать TCP-пакет от балды, с каким-то набором установленных флагов, который будет отправлен в сеть и перевернет для тебя все вверх ногами. Рассмотрение всех этих законов является темой отдельной статьи, поэтому не пугайся - в этой статье тебе будет дано все, что тебе необходимо знать, и не больше.

Все, что бы тебе ни говорилось, конечно же, требует незамедлительной проверки и подтверждения. «Доверяй, но проверяй» - как гласит народная мудрость. В качестве подтверждения описываемых ниже методов и примеров их использования будет юзаться супер всемирно известная боевая софтина - nmap - и не менее известная прога - hping. Кстати, недавно в сети был выложен свежий релиз - nmap-3.0 (http://www.insecure.org), так что, недолго думая, чтобы быть на гребне волны, вперед, запускай свой супер грабер Интернета и будешь во всеоружии. Тем более, что описание обеих софтин и их применение уже не раз приводилось в][. Да, кстати, чуть не забыл, если ты яростный поклонник форточек, то на том же сайте (http://www.insecure.org) ты можешь залить себе релиз данной тулзы под Win32, и тогда тебя вообще ничего не будет напрягать, кроме возможных последствий производимых тобой действий, так что намотай себе это на ус и будь осторожен. Аминь!

Ну, вроде все, после необходимого этапа вооружения можно перейти к этапу применения.

МЕТОДЫ СКАНИРОВАНИЯ

1. TCP Connect scan (TCP-сканирование подключением)

Вспомни о рукопожатии. При сканировании данными типом осуществляется попытка полного подключения посредством протокола TCP к интересующим тебя портам, то есть в данном случае происходит полная процедура установления соединения (handshake). После чего происходит отключение.

Применение:

```
# nmap -sT target-ip
```

или просто

```
# nmap target-ip
```

```
Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on (target-ip):
(The 1513 ports scanned but not shown below are in state: closed)
```

Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
80/tcp	open	http

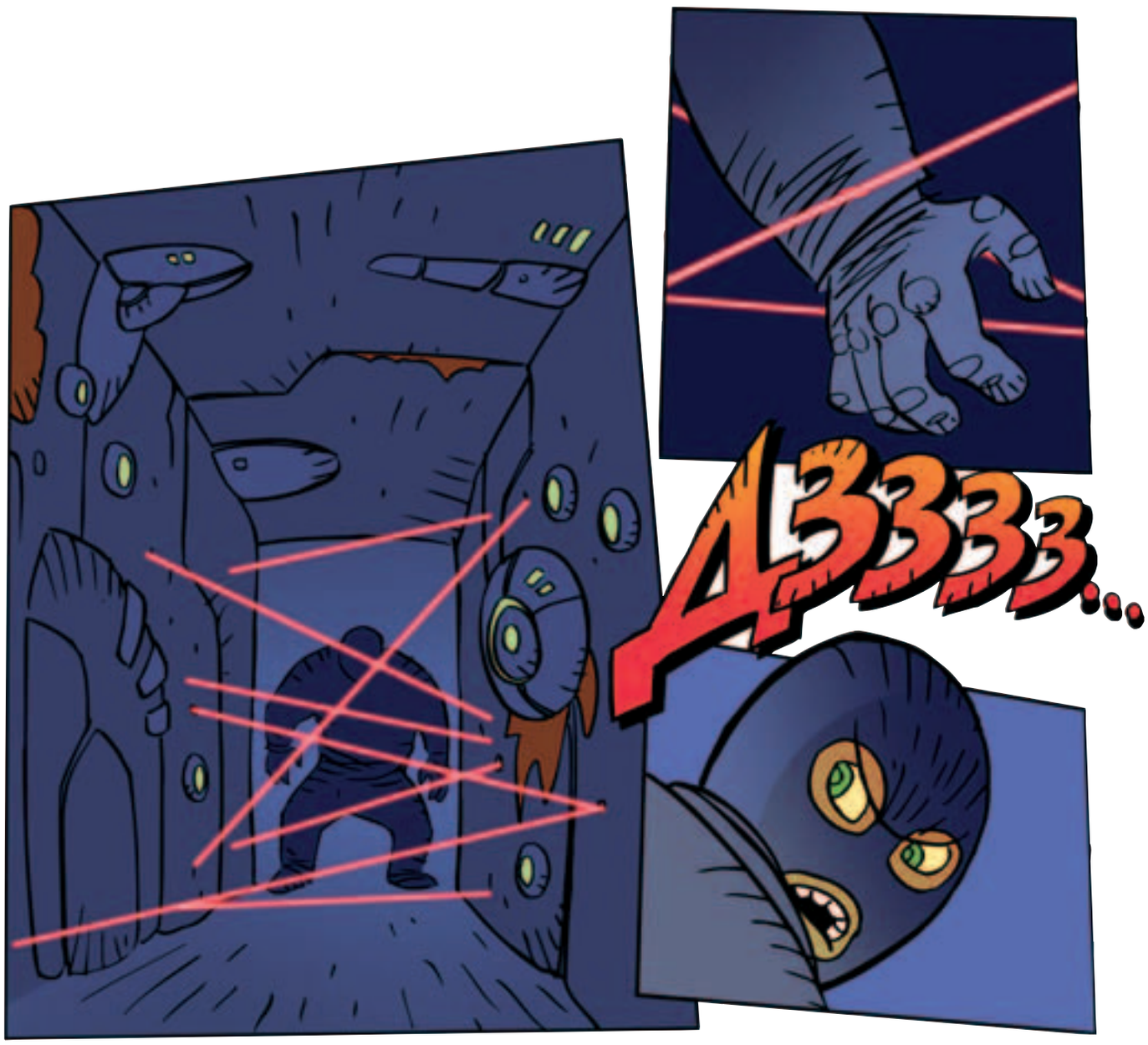
Вторая строка в примере означает то, что данный тип сканирования используется по умолчанию, то есть прямой необходимости в опции -sT нет. Target-ip - айпишник исследуемой системы. С данной опцией без указания определенного порта (см. опцию -p) сканироваться будет вся система на наличие открытых портов.

Если ты еще ходишь на своих двоих, то есть тебе их еще не поломали, это значит, что админы до полусмерти упились пивом, поскольку данный тип сканирования очень легко вычисляется и твой ip-адрес наверняка попадет в логи, поэтому мой добрый тебе совет, старайся данный тип сканирования не использовать вообще!

2. TCP SYN scan (TCP-сканирование пакетами с установленным флагом SYN)

Главное отличие данного типа сканирования от предыдущего заключается в том, что фаза установления соединения (handshake) обрывается на половине. Рассмотрим более детально данный тип сканирования. На порт назначения отправляется TCP-пакет с установленным флагом SYN. Если в ответ поступает пакет, содержащий установленные флаги SYN/ACK, это означает, что данный порт открыт (находится в состоянии listeninig, информацию о состоянии портов, открытых на твоем компе, ты можешь получить, воспользовавшись из командной строки командой netstat -an; введя эту команду без параметров, ты сможешь получить информацию о других опциях (существует несколько основных состояний порта listening - порт открытый, в состоянии прослушивания и establishing - соединение с портом установлено, и еще куча промежуточных, которые не имеют для нас особой важности). Если же в ответ приходит пакет с установленными флагами RST/ACK, то, как правило, данный порт отключен или находится за файрволом.

Применение данного типа сканирования более предпочтительно, нежели TCP Connect scan, поскольку он скрытнее, но, тем не менее, если на целевой системе работает система обнаружения кул хацкеров (IDS - Intruder Detection System - система обнаружения вторжений), то тебе не поздоровится! Но поскольку системы обнаружения вторжений



не понатыканы еще везде, то такие действия скорее всего останутся незамеченными.

Применение:

```
#nmap -sS target-ip
```

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)
Interesting ports on (target-ip):
(The 1543 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
80/tcp	open	http
110/tcp	open	pop-3
443/tcp	open	https
8080/tcp	open	http-proxy

Nmap run completed — 1 IP address (1 host up) scanned in 2 seconds

3. TCP Fin scan (TCP-сканирование пакетами с установленным флагом FIN)

Флаг Fin отправляется в TCP-пакете в случае закрытия TCP-соединения. В соответствии с опусом RFC 793 о TCP в ответ на данный пакет целевой комп должен ответить TCP-пакетом с установленным флагом RST для всех закрытых портов. Но здесь есть одна особенность, которая заключается в том, что стэк TCP/IP юниховых систем действует по RFC 793, а стэк форточек работает от балды в зависимости от версии, часто вообще непредсказуемо, но удивляться нечему, ведь это мелкософт. Поэтому данный тип сканирования желательно применять только к юниховым системам, иначе ты рискуешь получить рак головного мозга от результатов сканирования. Данный тип сканирования сравнительно трудно определить без специально настроенной системы IDS.

Применение:

```
#nmap -sF target-ip
```

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)
Interesting ports on xxxxxxxxxx (target-ip):
(The 1540 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
110/tcp	open	pop-3
143/tcp	open	imap2
443/tcp	open	https
1025/tcp	open	listen
3306/tcp	open	mysql

4. TCP Xmas Tree scan

(TCP-сканирование методом «рождественской елки»)

С Новым годом тебя! Короче, быстро одеваешься и бежишь в ближайшее место столпотворения елок... Елок - телок :)! Телок - елок ;)! Не забудь топор - он тебе понадобится. Срубай себе одну, возвращайся домой, наряди ее в своем компьютерном бункере возле компа и приступай к сканированию, которое заключается в следующем: на целевые порты отправляются TCP-пакеты с установленным флагами FIN/URG/PUSH. Флаги URG/PUSH указывают на то, что данный пакет должен быть отправлен срочно, не вставая в очередь пакетов на отправку. В соответствии с вездесущим опусом 793 целевой комп в ответ должен отправить пакет с установленным флагом RST для всех закрытых портов. Также данный тип пакетов может применяться для определения портов, которые фильтруются файрволом или брандмауэром. Такой метод сканирования определяется с напрягами ;).

Применение:

```
#nmap -sX target-ip
```

```
Starting nmap V. 2.54BETA30
All 1549 scanned ports on xxx.xxx.xxx.xxx (target-ip) are: filtered

Nmap run completed — 1 IP address (1 host up) scanned in 102 seconds
```

5. TCP Null scan

(TCP-сканирование нулевыми пакетами)

Во время сканирования нулевыми пакетами на целевой комп направляются TCP-пакеты - голяки (голимые :)), т.е. пакеты с отключенными флагами, такие себе пустышки. На что целевой комп должен послать тебя, то есть тебе, TCP-пакет с установленным флагом RST для всех закрытых портов.

Применение:

```
#nmap -sN target-ip
```

```
Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/)
Interesting ports on xxxxxxxxxxxxx (target-ip):
(The 1540 ports scanned but not shown below are in state: closed)
   Port        State       Service
   25/tcp      open        smtp
   53/tcp      open        domain
   80/tcp      open        http
   443/tcp     open        https
   3306/tcp    open        mysql

Nmap run completed — 1 IP address (1 host up) scanned in 11 seconds
```

6. TCP Ack scan

(TCP-сканирование пакетами с установленным флагом ACK)

Обычный стек TCP/IP должен ответить пакетом с установленным пакетом RST для всех закрытых портов. Данный тип сканирования очень полезен при определении и обходе брандмауэров, поскольку позволяет выявить критерии, в соответствии с которыми на нем производится фильтрация. Также данный тип пакетов очень удобно использовать для налаживания соединения сквозь уже пробитый брандмауэр, для этого существуют специальные проги, состоящие из клиента и сервера, типа троянов - подробно об этом в следующем номере ;). Так вот, в TCP-пакетах с установленным флагом ACK можно передавать свою инфу, то есть управлять удаленной системой, при этом брандмауэр ничего не заметит, так как в большинстве из них фильтрация пакетов с установленным флагом ACK отключена по умолчанию. Определяется трудно!

Применение:

```
#hping target-ip -S -p 80 -f
```

7. TCP Windows scan

(TCP-сканирование размером окна)

Есть такая штука в TCP/IP, как размер окна (соответственно в TCP пакете есть поле для него), которая определяет количество пакетов, которое может получить целевая система за один раз. Метод сканирования, основанный на данном поле TCP-пакета, позволяет выявлять порты на удаленных компах и определить, фильтруются они или нет. То есть определить, существует ли потенциальная угроза остаться без ног :). Определить данный вид сканирования трудновато.

Применение:

```
#hping target-ip -S -p 25 -w
```

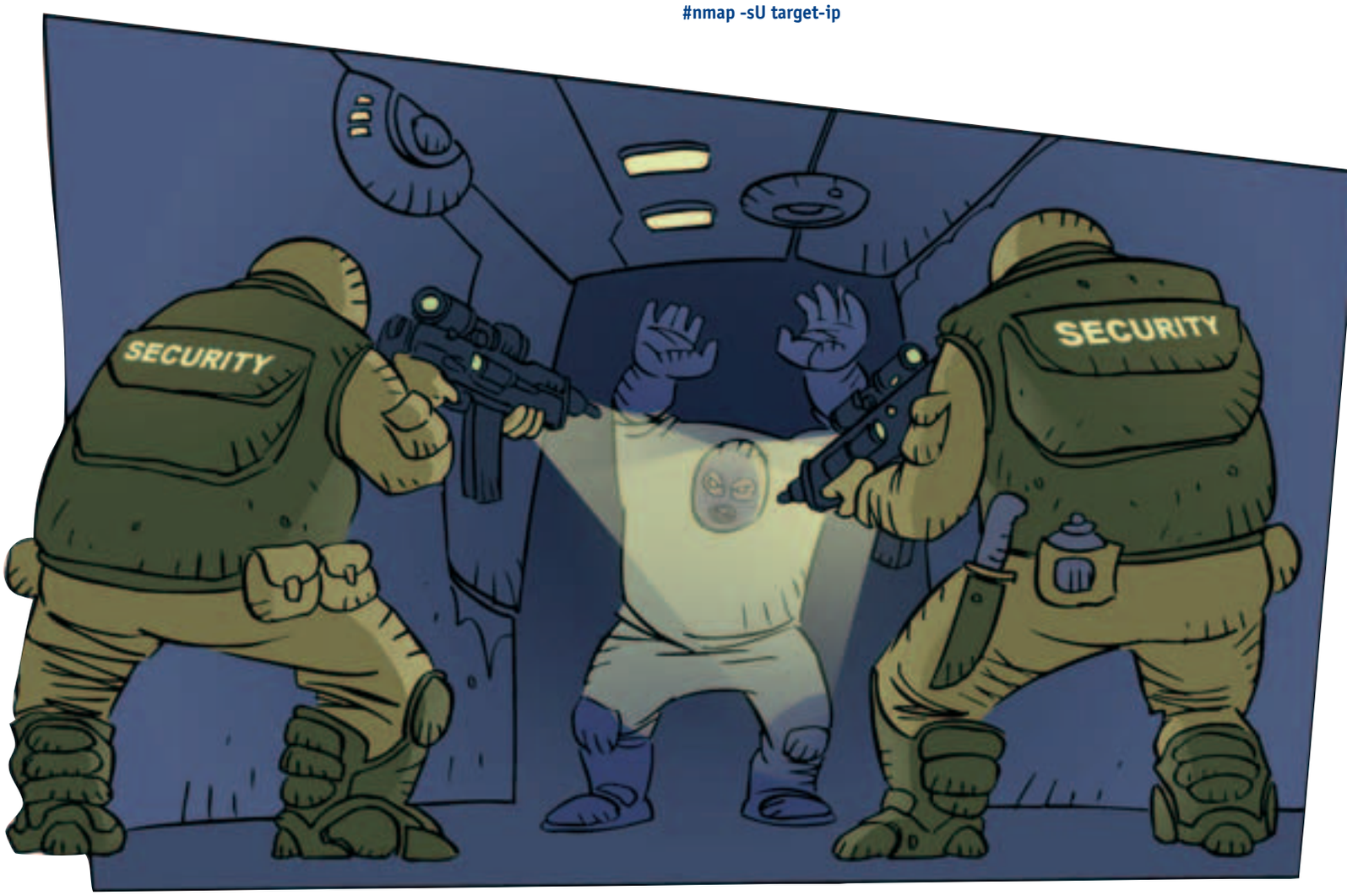
8. TCP RPC scan
(TCP-сканирование RPC портов)

Вообще RPC (Remote Procedures Calls) - это специальная сетевая служба, использующаяся для удаленного вызова процедур; данный метод сканирования применяется только к юникам. В юниках этой службе выделяется некоторый диапазон портов (как правило, 31000 - 32000), связанных с определенными сервисам, входящими в службу вызова удаленных процедур. Определить факт сканирования легко :(.

Применение:

```
#nmap -sS -R target-ip
```

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)
Interesting ports on xxxxxxxxxxxxx (target-ip):



(The 1540 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http

Nmap run completed — 1 IP address (1 host up) scanned in 9 seconds

Здесь параметр -R указывает на то, что необходимо отсканировать порты служб RPC; как правило, должен использоваться с каким-либо еще типом сканирования в паре, в примере с -sS.

9. UDP scan (UDP-сканирование)

Данный тип сканирования использует не TCP протокол, а UDP. Посылает UDP-пакет на какой-либо порт - если в ответе приходит сообщение Icmp port unreachable, это означает, что порт закрыт; если же такое сообщение не пришло, значит делай соответствующий вывод о том, что порт открыт. В соответствии с природой UDP данный протокол не гарантирует надежность доставки пакетов компу-адресату (в отличие от TCP), то есть достоверность результатов данного типа сканирования весьма относительна. После запуска данного типа сканирования советую тебе лечь поспать, поскольку данный метод очень медленный, я бы даже назвал его чемпионом мира по тормознутости среди всех перечисленных типов сканирования. В соответствии с чем применяй его на практике очень редко или вообще не применяй. Определяется легко.

Применение:

```
#nmap -sU target-ip
```

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)

Interesting ports on localhost.genevadata.net (127.0.0.1):
(The 1451 ports scanned but not shown below are in state: closed)

Port	State	Service
53/udp	open	domain

Nmap run completed — 1 IP address (1 host up) scanned in 470 seconds

Напоследок хотелось бы посоветовать тебе побольше практиковаться (не на чужих серваках, естественно), поскольку, даже вооруженный данными знаниями, ты можешь попасть в непонятку, поскольку, как уже было замечено в статье выше, очень многое зависит от конкретной реализации стэка TCP/IP каждой отдельной ОС. Так что крепись и будь внимателен!

СКАНЕРЫ БЕЗОПАСНОСТИ ПОД WIN

Любителей похакерить сейчас пруд пруди. А некоторые, особо одаренные делают это умышленно и даже (кто бы мог подумать!) с корыстной целью. Поэтому, еще со времен появления Первого Хакера Всея Инета, люди задумались о безопасности своих систем. Сканеры сетевой безопасности стали появляться лет десять назад, когда кого-то осенила идея, что не плохо было бы заиметь эдакое диагностическое средство, для анализа безопасности. Хотя это с какой стороны посмотреть: кого-то волнует безопасность сети, а кого-то «опасность»:).

marooned (fddx@land.ru)

ЧЕМ КОПАТЬ БУДЕМ

Сканер производит анализ сети (отдельного ее узла или просто удаленного компьютера), который состоит из поиска уязвимостей (скромно называемых в народе «дырами»): дефолтных паролей, бакланских настроек сервера, бажного ПО, установленного на нем, левых скриптов и так далее. Сначала, он собирает информацию о доступных узлах сети и анализирует полученные результаты, потом создает отчеты и выносит рекомендации, а некоторые сканеры могут даже автоматически устранить найденную уязвимость или выдать фикс-скрипт.

Разработчики, как правило, вовсю расхваливают свои продукты, уникальные технологии, хотя понятно, что ни один из них не способен обнаружить все дыры. По принципу действия все сканеры очень похожи на антивирусы, потому что у каждого сканера есть база данных, содержащая описание всех известных дыр, которое сравнивается с результатами анализа. Это и является своего рода ограничением.

По идее любой уважающий себя сканер должен уметь сканировать:
- Web-, FTP- и почтовые серверы;
- броузеры, почтовые программы и серверы баз данных;
- пароли и учетные записи;
- подверженность DoS-атакам;
- права доступа к файлам и каталогам;

а также:
- распознавать тип сервера;
- использовать многопоточное сканирование;
- работать через прокси;
- автоматически обновлять свои базы данных;
- выводить отчет в HTML;
- иметь дополнительные функции, типа Whois.

Ну и, естественно, у каждого сканера обычно есть своя фича, типа «супер-пупер эвристический анализ» с помощью которого он может попытаться найти новые дыры, которых нет у него в базе.

Для начала сканер определяет тип ОС, ее версию, используемые сервисы и протоколы. Выяснив это, он ищет все доступные ресурсы, например, открытые порты и «грабит» их заголовки, чтобы узнать оттуда, например, версию ПО. И если у него в базе данных есть дыра по этой версии, то он сразу скажет об этом, а также о степени опасности дырки. Но Хитрый админ, начитавшийся Bugtraq'ов, может изменить заголовок или, заранее зная о дыре, вовремя нашлепать фикс. Потому точно проверить, есть ли дыры, можно, проведя на сервак атаку (обычно сканеры предлагают всевозможные DoS-атаки и иногда брутфорс паролей), причем сканер честно предупредит, что это опасно и нехорошо :). И вот, наступает долгожданный момент: проверка закончилась - в отчете ни одной дырки. Лезем в лог сканера - опять ничего! Однако рано обламываться: если сканер дыр на хосте не нашел, это еще не значит, что их там нет. Может, там установлен файервол или еще какие фильтры. К тому же автоматическая проверка может и пропустить распространенную дыру, которую легко найти вручную. Конечно, шансов найти дыры в удаленной системе не так много, но кто ищет, тот ведь всегда найдет… А когда найдет…

Сканер-убийца. Убийца во всех смыслах. Работает очень медленно… Но эффективно. А медленно, наверное, из-за гигантского количества проверок - более 19000!

XSPIDER

«Первый российский сканер» - эта гордая надпись прочно приклеилась к XSpider'у. И это есть превеликий гуд :). Сканер бесплатен (пока), разговаривает на родном языке и уже успел завоевать известность. Интерфейс понравился мне больше всех - удобный, простой и в то же время не перегруженный всякими эффектами и графикой.

Рис. 1. Первый отечественный сканер.

И функциональность, надо сказать, не уступает. Имеются довольно подробные настройки и, что особенно приятно, по каждому сервису паук умеет проводить DoS-атаки. Порадовала фишка - проверка прокси на анонимность: задаешь IP-адрес и порт, и паук проверяет анонимность сервака. Имеется также отличный CGI-сканер. Так как все базы данных паука хранятся в текстовых файлах, их можно редактировать ручками: идем, например, на kodsweb.ru качаем cgi-словарь, сливаем и повышаем тем самым вероятность найти дыру. Плюс еще у XSpider'а имеются простые TCP и UDP порт-сканеры, TCP и UDP клиенты и WhoIs.

Отчеты получаются простые и понятные, есть линки на сайт с подробным описанием найденной дырки и на патч. Жаль, что некоторые описания на англицком языке. Одна только фигня - пока что нет мануалки. И напоследок скажу, что XSpider умет маскировать от IDS (Intrusion Detection System).

Что ж, первый блин, да не комом.

SHADOW SECURITY SCANNER

Это сканер от создателей известной проги Shadow Scan. Посмотрим, что же они наваяли. Встречают, как говорится, по одежке, а одежка у него ничего себе: появился «из воздуха», с плоскими контролзами, выделение при наведении мыши. И, уж не знаю от чего, все это хозяйство слегка тормозит ;). Однако под шубой обнаружились все стандартные функции и даже больше. Анализируются аж 19 сервисов, в том числе: MSSQL, IBM BD2,

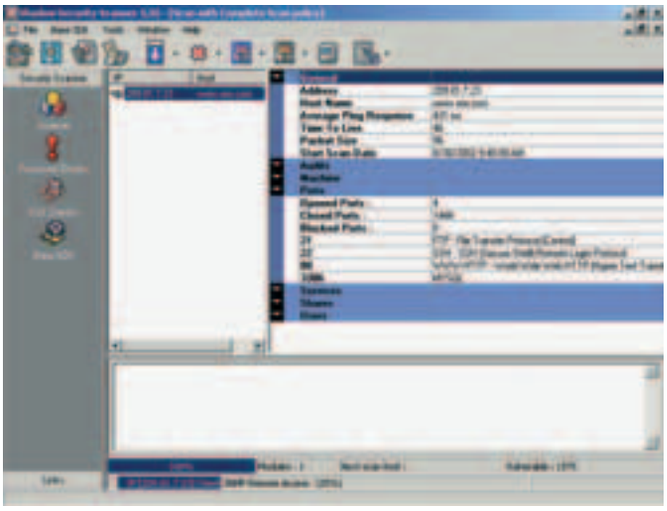


Рис. 2. Сканер от создателей Shadow Scan.

Oracle, MySQL, PostgressSQL, Interbase и MiniSQL, а DoS-атаки выделены в отдельную проверку.
Чтобы начать сканировать, надо создать новую сессию и выбрать правило/политику (policy), которое можно создать и редактировать там же. Правило представляет собой совокупность настроек, с которыми будет проводиться данная сессия. В принципе удобная штука: чем каждый раз лазить в настройки, лучше наделать правил и выбирать в соответствии с ситуацией. Сами настройки мне тоже понравились, все подробно и удобно: прямо в том же окне появляется описание проверки. Можно писать собственные модули сканов на любом языке, только в виде DLL (примеры на Си и Дельфях в папке Plugins). А можно создавать свои проверки с помощью встроенного средства с громким названием SDK. Выбираешь тип проверки, вводишь описание и данные для проверки (скрипт, номер порта и так далее).

Отчеты у SSS не менее навороченные, чем сам сканер: туда впихивают кучу графиков, а всю собранную инфу разбивают по категориям. Ну и фишка дня: при нажатии на Ok в окне about, оно почкуется на две части, которые расползаются в стороны, причем их можно ловить за заголовок. Я игрался минут десять :)))).

LANGUARD NETWORK SCANNER

Еще один неплохой сканер, хотя и платный. Простой, но продуманный интерфейс - справа информация о ходе проверки, а слева результаты.
Прога изначально задумывалась для локальных сетей, и только с версии 2.0 стала универсальным сканером. Сильно отличает этот сканер от остальных способность отлично работать с NetBIOS, фигачить список ресурсов, сервисов и пользователей. Также хорошо прога знает слабые места реестра. Все дыры в базе данных имеют Bugtraq ID. Есть также такая полезная функция

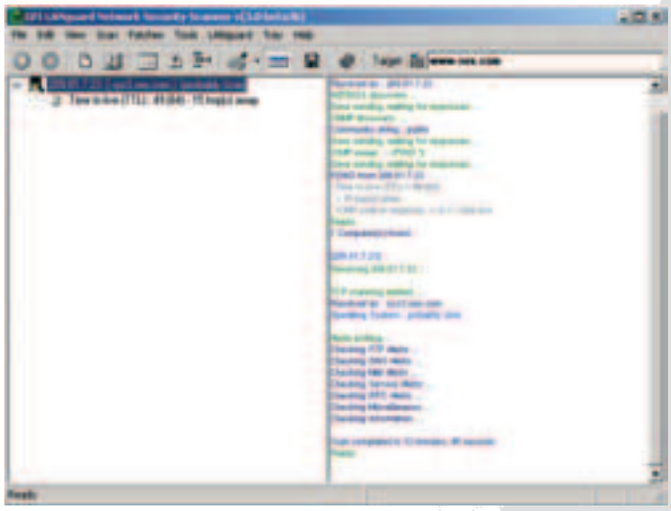


Рис. 3. LANGuard Network Scanner.

как Traceroute, забытая почему-то остальными прогами. Ну и пара фирменных вещей. Первая - это Results comparnison - сравнивает результаты сканирования с прошлыми результатами и позволяет обнаруживать изменения (например, новые сервисы и дыры, новых пользователей). И вторая - собственный язык скриптов (LANS) для написания своих проверок - очень простой с примерами и подробным мануалом. После проверки выдает довольно приятный HTML/XML-отчет.

X-SCAN

Эту вещицу сработали братья-китайцы, и она, конечно, бесплатная. Все в X-Scan'е очень просто. Минимум настроек: диапазон IP и портов, параметры HTTP-запросов, а также выбор сканируемых сервисов из стандартного набора. Интерфейс тоже небогат: вывод результата на одной вкладке и состояние текущего потока на другой.

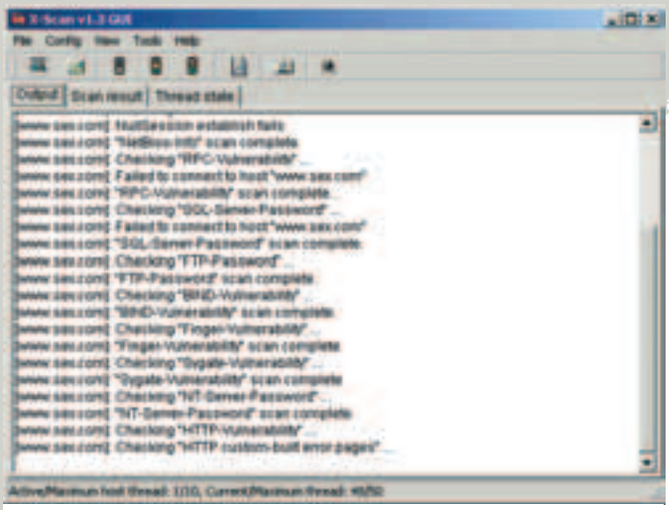


Рис. 4. Сканер из Китая.

Но с другой стороны, прога создавалась для работы из командной строки, потому, наверное, и интерфейс слабый. К тому же X-Scan имеет один из самых толстых CGI-словарей, так что пока еще может дать фору другим сканерам. В readme описан формат плагина, и умеющий писать на Си сможет написать его себе и возрадоваться.
Результаты можно сохранить в html-формате, правда, зачем-то в двух файлах, один из которых почти пустой, а тот, который не пустой, не очень читабельный, так как комментарии отсутствуют напрочь. Как и у всех, для известных дыр есть заплатки, а за остальными надо идти на сайт разработчика - может там есть.

NMAP

Мощный бесплатный сканер с открытым кодом. Есть варианты сканера для командной строки и почти для всех ОС. По сути, это сканер портов, так как предупреждать о том, что есть дыра, он не умеет. Зато с портами работает профессионально, быстро и имеет очень гибкие настройки.

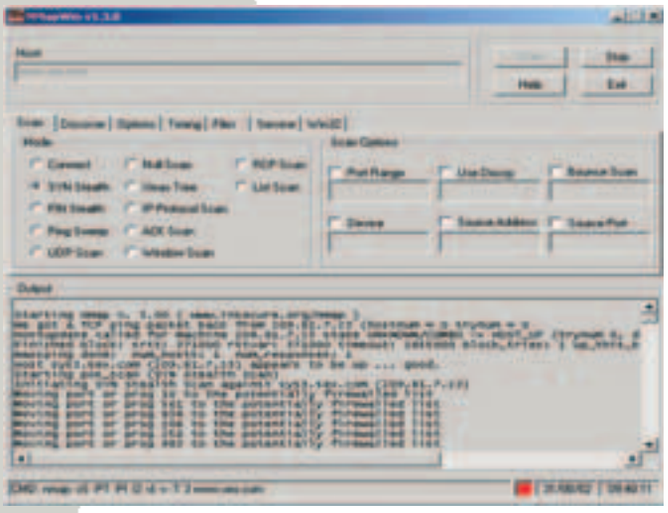


Рис. 5. Network Mapper - теперь с GUI.

Для работы Nmap использует кучу методов сканирования, таких, как UDP, TCP connect, SYN (полуоткрытое), FTP proxy, ICMP (ping), FIN, ACK, Xmas tree и NULL-сканирование (подробно и с примерами все эти методы рассматриваются с статье «Пожмем друг другу руки!» – прим. ред.).
Еще он умеет определять ОС хоста по отпечатку стека TCP/IP, делать «невидимое» сканирование, сканирование с использованием ложных хостов, определять наличие пакетных фильтров, RPC-сканирование. Весь процесс отражается в окне в виде текста и цифр, почти без комментариев.
В результате получается список портов удаленной машины с указанием номера и состояния порта, типа используемого протокола, а также названия службы, закрепленной за этим портом. По Nmap'у порт может иметь три состояния: «открытый», «фильтруемый» и «нефильтруемый». Состояние «открыт» означает, что удаленная машина прослушивает данный порт. Состояние «фильтруемый» означает, что файерволл, пакетный фильтр или другое устройство блокирует доступ к этому порту и Nmap не смог определить его состояние. «Нефильтруемый» означает, что по результатам сканирования Nmap воспринял данный порт как закрытый, при этом средства защиты не помешали Nmap определить его состояние. Это состояние Nmap определяет в любом случае (даже если большинство сканируемых портов хоста фильтруются).

N-STEALTH

Сканер-убийца. Убийца во всех смыслах. Работает очень медленно... Но эффективно. А медленно, наверное, из-за гигантского количества проверок - более 19000! Все это происходит в одном немасштабируемом окне, причем все элементы интерфейса: и опции, и статистика, и все остальное - появляются на одной и той же форме. Сначала от этого путаешься, потом привыкаешь.
Когда я увидел большущую кнопку Language, сразу же радостно выбрал в списке русский язык, и понял, что радовался рано. Вместо знакомых слов я

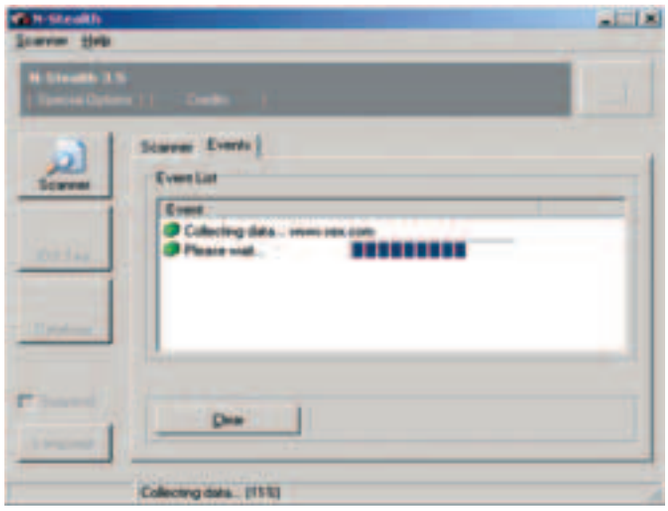


Рис. 6. Сканер-монстр N-Stealth.

увидел кракозябры транслита. Получилось очень необычно и неудобно, и я переключился назад на english.
Продолжая изучение опций, я нашел в N-Stealth целый набор инструментов для уклонения от IDS, но он посоветовал их вырубить, чтобы процесс шел быстрее. Ну, и конечно, как не быть средству для добавления своих проверок - ExploitDev. Средство это очень простое и идет с примерами.
Когда во время проверки оборвалась связь, всплыла еще одна нехорошая подробность - у проги нет паузы. Пришлось начинать сначала и ждать, ждать, ждать...
N-Stealth комплектуется еще и анализатором логов сервера, сканером вебконтента сервера, средством для автообновления и средством для автоматического намыливания результатов. Называется все это N-Stalker Security Intelligence Service и стоит денежков. Вот так.

TYPHON II

Еще один «самый мощный и быстрый» сканер, который раньше звался Cerberus Internet Scanner. На самом деле, Typhon очень простой: буквально старт, стоп и опции.
Начав сканировать, ты увидишь только два слова: сначала Running, и, когда прога кончит, Completed и все! Даже как-то скучно смотреть - ни тебе прогрессбара, ни текущего статуса. Как будто создатели поставили себе задачу как можно меньше взаимодействовать с пользователем. Несмотря на внешнюю простоту, в опциях довольно неплохой выбор сервисов. Хорошо умеет сканить реестр, если, конечно, доберется до него.

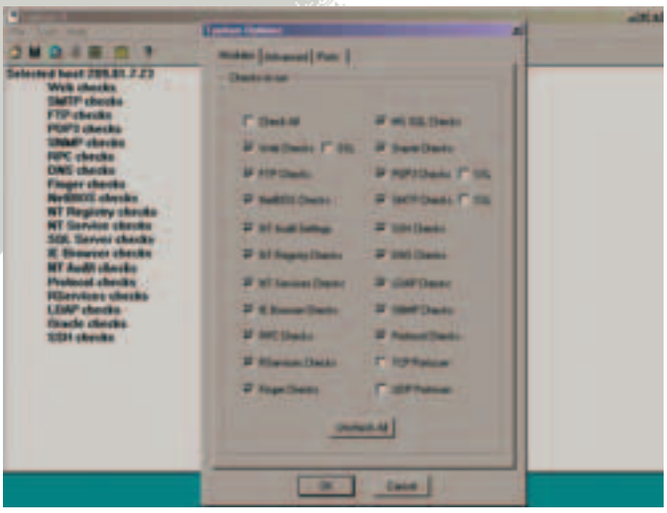


Рис. 7. Typhon - невидимый ураган.

Также Typhon можно использовать как wardialer, то есть звоним по определенным телефонным номерам и узнаем, есть ли на другом конце линии модем.

ТЯНЕМ - ПОТЯНЕМ, ВЫТЯНУТЬ...

Теперь, когда я накачал себе сканеров, осталось выяснить, пригодны ли они для вытягивания репки, или нет. В качестве репки были выбраны сайты www.sex.com и www.mail.ru (только т-с-с, они еще об этом не знают :)). Проверялись оба сайта всеми сканерами по два раза, время бралось наименьшее, интерфейс и отчет оценивались по пятибалльной системе. Вот что получилось.

Параметр / Сканер	Интерфейс	Отчет	Доп. функции	Размер	Бесплатный
Xspider 6.10	4.5	5	есть	1.08 MB	да
Shadow Security Scanner 5.35	4.5	4.5	нет	3.59 MB	нет
LANGuard 3.0 (beta 3b)	3.5	5	есть	4.35 MB	нет
X-Scan 1.3 GUI	2	1.5	нет	1.57 MB	да
Nmap 1.3.0	3	3.5	нет	6.10 MB	да
N-Stealth 3.5 build 55	3	4	нет	1.08 MB	да
Typhon II	2	4	есть	4.06 MB	нет

Рис. 8. Сравнительные характеристики сканеров.

Репка вытащена успешно. (Чтобы изменения вступили в силу, нужно перезагрузить компьютер:)).

Судя по общим результатам, на sex.com было 4 открытых порта и (предположительно) одна опасная дыра - в OpenSSH - возможность получения привилегий root, а на mail.ru - 3 порта и возможность неавторизованной отправки почты. Замечаниями считаются возможность получения информации с сервера и уязвимости с низким уровнем опасности.

Параметр / Сканер	Найдено открытых портов	Найдено дыр/замечаний	Затраченное время
XSpider 6.10	4	2 / 7	38 мин 41 сек
Shadow Security Scanner 5.35	4	1 / 6	18 мин 25 сек
LANGuard 3.0 (beta 3b)	4	1 / 2	28 мин 04 сек
X-Scan 1.3 GUI	3	1 / 1	3 мин 34 сек
Nmap 1.3.0	4	-	9 мин 34 сек
N-Stealth 3.5 build 55	4	1 / 6	72 мин 38 сек
Typhon II	4	1 / 2	5 мин 02 сек

Рис. 9. Жертва №1 - www.sex.com.

Как я и ожидал, XSpider показал себя вполне достойно. Хоть и не спеша, он все же обнаружил все что надо, и даже больше. Паук выдал целых два предположения об уязвимости на sex.com. Среди замечаний можно отметить найденные доступные директории на обоих сайтах.

Shadow Security Scanner также справился с задачей, но быстрее и нашел больше существенных замечаний, касающихся настроек сервера на sex.com.

С sex.com LANGuard справился почти за полчаса, причем сразу явно определил ОС (FreeBSD). А вот mail.ru сканировать отказывается, не может найти ни одного компа в сети! Я и таймауты увеличивал, и загружал файл настройки для медленной сети - как рыбой об лед. Посему эту половину теста предлагаю считать им не пройденной.

Параметр / Сканер	Найдено открытых портов	Найдено дыр/замечаний	Затраченное время
XSpider 6.10	3	0 / 5	13 мин 20 сек
Shadow Security Scanner 5.35	3	0 / 1	8 мин 10 сек
LANGuard 3.0 (beta 3b)	-	-	-
X-Scan 1.3 GUI	3	1 / 1	4 мин 12 сек
Nmap 1.3.0	3	-	4 мин 26 сек
N-Stealth 3.5 build 55	3	0 / 3	57 мин 45 сек
Typhon II	3	0 / 1	3 мин 48 сек

Рис. 10. Жертва №2 - www.mail.ru.

X-Scan нашел дырки быстрее всех и выдал свой ужасный отчет. Только вместо дырки в OpenSSH он нашел какую-то дырку в HTTP. Комментариев на сайте нет... Загадочный народ китайцы.

NMap, как сканер портов, свое дело сделал на 5 с плюсом - относительно быстро и информативно. Показал открытые, закрытые и защищенные порты и кучу дополнительной инфы. Отчего он столько весит, пока остается загадкой (от кривого портирования под винды, никсовая версия весит нормально – прим. ред.).

N-Stealth, основательно помучив оба сайта, нашел обе дырки. Если бы была конкретная цель, можно было бы существенно уменьшить время сканирования, убрав ненужные проверки.

Typhon также с проверками справился, причем гораздо быстрее некоторых. Оно и понятно: при таких размерах и таком интерфейсе остается надеяться на качество.

...ВЫТЯНУЛИ РЕПКУ!

В общем, все сканеры чем-то хороши, и мне остается дать пару заключительных советов. Если время тебе пофигу, можно «маскироваться», использовать прокси и включать сканирование UDP. Было бы неплохо почаще обновлять базу данных уязвимостей.

Сканеры работают по-разному и дают различные результаты, поэтому самое главное - это выбрать, какой именно тебе подойдет. Такие сканеры, как XSpider, Shadow Security Scanner, N-Stealth и Typhon будут полезны как для админов, так и для желающих взломать какой-нибудь сервак. Nmap - прога для тех, кто умеет работать с сетью ручками и читать сложные логи. LANGuard скорее подойдет для сканирования локалки, а X-scan - для тех, кто спешит, и кого не интересуют подробности.

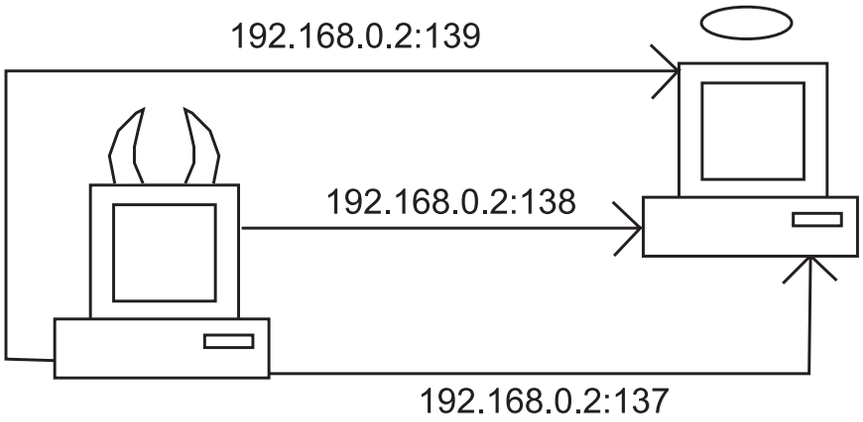
А для энтузиастов сойдет любая прога :). Им и флаг в руки.

КРАТКИЙ ПУТЕВОДИТЕЛЬ ПО СКАНИРОВАНИЮ

наводим справки

Для тех, кто не любит или не умеет читать, или все прочитал, но мало понял, публикуем картинки! Из этих картинок тебе наконец-то должно стать понятно то, что мы пытаемся объяснить тебе в этом номере. На самом деле сканирование бывает четырех основных типов. Все остальное - вариации. Разбирайся, это просто! Все получится :).

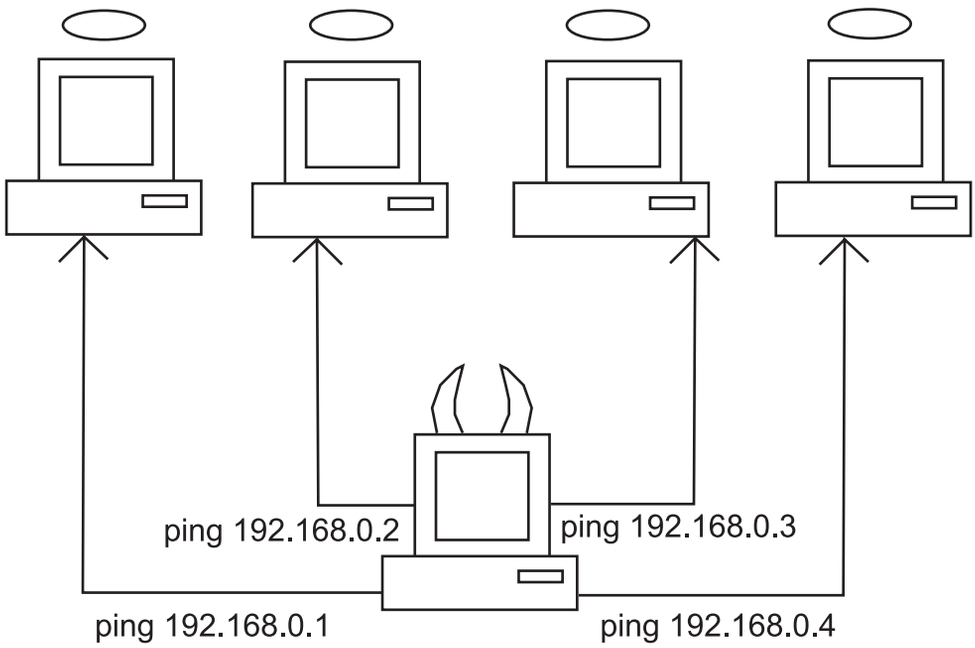
Злой Невыспавшийся Сканер



Сканирование портов

СКАНИРОВАНИЕ ПОРТОВ

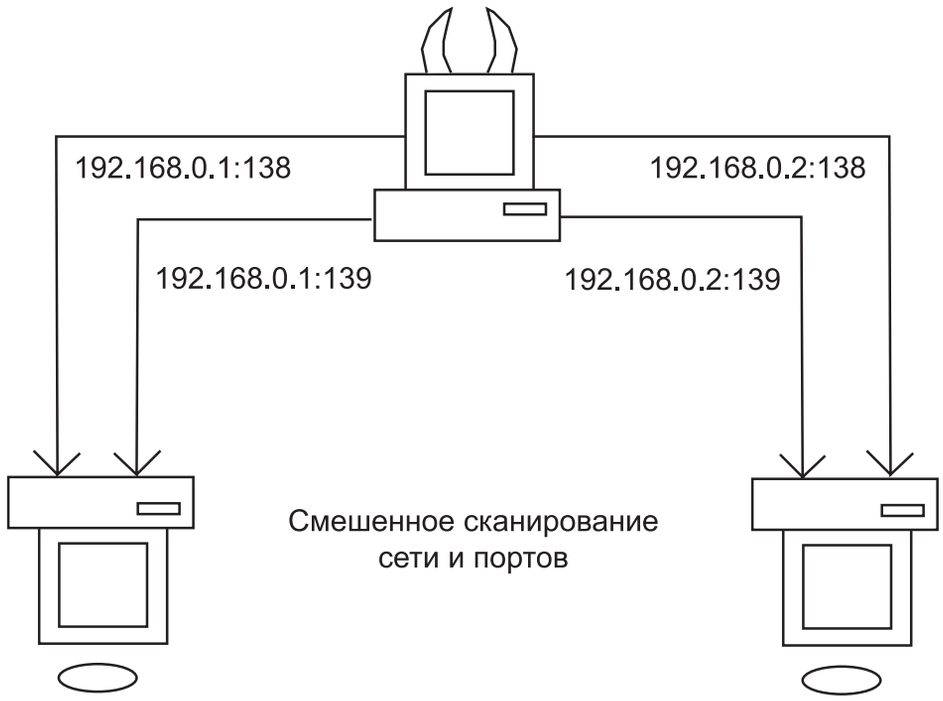
А здесь зло пробует установить сеансы связи с добром по определенным портам. Задача зла определить какие порты открыты, поэтому зло по очереди пробует все порты. Если порты не отвечают, значит, они закрыты. Для того чтобы проверить порты зло использует сканер портов. Этот вид сканирования используется, когда жертва уже найдена!



Сканирование сети

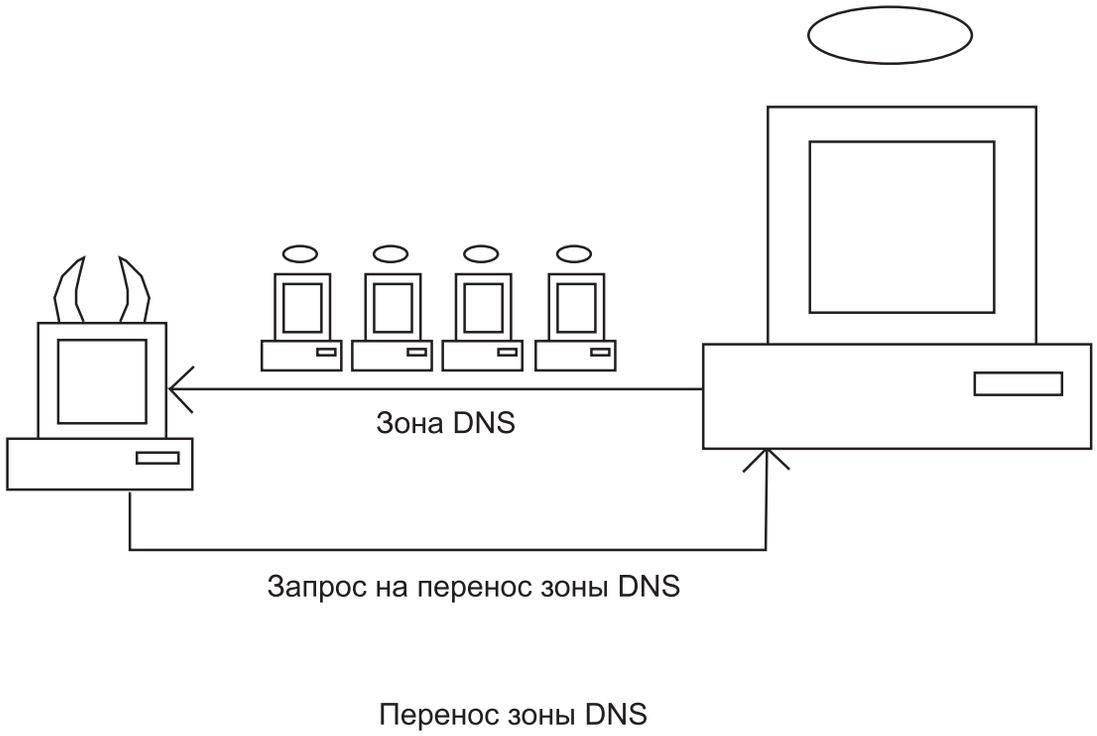
СКАНИРОВАНИЕ СЕТИ

Тут зло перебирает все возможные айпишники выделенного диапазона добра. Задача зла - выяснить какие из компутеров добра доступны, а какие нет. Поэтому зло пингует все машины из заданного диапазона. Те машины, которые не пингуются - не работают или им запретил Большой Админ отвечать на пинги. Этот способ применяется, когда зло хочет просканить конкретную сеть добра.



СМЕШАННОЕ СКАНИРОВАНИЕ ПОРТОВ И СЕТИ

Наконец, когда зло решается совместить приятное с полезным, оно вспоминает, что можно сканить в сети определенные порты. То есть зло ищет компутеры добра с дырками на определенных портах. Обычно такое сканирование используется когда есть известная дырка и ее хочется найти в заданном диапазоне адресов.



ПЕРЕНОС ЗОНЫ DNS

Ленивое зло ломает утомительное сканирование и исследование сети, поэтому оно претворяется DNS-сервером с помощью утилиты nslookup и запрашивает у незащищенного сервера добра базу данных DNS. Если в этой базе данных есть вся информация о локальной сети, то сканировать ее уже не придется.

СТАНДАРТНЫЕ ПОРТЫ

список стандартных портов с описанием сервисов

Сканер портов – это, конечно, большой рулез. Но, взяв его в зубы и накинувшись на безобидный хост, ничего особого не добьешься. Ну, выдаст он тебе что-нибудь в стиле:

22/listening
25/listening
79/listening
80/listening
111/listening
117/listening

uUcp (uucp@xakep.ru)

И что? Многим это вообще ни о чем не говорит. Кто-то поймет, что на сервере открыты порты 22, 25, 79, 80, 111 и 117. Но кто его помнит, что за этими портами скрывается? Ладно, допустим, 80-ый порт знают все – web-сервер, а что стоит за, скажем, 117-ым? Ты помнишь? Я – нет. Так что давай посмотрим, как надо разруливаться в таких ситуациях. Есть два варианта: либо пользоваться сканерами, которые хоть как-то показывают, какой сервис висит на открытом порту (такими, как nmap – да и тот выдает о сервисе не очень много информации, только название), либо самому научиться определять по номеру любого порта сервис, который на нем висит. Мы пойдем вторым путем, так как он универсален и не привязывает тебя к каким-либо конкретным сканерам, платформам, ОС'ям архитектурам процессора и прочим ограничителям свободы и воли :).

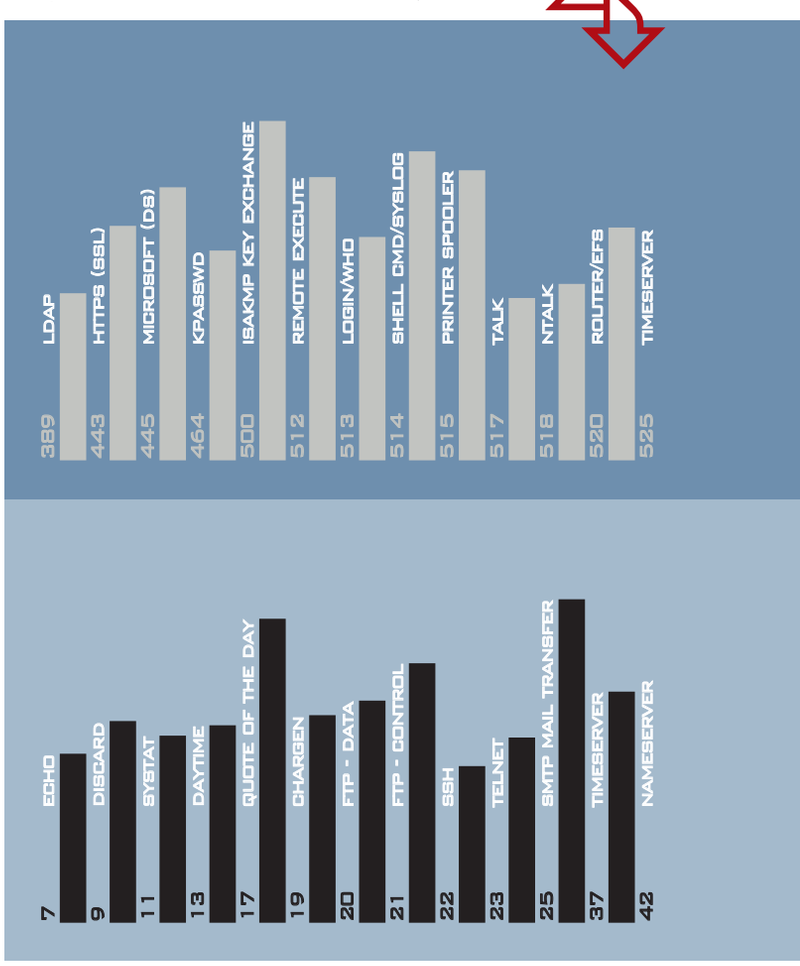
ЧТО ЕСТЬ ЧТО?

Начнем с самого тривиального – что есть порт? Все знают, что у каждой машины в сети есть свой IP-адрес, и для того чтобы приконнектиться к ней и воспользоваться каким-нибудь сервисом (если машина его предоставляет, т.е. является сервером), надо знать этот самый айпишник. Но что делать, если машина предоставляет сразу несколько сервисов: вэб, почта, телнет? Вэб браузер будет коннектиться по этому IP точно так же, как и почтовый клиент, а ведь каждому из этих приложений надо предоставлять отдельный сервис. Как их разделить? Чтоб не возникало таких проблем, используются порты. Браузер коннектиться к серверу по его IP'шнику, но уточняет, что ему нужен такой-то порт (тот, на котором предоставляется вэб-сервис – 80), и почтовый клиент коннектится к тому же IP, но уточняя, что ему нужен другой порт (вернее порты: POP3/SMTP – 25/110, один для приема почты, второй для отправки – для приема и отправки почты используются разные сервисы). Вот и получается, что порты – это, как бы, адреса конкретных сервисов в пределах одного сервера (можно еще сказать в пределах одного IP). Ок, все отлично, но есть еще одна проблема: что будет, если каждый владелец сервера будет вешать свои сервисы на произвольных портах? Например, один повесит web-сервер на порт 40, а второй на 45 и тд. Будет неразбериха, потому что браузер не будет знать, к какому порту ему коннектиться на каждом новом сервере. Во избежание этих неприятностей и был создан список стандартных портов. В нем ясно сказано, что, например, web-сервис должен находиться на 80-м порту, телнет-сервис – на 23-м, DNS – на 53-м и тд. При таком раскладе браузер всегда знает, что ему нужен порт 80, точно так же telnet-клиент всегда коннектится на порт 23.

За списком стандартных портов следит организация под названием IANA (Internet Assigned Numbers Authority). Базируется эта контора по следующему адресу: http://www.iana.com/. В ее полномочья входит, собственно, редактирование и поддержание списка стандартных портов в надлежащем состоянии. Не завидую я этим ребятам - работа у них, блин, гиморная. Прикинь, каждый разработчик, решивший, что его сетевое приложение (или протокол) должно занимать такой-то порт, должен отправить в IANA'у соответствующий запрос на регистрацию этого порта (все это можно сделать прямо с сайта). После того, как IANA рассмотрит запрос и даст добро, порт будет добавлен в список стандартных портов и будет официально закреплен за соответствующим приложением (чтоб клиентская и серверная часть этого приложения могли спокойно взаимодействовать на всех серверах через этот порт).

LET'S DO IT

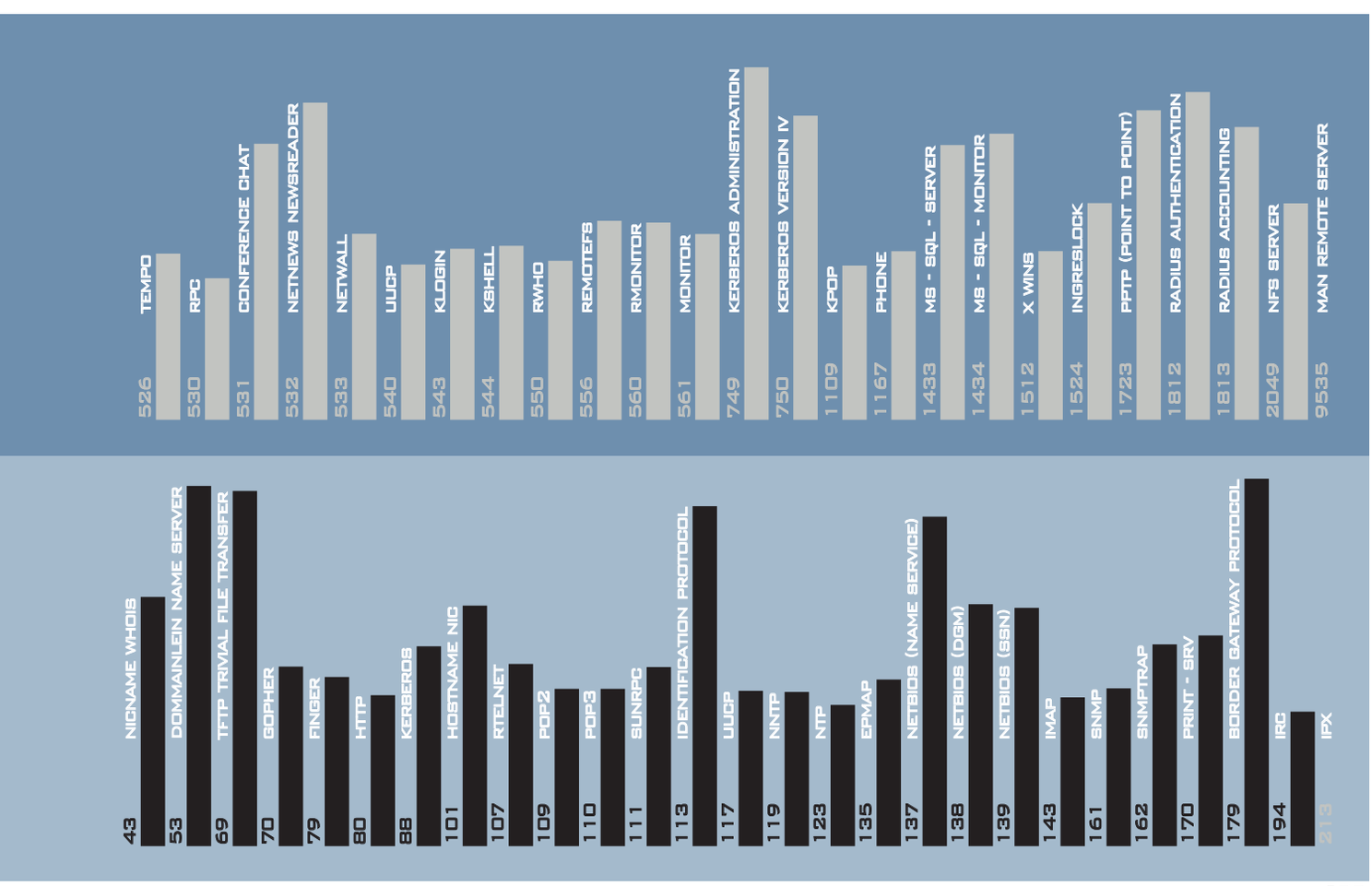
Итак, мы поняли, что такое порт и что такое список стандартных портов. Теперь вернемся к нашему любимому сканеру портов. Когда эта замечательная тулза выдает нам список открытых портов на каком-нибудь сервере, мы вооружившись списком стандартных портов, сверяем открытые порты со стандартными и смотрим, какие же сервисы все-таки предоставляет интересующий нас сервак. Вот теперь какртинка складывается полностью: посканил, посмотрел, какие порты открыты, глянул в список и определил, какие сервисы работают на серваке. Полный список стандартных портов доступен по адресу http://www.iana.org/assignments/port-numbers. Их там просто огромное количество, но большинство из них используются очень редко. Чтоб не гонять туда тебя каждый раз, я приведу прямо тут список наиболее часто встречающихся открытых портов. Короче – теперь просканив что-нибудь можешь открывать этот Спец и смотреть, что это ты там такого насканил ;). Поехали:



Вот такой вот небольшой списочек на заметку ;). Кстати, еще инфо для тебя: список стандартных портов от IANA рассортирован следующим образом. Сначала идут Well Known Port Numbers (хорошо изученные/отсортированные/известные порты). Это порты с номерами от 0 до 1023. Обычно эти порты отдаются пот сервисные службы: всякие демоны и прочее. Далее идут Registered Port Numbers (зарегистрированные порты). Это порты с номерами от 1024 и до 49151. На этих портах обычно висят клиентские проги (ведь серваку тоже надо знать, куда посылать ответ). И замыкают структуру Dynamic and/or Private Ports (динамичные и приватные порты). Это порты с номерами от 49152 до 65535.

ЗРИ В ОБА

А теперь о грустном: список стандартных портов от IANA – это всего лишь рекомендации админам и разработчикам. Понятно, что любой кодер может написать свою прогу так, чтоб она юзала какой угодно порт (хоть тысячу раз зарегистрированный). С тем же успехом любой админ может повесить любую прогу на своем серваке на любой порт :(. Правда, при этом у него возникнут проблемы с тем, куда девать законное «приложение» этого порта, но это так – раздражающее обстоятельство, а не реальная проблема. Если по Well Known портам все более менее стабильно (мало кто любит гемориться с переносом, скажем, вэб-сервера с 80-го порта на 151-ы), то с Registered портами все уже достаточно смутно (а о Dynamic и говорить нечего). Фишка в том, что когда , например, браузер обращается к веб-серверу, он должен знать точно, на каком порту постоянно тот висит, а когда наоборот – такого ограничения нет. Ведь браузер сообщает в запросе, номер своего порта, поэтому серверу не надо знать какого-то одного постоянного номера порта – обратился к нему браузер с порта 31270, он туда и ответил, обратился с 33109 – ответил на него. Так что будь внимателен и не пытайся заэксплоитить telnetd эксплоитом от ftpd :). Удачи!



ПЕРЕНОС ЗОНЫ DNS

Прежде чем куда-то что-то переносить, перетаскивать, кантовать и забрасывать давай присядем и постараемся ответить на вопрос: «ЗАЧЕМ?». Как ты уже понял, залог удачного хака - тщательная разведка. То есть хакер перед боем должен тщательно исследовать условного противника.

Рваный Нерв

Изучение таблиц DNS (Domain Name System) – один из эффективных способов выяснить топологию вражеской сети. И что же мы хотим увидеть в таблице? А в таблице мы хотим увидеть структуру вражеской сети. Дело в том, что современные админы активно используют DNS в своих локальных сетях. Если присвоить имена каждому компьютеру в локалке, то ее удобнее администрировать. При этом админы любят для максимального удобства написать в базе DNS, в какой комнате стоит компьютер, какая на нем операционная система, как зовут его хозяина.

ТАК ЧТО ЖЕ ТАКОЕ DNS?

Служба доменных имен нужна для того, чтобы превратить сложные для восприятия цифры IP-адреса в слова на человеческом языке. При этом таблицы соответствия адресов именам хранятся на специальном сервере. Когда пользователь обращается к компьютеру по имени, его система формирует серверу DNS-запрос с требуемым именем компьютера. В ответ на такой запрос DNS-сервер отправляет DNS-ответ, в котором указывает IP-адрес, по которому находится нужное имя. Это конечно неудобно, но в сети TCP/IP машины могут находить друг друга только по электронному адресу. Для того, чтобы можно было использовать удобные имена, нужен DNS-сервер, или другая похожая служба. Этим и пользуются хакеры в своих гнусных целях.

КАК ВЫГЛЯДИТ БАЗА DNS?

Обычно это небольшая текстовая табличка (это смотря какая сеть! не хотел бы я получить такую «небольшую» табличку себе на мыло :) – прим. ред.), которую серверы время от времени посылают друг другу, для того, чтобы быть в курсе изменений имен в сети. Каждому компьютеру или домену отводиться несколько строчек, давай мы в них поковыряемся!

Каждая строчка помечается в начале специальным маркером, вот примерный список этих маркеров, которые могут быть интересны хакеру.

A
С этого маркера начинается запись, в которой храниться IP адрес. Самое интересное, когда адрес начинается на 192.168.XXX.XXX., это означает, что хакер видит запись компьютера из локальной сети. Такие адреса в Интернет зарезервированы только для локальной сети и из глобальной сети не видны, поскольку их прикрывают злобные шлюзы. Изучение базы DNS позволяет хакеру узнать даже о таких скрытых компьютерах локальной сети, если администратор не прикрыл эту великолепную возможность.

HINFO
Важнейшая запись для хакера. В поле с этим маркером храниться информация об операционной системе, которая стоит на компьютере. Кроме того, из этого поля, если повезет, можно узнать даже аппаратную платформу удаленного компьютера.

CNAME
Эта запись позволяет узнать псевдоним и официальное имя чужой машины. Официальное имя может быть типа: moi_compuster.moi_lan.net. То есть это и есть доменное имя компьютера. Хотя в локальной сети можно не указывать хвост moi_lan.net, достаточно указать moi_compuster и DNS вернет тебе нужный айпишник.

MX
Mail eXchanger – почтовый шлюз, который помогает переадресовать почту и поставить IP-адрес в соответствие доменному имени. Помнишь, какие страшные адреса почты в FIDO? Или лучше вспомни, какие страшные номера у мобильных телефонов или у ICQ. Это все потому, что у них нет службы имен, которая позволяет вместо этих уродливых многозначных номеров поставить буквенные имена.

TXT
В этом поле хранится текстовое описание компьютера, или просто какие-то пометки, сделанные администратором. Тут можно найти информацию о хозяине компустера, его назначение, его расположение в помещениях офиса и другие полезные вещи.

Что же дает хакеру анализ базы DNS?

Если в офисе много машин, и админ использовал DNS для того, чтобы как-то расклассифицировать машины, то хакер может узнать всю топологию сети. То есть негоднику станет известно: сколько каких машин, с какой операционной системой в чем задействованы. Доменная система с анатомической точностью повторяет административное устройство организации. Если бы солдаты на военной базе использовали DNS, то эта база стала бы лакомым кусочком для настоящих шпионов. Попробуй зайти в папочку «сетевое окружение» на компьютере у себя на работе, или у себя в институте! Ты сразу заметишь, что структура имен повторяет административное устройство.
Если бы всем сотрудникам института вживили в башку сетевые адаптеры с поддержкой стека протоколов TCP/IP, то из министерства образования до студента можно было бы добраться по такому примерно имени: вася_гнойный.группа_ижо.институт_МИРЭА.учебные_заведения.

В текстовом файле с базой DNS хакер проводит автоматический поиск и выявляет интересные для него тачки. При этом особое внимание уделяется описанию машины. Вряд ли личный компьютер секретарши, повара или железячника-экспериментатора обладает мегазащитой. Такую машину хачить намного безопаснее и проще.

Ну а если разведчик завладел одной машиной, то можно ее использовать как опорную точку в завоевании всей сети!

Получается, что информация DNS – важный инструмент в сканировании вражеских сетей!

КАК ЖЕ ХАКЕР УКРАДЕТ ЗАВЕТНЫЙ ФАЙЛ С БАЗОЙ DNS?

А не нужно его красть. Многие сервера настроены так, что могут отправить по запросу свою базу другому серверу. Таким образом происходит обновление информации об именах на вторичных серверах. Обычно администратор прописывает имена на первичном сервере вручную, это главный сервер. Вторичные сервера подстраховывают первичный на случай перегрузки или отказа, для этого они выкачивают базу DNS с первичного сервера к себе. Хакеру остается претвориться вторичным сервером и тоже потребовать базу. Если DNS-настроен выдавать доменную информацию кому попало, он отвечает на запрос закачкой текстового файла.

УТИЛИТА nslookup

Эту утилиту можно найти и в стандартной установке Windows или Unix. Для этого в командной строке нужно набрать:

```
> nslookup
```

В ответ ты получишь имя DNS-сервера по умолчанию. После того, как того как ты запустил nslookup, то открылся диалоговый режим с этой софтиной. То есть программулина ждет твоих команд. Чтобы выйти из этого режима набери:

```
> exit
```

Чтобы разобраться в командах этой утилитки используй подсказку, для этого набери:

```
> nslookup help
```

Для того чтобы утилита выводила максимум полезной информации используй команду:

```
> set all
```

После этого программа будет очень подробно рассказывать тебе о каждом своем шаге, но не торопись, так как избыток информации может тебя запутать! Чтобы подключиться к чужому DNS, набери:

```
> server chujoy_dns.plohoy_domen.ru
```

После этого можно пролистать его чужую базу данных DNS, для этого используем команду LIST с ключиком «d», для того чтобы вывелось все записи базы:

```
> LS –d plohoydomen.ru.
```

Заметь, что нам не пришлось сканировать сеть plohoy_domen.ru, DNS сервер сам прислал всю важную инфу о ней, а мы сэкономили время на возне со сканерами! После того как ты введешь такую строчку nslookup выведет тебе базу DNS в текстовом формате. Как пользоваться ей ты уже знаешь. Однако, если администратор попался грамотный, то команда LS будет отнекиваться. Это значит, что злобный админ запретил своему днсу отсылать свою базу кому угодно. Придется искать другой DNS с менее просвещенным админом. Если тебе повезло, и на экран повалила нужная текстовая информация можешь сохранить ее в файле. Нужно перенаправить вывод с экрана в нужный файл, для этого используют стрелочку : «>>». Команда со стрелочкой перенаправления в файл будет выглядеть так:

```
> LS –d plohoydomen.ru. >> moy_file.txt
```

При этом на экране ты ничего не увидишь, за то после того как выйдешь из утилиты сможешь просмотреть файл с базой DNS в текстовом формате. К этому файлу удобно применять поиск текстового редактора. Хакеры пишут скрипты преобразующие этот файл для загрузки сканера портов. Негодник выясняет какие тачки в сети живы и заряжает этой инфой свой сканер, чтобы определить какие тачки имеют нужные дыры.

АДМИНИСТРАТОР СЛЕДИТ ЗА НАМИ!

Такой способ получения информации редко бывает обнаружен администратором или системой защиты. Однако такая возможность есть! Дело в том, что при переносе зоны DNS (при копировании базы), используется TCP соединение по 53-ему порту. А обычный DNS-запросы проходят по 53-ему UDP порту. Админ или программа безопасности могут обнаружить излишнюю активность по этому TCP порту и прикрыть всю халяву, вместе с портом!

РАСКЛАДКА ПРОТОКОЛА NETBIOS

NetBIOS по полочкам

Матушка Лень (Mlen@mail.ru)

ИСТОРИЯ ПЕРВАЯ (В ДУХЕ КИПЛИНГА)

Как NetBIOS стал Биосом

Когда-то давным-давно (1986 год) фирма IBM припаяла BIOS к своим сверхскоростным сетевым адаптерам Token-Ring. То есть микросхему с базовой системой ввода-вывода (Basic Input/Output System). Базовая система ввода-вывода (BIOS) стоит и на современных компах. Эта маленькая микросхема осуществляет тестирование и настройку большинства железок, а также запуск операционной системы. А как ты хотел? Ведь твой компьютер с выключенным питанием - это куча металлолома соединенного проводами. Каждый раз, когда компьютер включают, BIOS начинает искать жесткие диски, дисководы, видеокарты... Базовая система собирает все эти разрозненные железки в единый механизм. После того как сбор окончен, очень удобно обращаться к железкам через прерывания BIOS. То есть пара строк на ассемблере может высветить точку на экране монитора или записать байт на поверхность жесткого диска.

NetBIOS (Network BIOS) должен был делать все то же самое, только с сетью. Это было очень удобно и повысило производительность маркерного кольца (Token-Ring). Все дело в том, что сетевые программы смогли обращаться к сети через прерывания NetBIOS. То есть пара строк на ассемблере позволяли передать пакет с данными через сеть. Весь геморрой с протоколами взяла на себя микросхема, запаянная в сете-

вую карточку IBM, что позволило разгрузить и без того тормозной компьютер. Этот набор сетевых средств оказался очень удобным, его используют до сих пор для разработки простеньких сетевых программ, а называют BIOS API (Application Program Interface), то есть интерфейс прикладной программы с сетевыми службами. Или NetBEUI (NetBIOS Extended User Interface). В исконном NetBIOS, не был формализован транспортный и сетевой протокол. Поэтому API был не полным. Для того чтобы дополнить NetBIOS ввели протокол NetBEUI, который и служит транспортно-сетевым протоколом. А стек называется NetBIOS/NetBEUI.

Для справки, расскажу, что Token-Ring - это эстафетная сеть передачи данных по кольцу. Тот компьютер, у которого есть маркер имеет право передавать данные, после того, как он передал маркер другому компу - данные передает другой. Маркер - это служебный кусок информации, передаваемый по сети от машины к машине. На основе Token-Ring сделали такие технологии как Fast Ethernet и FDDI, которые используются в современных локальных сетях.

А теперь я открою тебе страшную тайну! Настоящий NetBIOS сгинул вместе с адаптерами 86-ого года! Все с чем мы имеем дело - это эмуляторы этой микросхемы. На первый взгляд это глупо, но протокол и прерывания этой микросхемы были настолько удобными, простыми и быстрыми, что оказалось выгодным ее эмулировать. Тем более что IBM открыла информацию о протоколах NetBIOS для всех бесплатно.

Рисунок 1
Формат пакета сервиса имен NetBIOS

ИСТОРИЯ ВТОРАЯ (ЭРОТИЧЕСКАЯ)

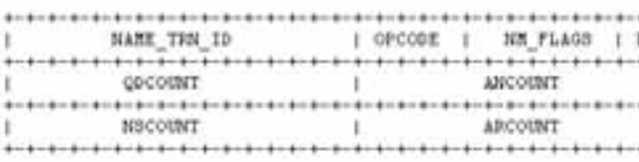
Про то, как NetBIOS оказался сверху

По началу NetBIOS заменял собой почти все. И многие вещи в нем были очень удобны, но главные недостатки скрывались в отсутствии маршрутизации и в широковещательных запросах. Поэтому теперь NetBIOS бегает поверх IPX (Internetwork Packet eXchange - обмен пакетами международной сети) в операционных системе фирмы Novell. Или поверх TCP/IP в сетях Microsoft. Юниксы как всегда ухитряются быть совместимыми и с теми и с этими.

Оба сетевых протокола умеют переносить на себе пакеты NetBIOS, это позволяет использовать его в таких больших сетях как Internet. С Novell с его IPX мы заморачиваться не будем потому, что редко хакеру приходится сталкиваться с Novell NetWare (такая сетевая операционная система). Будем разбираться в NetBIOS over TCP/IP, потому что именно в таком виде NetBIOS использует Unix и Windows, а с ними хакер здоровается за руку каждый день, особенно когда сканирует всякие шары! Хотя основные принципы NetBIOS over TCP/IP и NetBIOS over IPX сильно похожи!

Фишка TCP/IP такая: для службы имен NetBIOS использует 137-ой порт TCP/IP, для дэйтаграм использует 138-ой, а для сессий 139-й порт. О том, как все это происходит подробно написано в RFC 1001, RFC 1002. По сути, это единственные документы хоть как-то стандартизующие NetBIOS, и то там говориться про NetBIOS over TCP/IP (NBT сокращенно). Поскольку этот протокол так и не был стандартизован полностью, а информация по нему была открыта, поэтому практически каждая фирма придумала свою версию со своими надстройками, которые с другими клонами NetBIOS не работают. Вот и геморроются админы, чтобы заставить работать вместе Винды с Нетварью, Нетварь с Линухом, Линух с Виндами и так далее.

Рисунок 2
Формат заголовка пакета сервиса имен NetBIOS



NAME_TRN_ID	Идентификатор именной транзакции нужен, чтобы узнать, на какой из запросов пришел ответ.
OPCODE	Тип пакета бывает: (запрос/ответ) -запрос имени -регистрация имени -ожидание подтверждения -состояние станции -обновление
NM_FLAGS	Флаги
RCODE	Код результата запроса (ошибки)
QDCOUNT	Размер поля "Запрашиваемый ресурс"
ANCOUNT	Размер поля "Ответная запись ресурса"
NSCOUNT	Размер поля "Идентификационная запись ресурса"
ARCOUNT	Размер поля "Дополнительная запись ресурса"

ИСТОРИЯ ТРЕТЬЯ (ФилоСОФТская)

Про власть имен

NetBIOS - первый протокол с человеческим лицом, который позволил простым пользователям пользоваться удобными именами, а не замороченными компьютерными адресами. Уже за это его так полюбили разные канцелярские крысы. Протокол позволил дать компьютеру имя и дать имя группе компьютеров,

Рисунок 3
Формат пакета сессии NetBIOS

TYPE — Тип сессионного пакета:
-сессионное сообщение (пакет с данными пользователя)
-запрос на установление сессии
-положительный ответ на установление сессии
-отрицательный ответ на установление сессии
-переадресация сессии
-поддержание сессии
FLAGS — Флаги
LENGTH — Длина прицепа
TRAILER — Прицеп (Тут лежат специфические данные в зависимости от типа пакета)

обычное человеческое имя из шестнадцати символов. Это имя можно использовать как сетевой адрес компьютера. Когда ты в сети Windows видишь группу компьютеров «MyCrazyFriends», а в ней компьютеры: «Pasha», «Sasha», «Klusha» и «Andrusha», это и есть netбиосовские имена!

Но когда придумывали нетбиос в 84-ом году, никто и представить себе не мог, что сети будут такими огромными. Поэтому решили с именами все сделать дешево и сердито. Когда пользователь регистрирует новое имя в системе, NetBIOS отправляет широковещательный запрос (то есть запрос всем станциям) с новым именем. Если дублей нет, то в ответ ничего не приходит, а если такое имя уже есть, то приходит злобный ответ от хозяина.

Чтобы узнать, какая тачка висит под определенным именем, снова отправляется широковещательный запрос и так далее. Все это приводит к тому, что при большом количестве компьютеров сеть перегружается широковещательными запросами. Специалистам приходится с этим бороться.

Цель широковещательных запросов - узнать IP или MAC адрес тачки с нужным нетбиосовским именем. Microsoft для решения этой проблемы предлагает WINS (Windows Internet Name Service - виндовая интернет служба имен) - сервер на котором хранится список нетбиосовских имен. Вместо того чтобы спамить сеть широковещательными запросами, станция может обратиться к серверу за нужным IP адресом.

Для того чтобы уменьшить количество таких вредных запросов на самой станции может создаваться специальный файл с записями соответствия известных нетбиосовских имен и IP адресов.

И наконец, можно использовать обыкновенный интернетовский DNS (Domain Name System), как сервер имен NetBIOS. Правда в этом случае пользователь уже не сможет так вольно распоряжаться именами. Это не очень удобно.

Все запросы, и ответы на них у NetBIOS реализованы в пакете сервиса имен. Этот пакет имеет очень много разных модификаций, в зависимости от его назначения: широковещательный запрос, запрос о регистрации имени, запрос для WINS или DNS, или проверка имени на существование. В этой статье хватило места только для того, чтобы дать общий формат пакета и заголовок, подробнее читай в RFC 1002.

Кстати, для отправки и получения пакетов именного сервиса используется 137 порт TCP/IP.

Как я уже говорило, удобство именного сервиса NetBIOS в том, что ты можешь назначать имена для станций размером в 16 байт (16 символов). Кроме имени станции есть имя группы, то есть можно послать нетбиосовое сообщение сразу нескольким компьютерам с одним именем группы. Эти имена пользователь может менять по своему усмотрению, главное чтобы они не конфликтовали между собой, то есть не должно быть дублей!

Кроме этих имен возможно обращение по постоянному (permanent) имени, которое складывается из нулей и MAC-адреса сетевого адаптера. MAC (Media Access Control) - контроль доступа к среде, это физический адрес адаптера, прошитый в него намертво производителем.

Рисунок 4
Формат заголовка дейтаграммы NetBIOS

MSG_TYPE — Тип дейтаграммы бывает:
-персональная дейтаграмма
-групповая дейтаграмма
-широковещательная дейтаграмма
-ошибка дейтаграммы
-проверка работы дейтаграмм
-дейтаграммы пашут
-дейтаграммы не фурычат
FLAGS — Флаги
DGM_ID — Номер дейтаграммы, чтобы можно было разобраться, если на дейтаграмму придет ответ.
SOURCE_IP — Адрес отправителя
SOURCE_PORT — Порт отправителя
DGM_LENGTH — Длина дейтаграммы
PACKET_OFFSET — Смещение

Хакеру, который любит сканировать и изучать чужие локальные сети, полезно представлять работу службы имен NetBIOS. Такой хакер умеет узнавать по IP имя NetBIOS и наоборот. Имена машин в корпоративной сети могут здорово подсказать хакеру способы взлома. И потом, если хакер получил доступ к протоколу NetBIOS, это значит, что скоро он подберет пароль и получит доступ к диску удаленной тачки.

ИСТОРИЯ ЧЕТВЕРТАЯ (СТУДЕНЧЕСКАЯ)

О сессии NetBIOS

NetBIOS - это протокол с установлением соединения (сессии). Это нужно для того, чтобы можно было восстанавливать потерявшиеся в процессе передачи данные. Вообще-то TCP тоже протокол с установлением соединения, и он тоже умеет восстанавливать данные, которые не дошли (то есть запрашивать их заново). Но поскольку в NetBIOS все так исторически сложилось, будем разбираться с сессиями.

Прежде чем передавать данные две станции должны установить соединение. Для этого они обмениваются пакетами. Первым делом вызывающая станция должна по нетбиосовскому имени определить IP или MAC адрес другой станции, для этого она использует пакеты сервиса имен. Эти же пакеты используются для того, чтобы выяснить состояние вызываемой станции, вдруг она отключена.

Когда вызывающая станция определилась с именами и адресами, она отправляет запрос на установление соединения. На этот запрос приходит подтверждение установления соединения, отказ или переадресация. При отказе обязательно передается причина (код ошибки), а при переадресации новый адрес. После того, как соединение установлено, в сессионных пакетах высылаются пользовательские данные, а в ответ приходят подтверждения. В RFC 1002 про подтверждения ничего не сказано, может быть, их решили оттуда удалить за ненадобностью, либо они закопаны куда-то очень глубоко.

Но в первозданном NetBIOS механизм квитирования есть и работает! Квитирование - подтверждение полученной информации специальными ответными пакетами (квитанциями).

На рисунках ты можешь поглядеть общий формат кадра сессий NetBIOS, чтобы узнать подробнее - читай доки. В случае NetBIOS over TCP/IP сессии устанавливаются через 139-й порт TCP/IP.

Через этот же порт работает излюбленный хакерами WinNuke, эта злобная программа передает в порт срочную служебную информацию (Out Of Band) TCP/IP. NetBIOS путается и виснет. Хотя это, скорее всего, не единственный спо-

соб завалить NetBIOS, ведь даже в спецификациях нетбиоса указаны буферы критичные к переполнению. С незапамятных времен известны случаи зависания нетбиосового драйвера, который валит за собой всю систему. С выхода Windows 3.11 прошло столько лет, а нюк все еще работает даже на самых современных версиях виндов в той или иной модификации. Поэтому надежнее закрыть вообще все порты NetBIOS смотрящие в глобальную сеть.
Правда, некоторые фирмы не могут это сделать, поскольку используют NetBIOS и интернет для объединения офисов в разных концах страны в единую корпоративную сеть через интернет.

ИСТОРИЯ ПЯТАЯ (ПАТРИОТИЧЕСКАЯ)

В один конец

NetBIOS - очень продвинутый протокол. У него даже есть тип сообщений, которые не требуют подтверждения. Такие сообщения часто используются для того, чтобы быстро передавать какую-нибудь не очень критичную к потере информацию. Сообщения, не требующие подтверждения, называются дейтаграммами. Зачем же они нужны? Допустим, ты отправляешь широковещательный запрос, который получат все станции, и если каждая начнет высылать тебе подтверждение, то сеть перегрузится.
Запросы в NetBIOS бывают трех видов. Direct Unique - это персональный запрос только к одной станции. Broadcast - широковещательный запрос ко всем станциям. Direct Group - запрос к станциям с одним групповым именем. Дейтаграммы работают по 138-му порту.
Дейтаграммы применяются, когда мы не боимся потерять часть информации, но когда для нас критичны задержки и размер отправляемого пакета. Не нужно забывать, что все навороты типа установления соединения увеличивают задержки и размер передаваемой инфы. Поэтому реальное видео и аудио через интернет передается дейтаграммами. Если ты потеряешь пару кадров или пару звуков - это не критично. Но если изображение или звук будут заедать - это не годится. Получается, что NetBIOS способен передавать изображение и звук в небольших сетях, по нему даже можно устраивать мультимедиа конференции.
Перед посылкой дейтаграмм NetBIOS позволяет проверить способности источника принимать этот вид пакетов. Для этого источнику отсылается пробная дейтаграмма в ответ должно прейти либо сообщение об ошибке, либо подтверждение нормальной работы дейтаграммного сервиса.

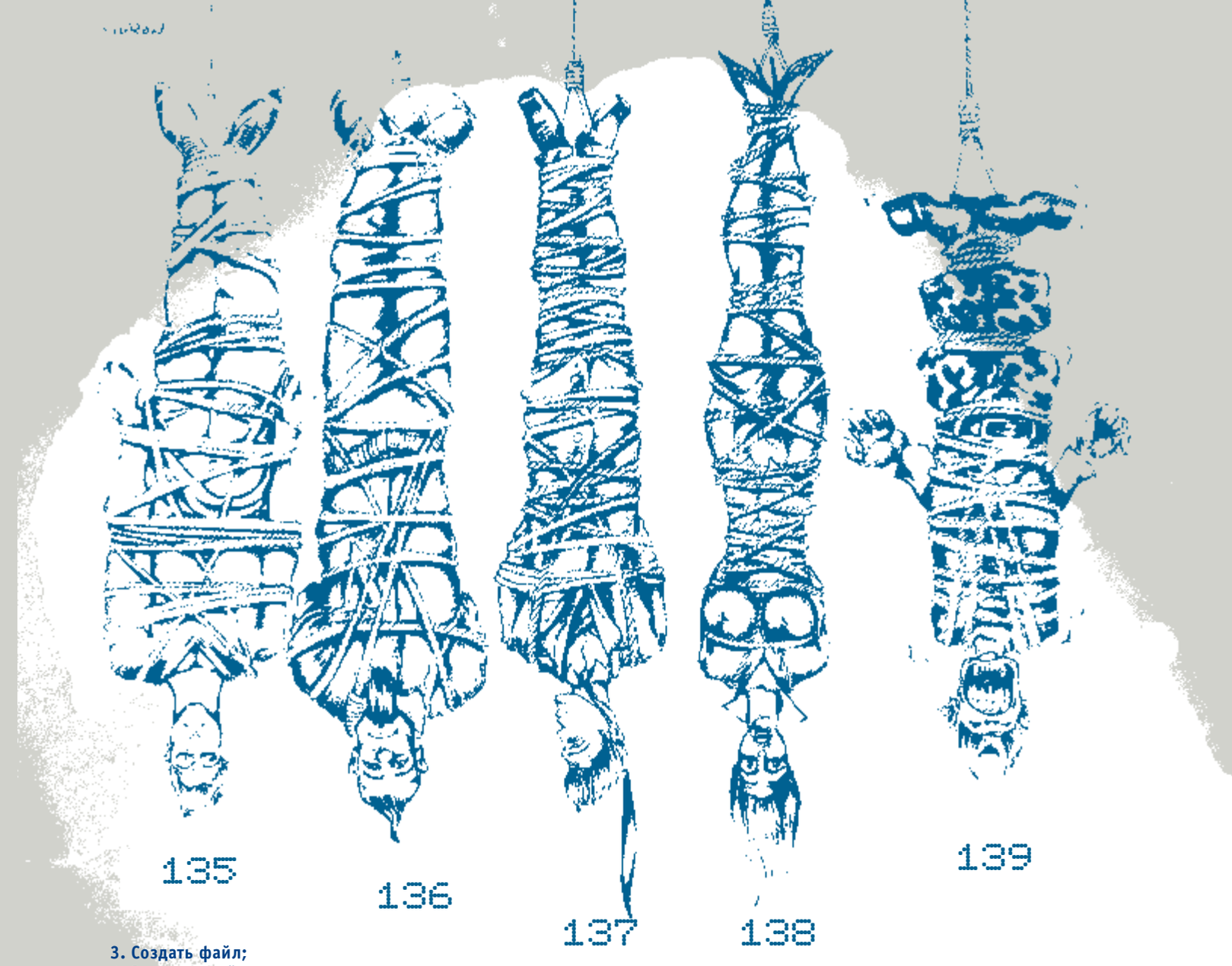
ИСТОРИЯ ШЕСТАЯ (ХАКЕРСКАЯ)

Не было печали, купила баба SMB

Казалось бы, зачем нужен этот старый полудохлый NetBIOS? Что все к нему так прицепились и не дают спокойно умереть? А все дело в том, что протокол SMB (Server Message Block) долгое время работал ТОЛЬКО через NetBIOS. Конечно, сказались простота и удобство имен, но главное это поддержка SMB! Этот протокол позволяет организовать доступ к спецпроцессору. А этот спецпроцессор умеет работать с файлами, принтерами и другими ресурсами Windows. Вшитый в систему троян, одним словом.
Как раз в честь этого протокола назвали юниксовую софтину САМБОЙ (SAMBA). Она умеет работать со станциями под управлением Windows или NetWare и использует протоколы SMB, NetBIOS, IPX. Так, что хакеры, которые любят хачить винды через юникс могут не расстраиваться. Конечно, с настройками Самбы придется покопаться, за то в результате компьютерный безобразник сможет подключать к себе чужие винты.

SMB/NetBIOS позволяет творить с удаленной машиной практически все. Вот примерный список его возможных команд:

1. Создать каталог;
2. Открыть файл;



3. Создать файл;
4. Закрыть файл;
5. Выполнить все файлы;
6. Стереть файл;
7. Переименовать файл;
8. Получить атрибут файла;
9. Установить атрибут файла;
10. Создать уникальный файл;
11. Создать новый файл;
12. Проверить каталог;
13. Конец процесса;
14. Начать соединение;
15. Закончить соединение;
16. Получить атрибуты диска;
17. Поиск нескольких файлов;
18. Возвратить очередь печати;
19. Послать сообщение;
20. Послать широковещательное сообщение;
21. Ретранслировать имя пользователя;
22. Отменить ретрансляцию;
23. Получить имя машины.

То есть SMB - это простейший механизм удаленной работы с дисками и периферией станции, подключенной к локальной или глобальной сети. Он очень просто настраивается, и поэтому его так любят пользователи. Пытаться добиться чего-то подобного через TCP/IP страшный гимор, поскольку этот протокол специально создавался так, чтобы что-то хакнуть было невозможно.
Надо ли говорить, что пароли к общедоступным дискам подобрать не проблема, они вряд ли сложнее чем «мама» или «маша». Поэтому, если хакер насконировал открытые порты NetBIOS, значит доступен и SMB. А если доступен SMB, значит хакер может подключить к себе чужой диск как сетевой, а еще сможет воровать оттуда информацию, менять ее, стирать ее, да все что в голову придет. Тут WinNuke покажется детскими шалостями. При чем если на твоей обычной домашней машине установлен NetBIOS и открыты его порты - это огромный проход для хакеров в твою систему.

ИСТОРИЯ СЕДЬМАЯ (ПОУЧИТЕЛЬНАЯ)

Да надоел он всем, пристрелили его!

Как бы мы не любили с тобой NetBIOS за все его хакерские и пользовательские возможности, надо признать, что это жуткое глючное старье. Даже Microsoft изо всех сил старается от него избавиться. Этот протокол просто не предназначен для работы в глобальных сетях или в больших локальных сетях. Он не проходит через маршрутизаторы (не маршрутизируется), он устраивает широковещательные штормы, он обеспечивает очень низкую безопасность, у него много несовместимых версий (потому, что он толком не стандартизован). Одним словом давно пора его менять на что-нибудь более прогрессивное.
Очевидно, что очень скоро эту рухлядь отключат везде. Поэтому хакерам осталось наслаждаться гигантскими дырищами нетбиоса совсем не долго!

NMAP

установка/настройка/разбор

Даже не знаю, что можно написать во вступлении к этой статье. Скорее всего, ничего писать и не надо - и так всем понятно, что nmap - самая большая рыба в водоеме сканирования удаленных сетей и машин. Это самый мощный на сегодняшний день сканер! Кроме того, он постоянно поддерживается и совершенствуется. Разработчик (некто Fyodor) не просто написал тулзу и выкинул ее в народ, а очень тщательно следит за проектом, все время выкладывая новые версии. Прога настолько качественная, что многие дистрибутивщики включили ее в поставки своих линей. Не имея под рукой nmap а, лучше вообще никуда не соваться.

aDm

КАЧАЕМ И СТАВИМ

Совсем недавно была зарелизена новая версия nmap - 3.00. Именно ее я и предлагаю скачать и установить. В комплекте твоего Linux'а, скорее всего, окажется пакет с nmap'ом, но лучше качнуть последнюю версию, так как у нее, наверняка, обновлена база OS fingerprints, что позволит тебе при сканировании идентифицировать самые свежие ОСи, например, Windows XP или Mac OS X.

Сайт проекта находится по адресу http://insecure.org/, а качнуть последнюю версию сканера можно по этой ссылке: http://download.insecure.org/nmap/dist/nmap-3.00.tgz. После

http://insecure.org/

того, как tgz'шник сольется на винт, его надо распаковать командой

```
gzip -cd nmap-3.00.tgz | tar xvf -
```

Либо можно его просто открыть в mc и скопировать в каку-нибудь папку. Прога распространяется в виде исходников, поэтому после распаковки ее необходимо скомпилировать. Переходим в папку с свежераспакованными сорцами:

```
cd ./nmap-3.00
```

Далее производим стандартную никсовую процедуру сборки/установки:

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

Последнюю команду нужно выполнить с правами root'а, но, думаю, у тебя с этим проблем не должно возникнуть, так как все порядочные хацкеры на своих домашних машинах всегда сидят под рутом :) (по этому поводу можно очень долго спорить, но мое личное мнение сложилось окончательно уже очень давно - если ты работаешь не за каким-нибудь серваком, то под рутом можно и нужно сидеть, и ничего опасного/плохого в этом нет). После выполнения последней команды, nmap установится в директорию бинарников, и его можно будет запустить из любого места, просто набрав в командной строке «nmap».

ЮЗАЕМ

Если вызвать nmap без параметров (просто вбацать в командной строке «nmap» и нажать Enter), сканер просто выведет на экран свой Help Screen - укороченный вариант справки с описанием возможных ключей и параметров. Чтоб сканер начал работать, ему надо передать хотя бы один параметр - ip-адрес, который надо просканировать. Давай для начала отсканим самих себя:

```
nmap 127.0.0.1
```

Вот что выдает прога (скрин 1). В первой строке прога пишет информацию о себе и дает ссылку н свою домашнюю страничку. Если это тебя очень сильно раздражает, можешь найти в исходниках эту строчку, удалить ее на фиг (или закомментировать) и повторить еше раз процедуру сборки/установки - больше ты этой строки никогда не увидешь. Чувствуешь преимущества Open Source софта ;)? Кто бы тебе в винде позволил поступить таким хамским образом? Ладно, поехали дальше: во второй строке nmap лишний раз заботливо поясняет, какой хост/ip'шник был только что посканен, а в третьей - выводит количество просканеных по этому адресу, но закрытых портов - авось пригодится. А дальше начинается самое интересное - перечисление открытых портов. Как видишь, на моей машине их не так много: ssh, smtp, сервис Sun Remote Procedure Call и X Window System. В последней строке сканер сообщает, сколько ip'шников было просканено и сколько на это ушло време-

скрин 1

ни. Это был самый простой пример - перейдем к более сложным. Чтоб узнать, чего еще умеет nmap, запусти его без параметров и посмотри на пресловутый Help Screen:

```
nmap
```

В первую очередь сканер сообщает, каким образом можно передавать ему параметры (скрин 2). Перевожу:

```
nmap [Тип/типы сканирования] [Опции] <хост/хосты>
```

nmap'овский Help Screen

В юникс принято обозначать параметры запуска следующим образом: все что в квадратных скобках - это необязательные (опциональные) поля, в угловых - переменные. Чем они отличаются? В переменных полях ты сам решаешь, что туда вставлять - в данном случае ты выбираешь хост/хосты для сканирования. А в опциях, например, ты можешь либо что-нибудь вставлять, либо нет, но если будешь вставлять, то только заранее определенные значения. Какие же это значение для nmap? А вот они, в том же Help Scree, только чуть ниже. Типы сканирования могут быть следующими:

-sS: TCP SYN сканирование
-sT: TCP-сканирование соединением
-sF: TCP FIN сканирование
-sX: TCP Xmas сканирование
-sN: TCP Null сканирование
-sR: TCP RPC сканирование
-I: Ident-сканирование
-sU: UDP-сканирование
-sP: Ping-сканирование

Обо всех этих типах сканирования, кроме последнего, ты можешь узнать подробнее из соответствующей статьи в этом же номере :). А о последнем не узнаешь, так как это не сканирование портов - это сканирование сети (либо просто сразу нескольких компов) на работающие тачки. Грубо говоря, обычный пинг - скармливаем nmap'у ip'шники какой-нибудь сети, и он начинает их пинговать, что определить, на каких из них есть работающие тачки, а на каких - нет. Если ты путаешься в понятиях сканирования портов и сканирования сетей, глянь в рубрику «Биты» - там об этом как раз пишут ;). Ок, вернемся к нашему сканеру. Видешь, он пишет, что для большинства типов сканирования необходимы права рута. Если запускать сканер под рутом, он по дефолту будет юзать продвинутый scan type TCP SYN, а если пускать под обычным юзером - будет юзаться тормозной и легко обнаруживаемый тип сканирования: TCP-сканирование соединением. Ок, с типами сканирования разобрались - перейдем к опциям. А они следующие:

-O: Эта опция включает функцию определения ОС, под которой живет сканируемый комп (и об этом можно почитать в этом номере Спеца - прим. ред.);

-p <диапазон>: Опция с переменным параметром, позволяет задать диапазон портов для сканирования. Пример диапазона прилагается;
-F: Запрещает nmap'у сканировать какие-либо порты, кроме тех, что есть в его списке (nmap services);
-v: Выдает более подробную информацию. Если вбить эту опцию два раза, инфа будет в два раза подробнее :);
-PO: Запрещает пинговать сканируемые хосты, применяется к хостам, о которых известно, что на пинг они не отвечают, но тем не менее не находятся в дауне;
-T: Определяет политику временных параметров;
-n: Запрещает производить DNS-преобразование;
-R: Всегда производить DNS-преобразование;
-oN <logfile>: Вывод результатов не на экран, а в файл. Очень удобно – всегда можно посмотреть;
-oX <logfile>: Вывод результатов в файл в XML-формате;
-oG <logfile>: Вывод результатов в файл в формате grep-совместимом формате (позволяет производить хитрый поиск по файлу);
-iL <inputfile>: Брать хосты/IP для сканирования из файла. Для тех случаев, когда приходится сканировать огромное количество хостов или ip'шников;
-S <your_IP>: Позволяет явно указать свой IP;
-e <devicename>: Позволяет явно указать сетевой интерфейс;
—interactive: работать в интерактивном режиме. На самом деле неудобно – намного быстрее задавать все параметры в командной строке, но если ты их пока плохо знаешь...

Вот, в общем-то, и все, что надо знать, чтоб эффективно юзать nmap. (все очень просто: вбиваем «nmap», выбираем тип сканирования, включаем если надо какие-либо опции и вперед). Но это далеко не все возможности nmap :)! Введи следующее:

```
man nmap
```

и ты увидишь, сколько там еще опций и типов сканирования, не представленных в Help Screen'е (скрин 3).

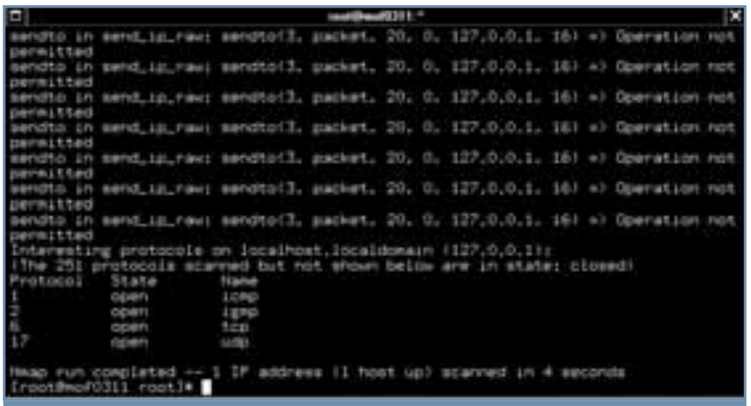
мануалка на nmap

-sO: Очень важный scan type – позволяет определить, с какими протоколами может работать сканируемы хост.

```
nmap –sO 127.0.0.1
```

Как видишь (скрин 4), мой комп поддерживает четыре протокола: icmp, igmp, tcp и udp.

-sI <zombie host[:probeport]>: Тоже очень важная штука, воспользовавшись которой, можно просканировать машину не со своего компа (и не со своего IP), а с какого-нибудь другого.



скрин 4

-sA: TCP ACK сканирование (читай об этом scan type'е в статье про методы сканирования).

-sW: TCP window сканирование.

-sL: Просто выводит список вида «имя_домена(ip)», не сканируя хосты.

-PT: Еще одна очень удобная фишка – позволяет пинговать хосты (определять, живы они или нет) средствами TCP, то есть без icmp. Пригодятся, если icmp-пакеты режутся на файрволе.

-PI: Пингует хост нормальными ICMP_ECHO-запросами.

-PP: Пингует хост ICMP_TIMESTAMP-запросами.

-PM: Пингует хост ICMP_NETMASK-запросами.

-PB: Пингует хост одновременно и средствами ICMP, и TCP.

-f: Включает зло-фрагментацию пакетов при SYN, FIN, Xmas и Null scan type-'ах. Фрагментация – это разбиение пакетов на несколько маленьких частей. Фишка в том, что сильно фрагментированный заголовок пакета может проскочить через фильтры файрвола.

-oS <logfile>: Это прикол :)))))))! Я протащился. Попробуй эту фишку, а потом открой и посмотри logfile.

-g: Позволяет явно указать свой порт.

На самом деле, и это еще не все – всяких опций еще куча, но остальные уж очень специфические (например, как указание количества допустимых параллельных запросов и тд). Лучше их не трогать, так как забьешь голову лишним мусором, а самое важно не запомнится :). Главное – знать основы, а когда понадобятся всякие мелочи.., тогда до них и следует докапываться ;).

SCAN COMPLETE

Вот и все. Этого достаточно, чтобы научиться пользоваться самым мощным на сегодняшний день сканером. Кстати, если у тебя нет линя и ты по каким-то причинам не хочешь его себе ставить, можешь поюзать nmap под винды. Долгое время Fyodor не мог найти людей, которые помогли бы ему с портированием nmap'а на маздайную платформу, но вот, наконец, свершилось. Теперь рулезный сканер доступен и для виндовых юзеров :). Ну, если ситуация такая, что линя вообще - ну ни как! – под рукой нет, то можно, наверное, воспользоваться и виндовым nmap'ом, но я бы все равно рекомендовал использовать родную nix'овую версию :))). Удачи тебе в твоих сетевых исследованиях!

NESSUS

Nessus – это самый мощный на сегодня анализатор уязвимостей под nix. Так же как и nmap в сканировании, nessus – стандарт де факто в вопросах автоматического анализа уязвимостей хоста. Прога довольно качественная, но, к сожалению, немного тяжеловатая. Зато работает под X, а не в консоли. Хотя не факт, хорошо это или плохо ;). Во всяком случае, нессус можно отинсталить и без GUI, тогда он будет работать в консоли.

установка/настройка/разбор

aDm

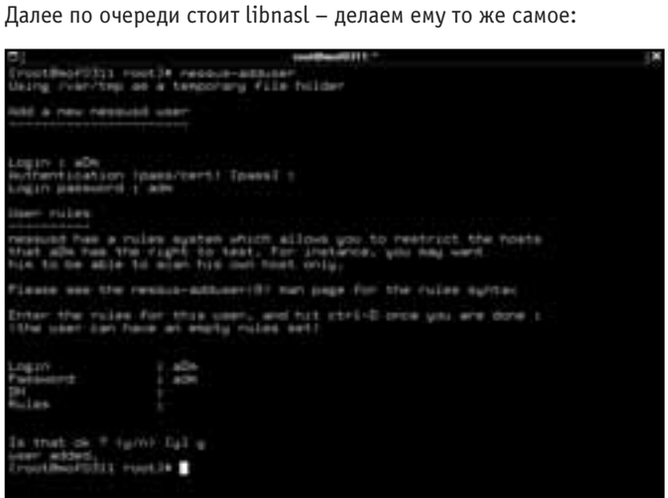
Nessus – это самый мощный на сегодня анализатор уязвимостей под nix. Так же как и nmap в сканировании, nessus – стандарт де факто в вопросах автоматического анализа уязвимостей хоста. Прога довольно качественная, но, к сожалению, немного тяжеловатая. Зато работает под X, а не в консоли. Хотя не факт, хорошо это или плохо ;). Во всяком случае, нессус можно отинсталить и без GUI, тогда он будет работать в консоли.

КАЧАЕМ И СТАВИМ

Кстати, nessus будет работать толко в том случае, если в системе установлен nmap – он использует его возможности для сканирования своих жертв. Так что эти две рулезные проги дружат :).
Сайт Nessus нессус находится по адресу http://www.nessus.com/. Там можно найти доки, всякую инфу, историю проекта и, конечно, саму тулзу. Текущая версия - 1.2.5. Качнуть нессус можно с этого ftp'шника: ftp://ftp.nessus.org/pub/nessus/nessus-1.2.5/src/. Надо утянуть libnasl-1.2.5.tar.gz, nessus-core-1.2.5.tar.gz, nessus-libraries-1.2.5.tar.gz и nessus-plugins-1.2.5.tar.gz. После того, как все это добро сольется, распаковывай его в какую-нибудь директорию и приступай к установке. В первую очередь надо установить nessus-libraries, для этого делаем следующее:

```
cd ./nessus-libraries
./configure
make
make install
```

Далее по очереди стоит libnasl – делаем ему то же самое:



1 nessus-adduser

```
cd ../libnasl
./configure
make
make install
```

Потом nessus-core:

```
cd ../nessus-core
./configure
make
make install
```

И напоследок nessus-plugins:

```
cd ../nessus-plugins
./configure
make
make install
```

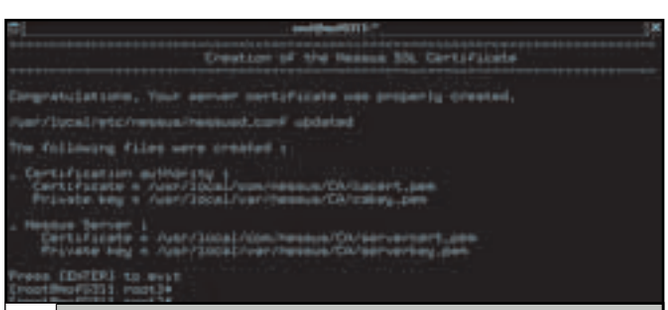
Компилится все это будет достаточно долго (даже если у тебя мощная тачка), так что имеет смысл сходить за пивком ;). Я свою дозу уже замерил - пока на моей тачке ставится nessus, я успеваю выдуть ровно бутылку горючего :). Ок, все откомпилилось и отинсталлилось, но чтоб тулза зафурычила надо сделать еще кое-что: открой файл /etc/ld.so.conf и пропиши в самом конце следующую строку:

```
/usr/local/lib
```

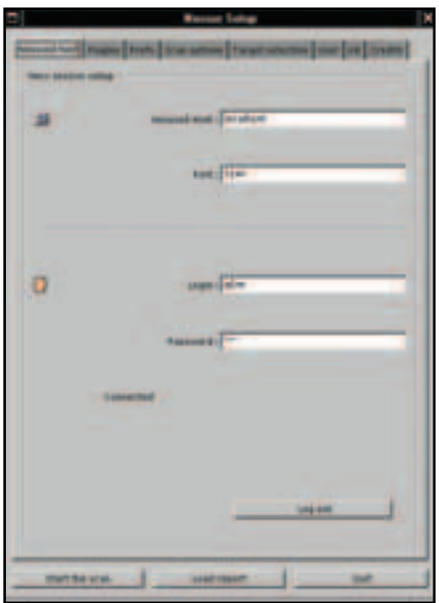
и выполни команду ldconfig. После этого прога должна работать. Все можешь удалять всякие уже ненужные директории, образовавшиеся после распаковки архивов nessus – они нам больше не понадобятся.

НАСТРАИВАЕМ

Пришло время поговорить о том, как устроена наша подопытная тулза. Nessus – это клиент-серверное приложение. То есть он состоит из двух частей: клиента и сервера. Килент – это та часть, которая взаимодействует с юзером: позволяет выбирать всякие параметры сканирования, настраивать плагины, выбирать исследуе-

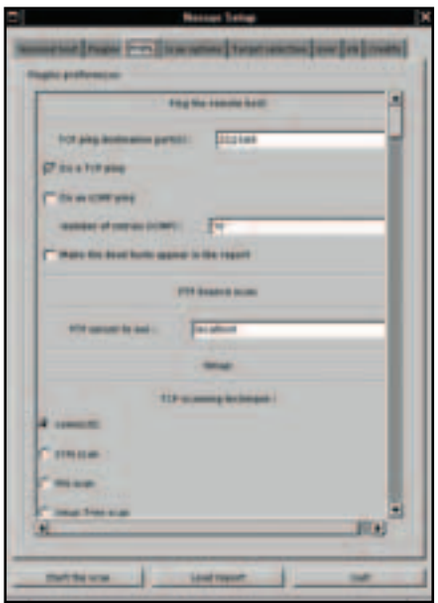


2 nessus-mkcert



3 Закладка Nessusd host

4 Закладка Plugins



5 Закладка Prefs.

мый хост и тд (как ты уже понял, клиентская часть nessus оборудована GUI'евым интерфейсом). Работа происходит по следующей схеме: nessus-клиент взаимодействует с пользователем, собирает у него полность всю инфу, которая необходима для начала сканирования и анализа жертвы (кого сканить, как сканить, на какие ошибки тестить и тд), далее nessus-клиент коннектится к nessus-серверу (адрес которого ему должен задать юзер) и передает ему всю необходимую информацию. Nessus-сервер производит анализ сканируемой системы и отправляет результаты nessus-клиенту, который выводит их юзеру в виде красивого окошка :). «Зачем этот гимор?» - спросишь ты «Нельзя ли сделать так, чтоб я нажимал на одну кнопку и все было?». Можно, но так, как есть сейчас, удобнее :). Фишка в том, что можно один раз поставить nessus-сервер на каком-нибудь шелле, а потом юзать его откуда угодно при помощи nessus-клиента. Комфорт, блин!
Для того чтобы запустить этот самый nessus-сервер, надо сначала выполнить команду:

```
nessus-mkcert
```

Это команда создаст какой-то идиотский сертификат (скрин 2), который нам, в общем-то, и на фиге не нужен. Скрипт будет задавать всякие дурацкие вопросы - если не охота ковырять, просто нажимай везде Enter, будет все по дефолту.
Теперь необходимо создать юзера на nessus-сервере. Надо это, чтоб всякие левые хаксоры не могли воспользоваться установленным тобой nessus-сервером. Вбивай:

```
nessus-adduser
```

Прога предложит тебе ввести имя пользователя, выбрать метод аутентификации (соглашайся на pass), ввести логин и определить правила для этого пользователя. У nessus-сервера есть механизм ограничения прав пользователей, и правила каждого пользователя определяют, какие хосты он может сканить и анализировать на ошибки (проще говоря, на какие хосты он может натравить nessus). Объясню, как это работает, на случай если ты вдруг захочешь создать аккаунт своему младшему братишке, но такой, чтоб он сканить комп только младшей сестренки, а не сервера, скажем, Microsoft'а. У каждого пользователя может быть бесконечное количество правил. Правило – это одна строка следующего формата:

```
accept|deny ip
```

Первая часть строки (accept|deny) – это действие, которое распространяется на втору часть – на IP'шник. Действие может быть либо accept (разрешить), либо deny (запретить), а IP'шник может быть любым (более того, можно задавать не один айпи, а маску, в которую может войти несколько адресов). Логика простая: берется IP и смотрится, какое действие к нему привязано – accept или deny. Если accept, то пользователю разрешается сканить этот IP, если deny, то, соответственно, иди на фиг и все такое :). Так как правил много, можно задавать сколько угодно IP'шников, к которым у юзера будет доступ или нет. Кроме того существует еще и завершающее правило, которое имеет формат:

```
default accept|deny
```

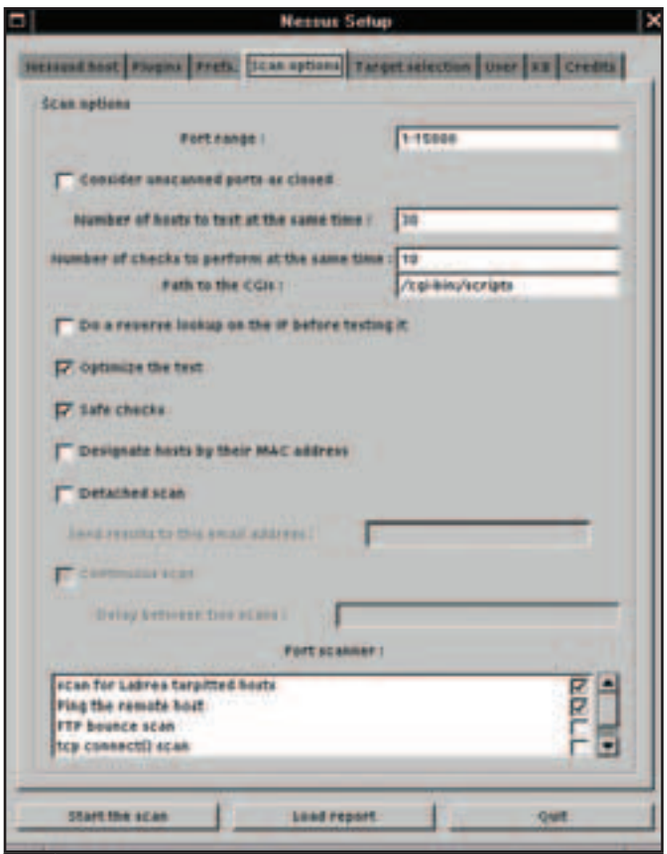
Оно определяет, что делать, если юзер решил посканить IP, который не определен ни в одном из его правил. Соответственно, если вбить default accept, сервер разрешит пользователю сканить такие адреса, если же default deny – посылает далеко.
Короче, если комп твоей сестренки имеет адрес 192.168.0.65, то следующее правило запретит твоему братишке сканить что-либо, кроме ее компа:

```
accept 192.168.0.65
default deny
```

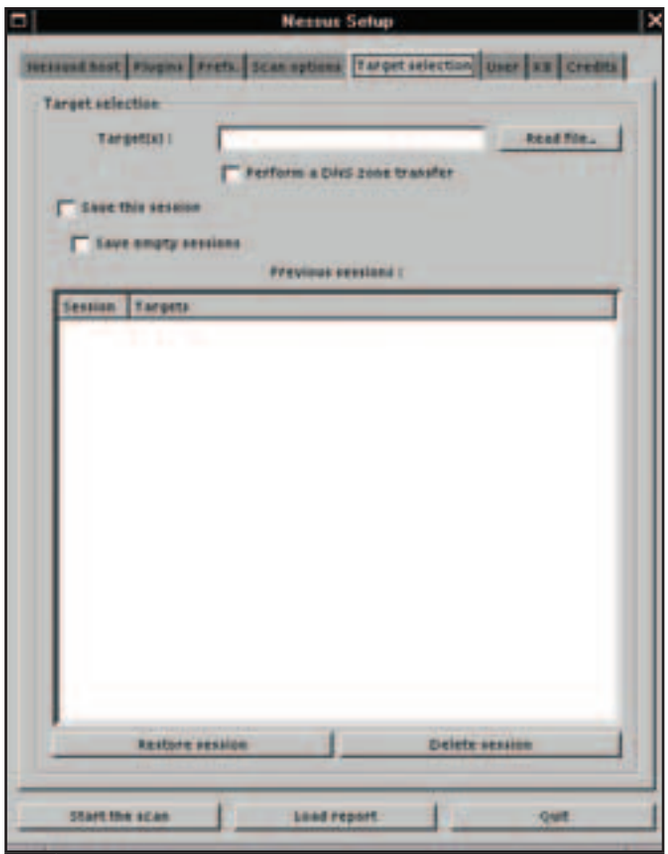
Можно сканить только 192.168.0.65, все остальное – гуляй. Это касательно твоего мелкого братишки, а если ты создаешь аккаунт для себя (и, естественно, не хочешь иметь никаких ограничений), то вообще не вводи никаких правил – просто нажми Cterl-D. В итоге должно получиться что-то типа этого (скрин 1).
Фууу, вроде всю подготовительно-настроечную работу nessus-сервера провели, теперь можно и запустить его. Вбивай:

```
nessusd –D –p 1090
```

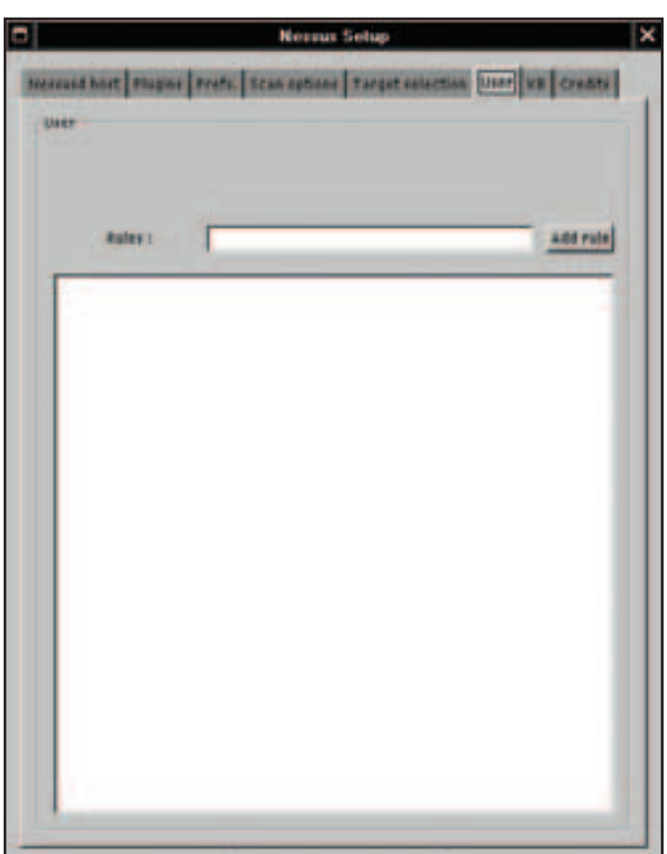
Этим ты запустишь демон сервера в бэкграунд-моде на порту 1090. Все, теперь он будет ждать соединения клиента. Чтоб запустить последнего достаточно просто набрать в командной строке



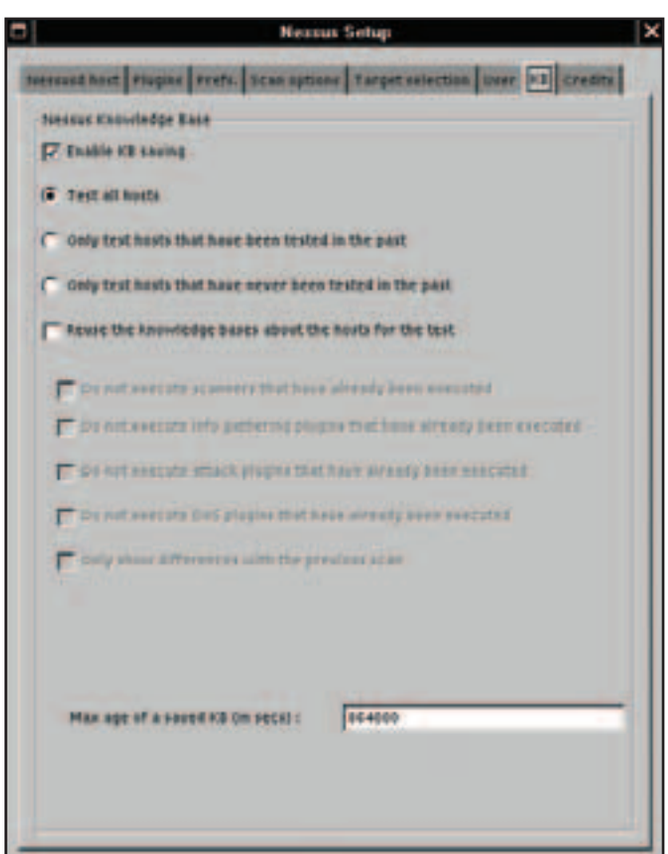
6 Закладка Scan options



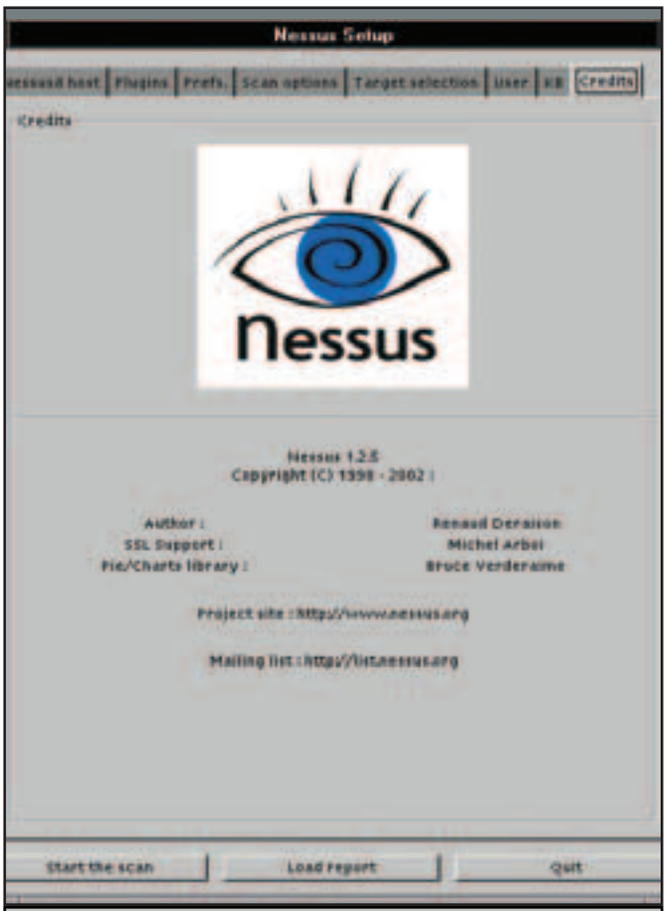
7 Закладка Target selection



8 Закладка User

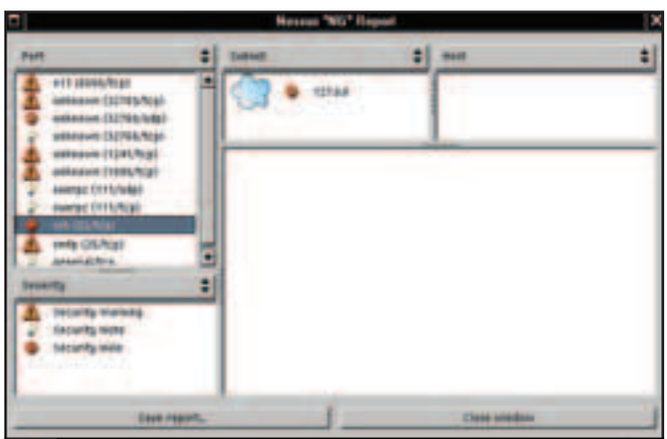


9 акладка KB



10 Закладка Credits

11 Nessus за работой



12 Тестирование завершено. Ошибок нет.

слово nessus и нажать Enter. Появится окно Nessus'а. В нем есть несколько закладок – давай пройдемся по ним.

Nessusd host (скрин 3)
Под этой закладкой кроются настройки соединения к nessus-серваку. В «Nessusd host» надо писать IP машины, на которой запущен сервак. В нашем случае это 127.0.0.1, так как мы запустили nessusd на своей машине. В поле «Port» пишем 1090 (это номер порта, который мы передали демону при зупуске). В полях «Login» и «Password» вводим соответствующие тому юзеру, под которым мы хотим работать, логин и пароль (в моем случае – «aDm» и «adm»). Ниже есть кнопочка Log in, которую надо нажать, чтоб начать работу (клиент сконнектится с серваком).

Plugins (скрин 4)
Тут валяются плагины и инструменты для управления ими. Все просто: включить плагин, отключить плагин – ну, дык, преимущества графического интерфейса :). Плагины – это самое главное. Они являются сценариями взлома, в соответствии с которыми производится анализ безопасности тестируемой системы. Плагинов много и они постоянно обновляются. В комплекте Nesus есть специальная утилита, которая позволяет аптейтить базу плагинов из инета.

Prefs. (скрин 5)
А на этой закладке живут настройки плагинов.

Scan options (скрин 6)
Настройки сканирования. «Port range» – диапазон портов. Галочка ниже позволяет воспринимать непросканенные порты как закрытые. «Number of hosts to test at the same time» – определят количество хостов, тестируемых одновременно. «Numbers of checks to perform at the same time» - определят количество проверок, производимых одновременно. «Path to CGIs» – путь к директории цгишек. Далее идет еще куча галочек, смысл которых понятен из названия. Предпоследняя из них – наиболее прикольная: позволяет запустить Nessus и свалить пить пиво, а результат потом приедет по мылу :).

Target selection (скрин 7)
На этой закладке следует вбить имя/IP хоста(ов), который будет сканиться и теститься. Можно ввести прямо в поле «Target(s)», а можно загрузить список из файла.

User (скрин 8)
Закладка пользователя – отсюда можно менеджерить настройки правил.

KB (скрин 9)
На этой закладка можно настроить все так, чтоб результаты сохранялись на nessus-сервере (на всякий пожарный).

Credits (скрин 10)
Ну и закладка авторов. Типа инфа о крутых кодерах и хакерах :).

ЮЗАЕМ

Ну и осталось сделать самую малось – поюзать Nessus. Настраивай все на закладках и смело жми кнопарь Start the scan в самом низу окна проги. Я потетстил свой родной комп :). Процесс тестирование продлился совсем недолго (скрин 11), но это благодаря тому, что я тестил не удаленный комп, а свой родной. Nessus, конечно, никаких дыр не нашел – так, какие-то мелкие предупреждения. Ну, это понятно – у меня же десктопная система, а не сервер какой-нибудь: сервисов нет, открытых портов мало – багов нет :) (скрин 12).

Вот и все, можно сказать освоили Nessus. Если захочешь полезть вообще в глубокие дебри этого сканера, глянь файл /usr/local/etc/nessus/nessusd.conf (настройки демона). Пока!

ПРОСТЕЙШИЙ СКАНЕР

изучаем исходник scan.c

Ну что стоит настоящему хакеру быстренько налабать программку простейшего сканера портов? Лень? Ну вот и нам тоже ЛЕНЬ! Поэтому как настоящие разленившиеся раздолбаи мы заходим по адресу: http://cs.baylor.edu/~donahoo/NIUNet/portscan.html и качаем оттуда файл scan.c с готовым сканером. Еще нам понадобиться файл listofports.dat с описанием портов (брать там же).

Рваный нерв

КАК ЗАПУСТИТЬ ПРОСТЕЙШИЙ СКАНЕР?

Мы откомпилили эту программу под Linux с ядром 2.4X. Для этого надо набрать:

```
> gcc –o ./scan ./scan.c
```

После компиляции получившемуся бинарнику надо выставить атрибуты запускаемого файла:

```
> chmod +x ./scan
```

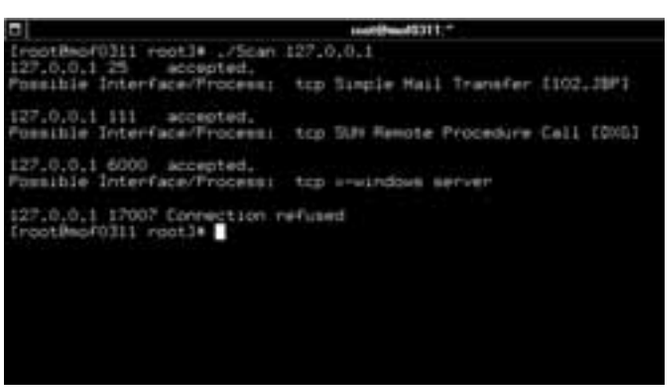
После этого можно запускать сканер, для этого укажи айпишник или доменное имя жертвы:

```
> ./scan 127.0.0.1
```

Таким образом, мы просканили самих себя. Сканер выдал нам порты, которые были открыты в нашей системе. А для того, чтобы посканить доменное имя плохого хоста можно запустить сканер так:

```
> ./Scan www.plohoy_host.ru
```

Вот и все, что нужно начинающему юниксойду, чтобы скомпелить и испытать свой сканер. Три строчки и ты можешь чувствовать себя богом!



МАЛЕНЬКИЙ БАГ!

Куда бы мы девались без багов? В коде этой программы был маленький баг: вместо файла listofports.dat программа обращается к файлу listoports.dat. Это легко лечится, если переименовать файл с описанием портов, удалив букву «f». Либо можно изменить код программы, добавив профуканное «f» в имя файла.

КАК РАБОТАЕТ ПРОСТЕЙШИЙ СКАНЕР?

Простейший сканер засасывает в себя айпишник жертвы и поочередно пытается открыть все порты из списка. Список портов находится в файле listofports.dat. Если порт открывается, то сканер выводит описание этого порта, которое тоже берет из списка портов. Порт, который удалось открыть сканер выводит на экран.
Можно задать программе доменное имя в виде www.plohoy_host.ru, тогда программа перед подключением запросит айпишник жертвы у сервера DNS.

Чтобы программа была, как можно меньше в ней использованы указатели. Чтобы лучше вникнуть в суть этой программы тебе придется разобраться с указателями. С помощью указателей мы записываем содержимое файла со списком портов в память в виде дерева. С помощью тех же указателей мы достаем нужные номера портов и описание к ним.
Указатель указывает на место в дереве, где лежит нужная информация, в этом вся его особенность. То есть нам не приходиться заморачиваться с перебором массивов и переменными, мы просто двигаем указатель по дереву.

ЛИСТИНГ ФАЙЛА SCAN.C с подробными комментариями.

```
/* Подключаем необходимые библиотеки */
#include <stdio.h>
#include <sys/socket.h>
#include <arpa/inet.h>
#include <errno.h>
#include <unistd.h>
#include <signal.h>
#include <string.h>
#include <netdb.h>

#define MARK '/'

/* Вот так с места в карьер мы начинаем главную функцию программы.
Во время запуска программы ты можешь передать цифры целого типа,
или строку символьного типа. */
void main(int argc, char *argv[])
{

/* Объявление переменных, используемых в сканировании портов */
  int probeport = 0;
  struct hostent *host;
  int err;
  int i;
  int net;
  struct sockaddr_in sa;

/* Объявление переменных, используемых при чтении файла */
FILE *ptr;
```

```
char buf1[100];
int c;
char *temp1;
char *temp2;

/* Открытие текстового файла listofports.dat. */
ptr = fopen(«listofports.dat», «r»);
if (ptr == NULL)
{
perror(«listofports.dat»);  /* Если такого файла нет, то программа сообщает об ошибке, не забудь качнуть этот файл и поместить его в рабочую директорию. */
exit(1);
}

/* Проверка, правильно ли введен адрес */
  if (argc != 2) {
    printf(«Usage: %s hostname\n», argv[0]);
    exit(1);
  }

/* Вся информация о портах храниться в файле listofports. Когда программа находит на теле жертвы открытый порт, она подбирает к нему описание из файла. Чтобы удобнее было использовать информацию, из файла мы записываем ее в виде дерева, по которому ползаем указателями. Этот кусочек кода отвечает за засасывание инфы из файла в дерево. */

while ((c = fgetc(ptr)) != EOF) /* двигаем указатель до конца файла (End Of File, EOF)*/
{
fgets(buf1, 100, ptr);
temp1 = strchr(buf1, MARK);
temp2 = temp1;
while (*temp2 != ' ') /*Двигаем указатель до пробела*/
{
temp2—;
}
temp1++;
if ((*temp1 == 't') || (*temp1 == 'T'))
i = atoi(temp2);
else
i = -1;

/* Если порт готов, начинаем сканирование! */
if (i>-1){
    strncpy((char *)&sa, «», sizeof sa);
    sa.sin_family = AF_INET;

/* Для сканирования портов сканеру нужно указать айпишник жертвы. А можно указать URL. То есть сканер понимает имя на нормальном человеческом языке с точечьками типа: www.plohoy_host.ru. Этот кусок кода отвечает за определение IP адреса по URL */
if (isdigit(*argv[1]))
      sa.sin_addr.s_addr = inet_addr(argv[1]);
   else if ((host = gethostbyname(argv[1])) != 0) /* получение IP по имени хоста*/
      strncpy((char *)&sa.sin_addr, (char *)host->h_addr,sizeof sa.sin_addr);
    else {
      herror(argv[1]);
      exit(1);
    }
/* Преобразуем вычисленный номер порта в удобный для использования вид */
sa.sin_port = htons(i);

/* Открываем сокет.*/
net = socket(AF_INET, SOCK_STREAM, 0);
    if (net < 0) {
      perror(«\nsocket failed in creation»); /* Если сокет не открывается, сообщаем об ошибке*/
      exit(1);
    }
    err = connect(net, (struct sockaddr *) &sa, sizeof sa);  /* Лазаем указателем по дереву и находим описание для порта, который желает открыться. Если ты не забыл, в дерево мы записывали информацию из файла с описанием портов. */
    if (err < 0) {
      printf(«%s %-5d %s\r», argv[1], i, strerror(errno));  /* Не открывается! Ошибочка :( */
      fflush(stdout);
    } else {

/* Если порт все-таки открылся, то печатаем на экране его номер с описанием, взятым из дерева. */
printf(«%s %-5d accepted.                    \n», argv[1], i);

/* Вывод номера порта, над которым работает программа. */
printf(«Possible Interface/Process:  %s\n», temp1);
if (shutdown(net, 2) < 0) {
       perror(«\nshutdown failed»);
       exit(1);
     }
    }
/* Ну и конечно нужно закрыть сокет. */
 close(net);
  }}
  printf(«
\r»);
  fflush(stdout);

}
```

КУСОЧЕК ФАЙЛА listofports.dat

```
tcpmux          1/tcp TCP Port Service Multiplexer [MKL]
tcpmux          1/udp TCP Port Service Multiplexer [MKL]
compressnet     2/tcp Management Utility [BV15]
compressnet     2/udp Management Utility [BV15]
compressnet     3/tcp Compression Process [BV15]
compressnet     3/udp Compression Process [BV15]
rje             5/tcp Remote Job Entry [12,JBP]
rje             5/udp Remote Job Entry [12,JBP]
echo            7/tcp Echo [95,JBP]
echo            7/udp Echo [95,JBP]
discard         9/tcp Discard [94,JBP]
discard         9/udp Discard [94,JBP]
systat          11/tcp Active Users [89,JBP]
systat          11/udp Active Users [89,JBP]
daytime         13/tcp Daytime [93,JBP]
daytime         13/udp Daytime [93,JBP]
netstat         15/tcp Netstat
qotd            17/tcp Quote of the Day [100,JBP]
qotd            17/udp Quote of the Day [100,JBP]
msp             18/tcp Message Send Protocol [RXN]
msp             18/udp Message Send Protocol [RXN]
chargen         19/tcp Character Generator [92,JBP]
chargen         19/udp Character Generator [92,JBP]
ftp-data        20/tcp File Transfer [Default Data] [96,JBP]
ftp-data        20/udp File Transfer [Default Data] [96,JBP]
ftp             21/tcp File Transfer [Control] [96,JBP]
ftp             21/udp File Transfer [Control] [96,JBP]
telnet          23/tcp Telnet [112,JBP]
telnet          23/udp Telnet [112,JBP]
priv-mail       24/tcp any private mail system [RA11]
priv-mail       24/udp any private mail system [RA11]
smtp            25/tcp Simple Mail Transfer [102,JBP]
smtp            25/udp Simple Mail Transfer [102,JBP]
nsw-fe          27/tcp NSW User System FE [24,RHT]
nsw-fe          27/udp NSW User System FE [24,RHT]
```

АНТИСКАН

изучаем исходник scan.c

Вот углубились мы тут в, несомненно, важнейшую тему сканирования, а про одну хитрую фишку чуть не забыли. Админы – те еще черти – защищая свои системы, иногда такого напридумают... Вот, например, научились бороться с нашим братом обманными методами, наплевав на то, что порядочному админу нельзя опускаться до такого уровня. Оказывается, еще как можно! А как еще назвать то, что многие серьезные админы используют сегодня в свих системах защиты deception (обман)?

kleZ admin's deception

Самый простой пример - это замена баннеров стандартных сервисов. Заходишь ты на какой-нибудь ftp с надеждой определить по приглашению, что за система установлена на серваке. Он тебе радостно кричит: «wu-ftp 2.1.7-12 on AIX 5L 5.0. Welcome!!». Ты потираешь ручки, начиная уже искать в базах эксплоитов соответствующую версию wu-ftp. А на самом деле никакой это не wu-ftp и AIX'ом там и не пахнет – просто хитрюга-админ изменил приглашение ftp-сервера таким образом, чтоб по всем параметрам было похоже на wu'шник под AIX'ом. При чем делается это элементарно – надо только отредактировать один проклятый файл!

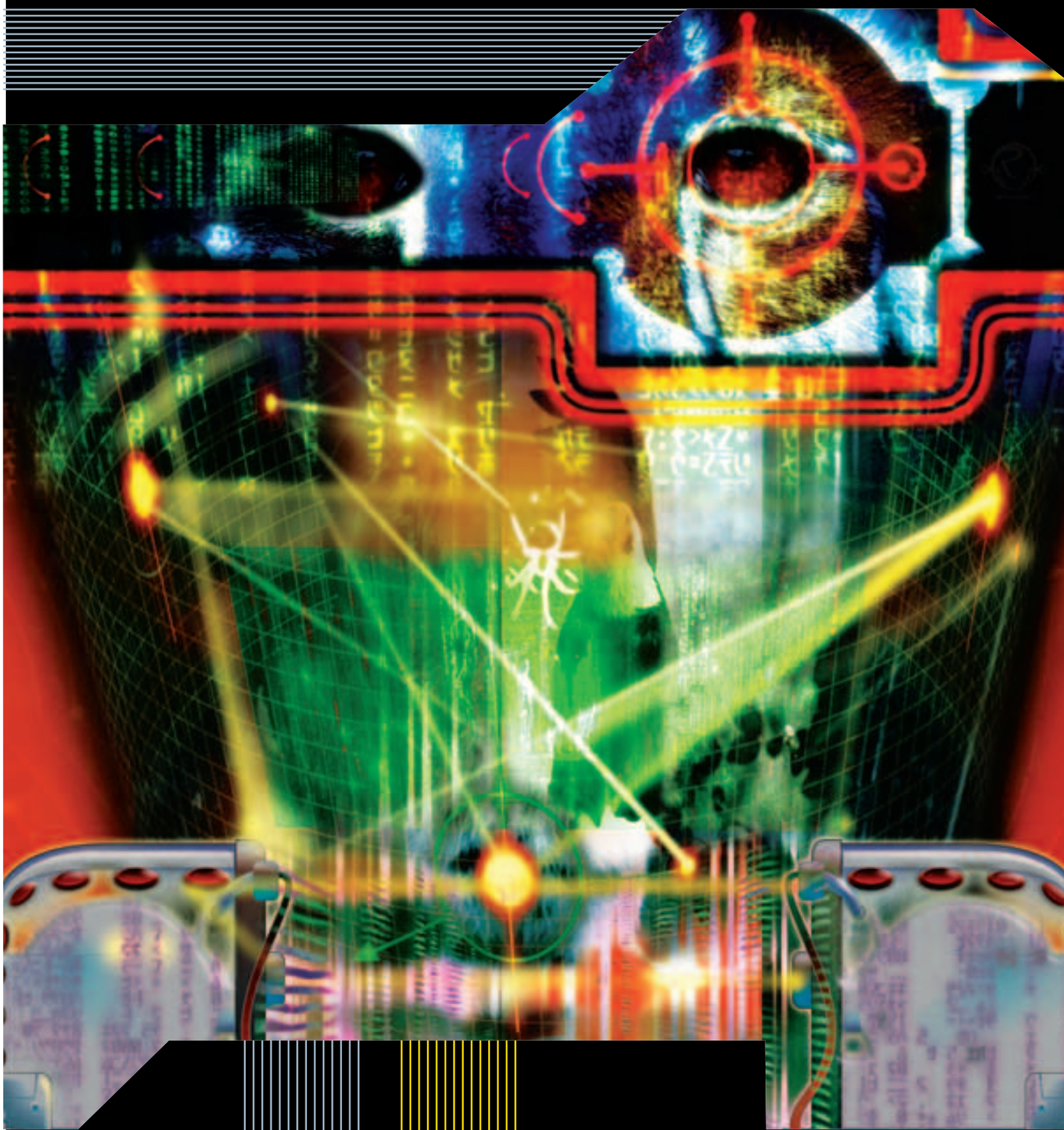
Но это еще не все, далеко не все. Почесав репы, доблестные труженники безопасности решили, что надо бы все это дело как-то автоматизировать, а то ведь удобная фишка. Почесали, почесали, да и накодили прогу, которую в наглую называли DTK (Deception ToolKit). То есть, набор для обмана. Расскажу вкратце, что это такое. DTK может повесить на любой порт своего демона, который ничего не умеет делать, кроме как брать из из стандартного ввода данные (то что вводит клиент, законнективший на этот порт) и выводить ответы в стандартный вывод (направляется прямиком клиенту). При чем поведение демона контролируется специальным скриптом-сценарием. В таком сценарии можно описать ЛЮБУЮ реакцию демона на ЛЮБОЙ пользовательский ввод. Все это делается настолько просто, что аж злость берет! Алгоритм работы демонов DTK следующий: если от пользователя пришел такой-то текст, вывести ему на экран сякой-то текст. Вот и все. Но фишка в том, что проявив терпеливость, любой админ может сэмулировать таким образом работу практически любого сервиса. Прикинь, заходишь, опять же, на ftp и думаешь: «Дай попробую дефолтовые логин/пароль – авось, админ-полный лох». Вводишь, а это на самом деле не ftp-сервер с тобой общается, а фальшивый DTK'шный демон. На твои дефолтовые логин/пароль он радостно отвечает: «Authentication complete» и ждет дальнейших команд. Ты думаешь: «Блин, а может и это прокатит?» и пишешь «get /etc/passwd». В действительно, катит – только это не настоящий passwd, а подделка, которую ты будешь еще две сутки расшифровывать (так как он никогда и не был зашифрован, а данные в нем – не пароли, а обычный мусор). Вот такие вот пироги :(.

Но такого злостного надувательства админам мало. Знаешь, что некоторые делают с помощью DTK? Они просто берут и открывают на своем серваке около сотни smtp-сервисов, один из которых настоящий, а все сотальные – DTK'шные демоны. Вот и пойди гадай, какой из них «BINGO»... Легче забить и пойти заниматься чем-нибудь еще, чем лазить на каждый из этой сони портов и проверять, похож ли он на реальный или все-таки DTK (если хорошенько присмотреться, можно все же отличить подделку от настоящего сервера – DTK не может полностью, до мелочей эмулировать настоящий сервис – слишком гиморные при этом скрипты-сценарии получатся).

Или еще другая фишка из этой же серии: сканируешь тачку, а на ней несколько тысяч открытых портов, из которых только 10-15 – реальные. Получается, что ты не можешь разобрать, какие порты на машине реально работают – теряется весь смысл сканирования.

Ну да ладно, к черту DTK – на самом деле, достаточно глючная и недоработанная софтина. Но в арсенале админов есть еще более жесткие обманные инструменты. Например, ip-маскарадинг. Это такая линевая фишка, которая позволяет полностью прятать внутреннюю сеть от интернета. Суть в том, что машина, которая является шлюзом в инет, переписывает в пакетах идущих из локальной сети во внешнюю все source IP на свой, а в ответах, пришедших ему на эти пакеты, переписывает destination IP на IP той машины из внутренней сети, которая изначально пакет и слала. Таким образом получается, что все внутренние машины ходят в инет, а снаружи все выглядит так, как будто это одна машина все время (та, которая как раз является шлюзом для внутренней сети). Теперь подумай, чем это грозит, если даже не принимать во внимание достаточно неприятный факт полного сокрытия схемы внутренней сети, ди и вообще факта ее существования? Представь себе, что админ такой хитрой сети открывает web-сервер на одной из внутренних машин, а шлюзу своему говорит, чтоб тот переписывал и пересылал все приходящие к нему на 80-ый порт пакеты внутреннему web-серверу. Выходит, что юзеры из инета работают как бы с шлюзом, считая его web-сервером, а сам web-сервер сидит себе в безопасности и комфорте, абсолютно ни для кого невидимый. Прикольно, да? А теперь представь что юудет, если какой-нибудь недалекий хацкер решит, скажем, посканить такой сервачек. Ведь все запросы на 21, 23 и прочие порты шлюз может слать не локальному web-серверу, а какой-нибудь другой локальной тачке (или может вообще сам их обрабатывать). Так что получается, что хацкер сканит совсем не ту машину, которую хотел. Вот такие вот они хитрые, эти админы ;).
Кстати ip-маскарадниг разрабатывался совсем не для таких низких целей! Первоначально он был предназначен тем, у кого был всего только один инетовский IP-адрес, но несколько машин в сети, которым все-таки надо было как-то выходить в интернет. Но со временем маскарадингу нашлось еще одно применение – то, о котором я только что рассказал ;).

Так что знай - админы не дремлют! И держи ухо востро!



Технологии LG FLATRON, опережая время, совершили революцию, позволив создавать мониторы, обладающие футуристически прекрасным качеством изображения и ультра-эргономичным дизайном.

Новый монитор FLATRON™ F700P

Абсолютно плоский экран,
уникальный динамичный дизайн, частота развертки 95 Khz,
экранное разрешение 1600x1200, USB интерфейс.

LG Flatron F700P - произведение искусства, которое притягивает взгляд, но абсолютно не утомляет его, сколько бы Вы не смотрели на этот монитор.

Модельный ряд: 17" F700P/F700B; FT775FT/FT795FTPlus; 19" F900P/F900B/FT915FTPlus

Новый монитор FLATRON™ LCD L1810B

Супер плоский монитор с диагональю 18,1",
футуристический дизайн просто великолепен,
экранное разрешение 1280x1024, USB интерфейс,
цифровое автосканирование и функция DVI-I – красота
окружающего Вас пространства в своем максимальном выражении.

Модельный ряд: 15" L1510P/L1510B/L1510S; FL575LE/FL563LE; 18" L1810B/L1810M/L1800P

Москва: D-Vision (095) 232-2030; Технотрейд (095) 291-2686; Ф-Н (095) 330-6359; Фалькон (095) 100-83-20; DVM Group (095) 777-1044; Дженнон (095) 787-4899; Сетевая (095) 745-2999; Эпси (095) 777-9779; Ландата (095) 193-5363; Ф-Центр (095) 472-6401; Формоза (095) 234-2164; Техносила (095) 777-8777; М.Видео (095) 777-7775; Мир (095) 152-4001; Эльдорадо (095) 979-5100; Полдис (095) 755-5557; Технотрейд Компьютер (095) 363-9333; Сетевая Лаборатория (095) 784-6490; СКИД (095) 956-8426; Кей Компьютер (095) 777-6655; Атлантик Компьютерс (095) 240-2091; Березка (095) 362-7840; ISM (095) 785-5707; Инкотрейд (095) 219-7001; ОЛДИ (095) 284-0239; Виртуальный мир (095) 234-3777; USN Computers (095) 775-8202; Старт-Мастер (095) 935-3892; Акситек (095) 737-3175; Радиокомплект-Компьютер (095) 902-8178; **Санкт-Петербург**: Сэлтэд (812) 321-6300; **Барнаул**: Мэйпл (3852) 244057; **Белгород**: Инфотех (0722)265819; **Воронеж**: РИАН (0732)512413; Сани (0732) 733222; **Екатеринбург**: Класс (3432) 589631; **Казань**: Алгоритм (8432) 365272; **Калуга**: Лого Контакт (08432) 564023; **Киров**: Гелиостиль (8332) 678366; **Краснодар**: Скай (8612) 621144; **Красноярск**: Альфа (3912) 211149; **Мурманск**: Экселент (8152) 450624; **Нефтекамск**: Мастерс Компьютерз (34783) 40002; **Нижневартовск**: Арикул (3466) 240920; **Нижний Новгород**: Аптэк (8312) 317078; **Новосибирск**: Компьютеры Оргтехника (3832) 490124; Техносити (3832) 332003; **Оренбург**: КС Центр (3532) 202160; **Пермь**: Амикон (3422) 196158; **Ростов-на-Дону**: Зенит-Компьютер (8632) 950000; Технополис (8632) 903111; **Самара**: Прагма (8462) 163367; Родник (8462) 345433; **Саранск**: Гелла ТЕСТ, (8342) 240591; **Саратов**: КомпьюМаркет (8452) 241314; **Тольятти**: СЭ плюс (8482)377871; **Томск**: Интэл (3822) 420224; **Тюмень**: Арсенал (3452) 464174; Компьютэл (3452) 463084; Инэкс-Техника (3452) 390036; **Уфа**: Монитэк (3472) 229989; **Хабаровск**: Компэлэ (4212) 302002; **Челябинск**: Никас-ЭВМ (3512) 349402; Реал-Урал (3512) 335812.

Информационная служба LG: (095) 742 7777; http://www.lg.ru

LG
Digitally yours

Открыта редакционная ПОДПИСКА!

СПЕЦ ХАКЕР

Теперь вы можете оформить редакционную подписку на любой российский адрес

Для этого необходимо:

1. Заполнить подписной купон (или его ксерокопию).

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета 100 рублей за 1 журнал. В стоимость подписки включена доставка заказной бандеролью.

3. Перечислить стоимость подписки через Сбербанк.

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

БОНУС!

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

ВНИМАНИЕ!

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

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

ПОДПИСНОЙ КУПОН (подписка через редакцию)

Прошу оформить подписку на журнал "ХакерСпец"

2002г.	■	■	■	■	■	■	■	■	■	■	□	□
2003г.	□	□	□	□	□	□	□	□	□	□	□	□
					(месяцы)							

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

Ф.И.О.

ПОЧТОВЫЙ АДРЕС: индекс область/край

Город/село ул.

Дом корп. кв.. код тел.

Сумма оплаты

Подпись Дата e-mail:

Копия платежного поручения прилагается.

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545

Плательщик

Адрес (с индексом)

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

Подпись плательщика

Кассир

ИНН 7729410015 ООО"ГеймЛэнд"

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545

Плательщик

Адрес (с индексом)

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

Квитанция

Подпись плательщика

Кассир

ИНФА ПО СКАНИРОВАНИЮ В СЕТИ

ЭТО СТОИТ ПОЧИТАТЬ

ТЫ, НАВЕРНОЕ, НЕ РАЗ ПАРИЛСЯ С ТОННОЙ УРЛОВ, ВЫЛИТЫХ НА ТЕБЯ ЯНДЕКСОМ ИЛИ РАМБЛЕРОМ, ПРИ ПОИСКЕ НУЖНОЙ ИНФЫОБЫЧНО СЛУЧАЕТСЯ ТАК, ЧТО ЗАВЕТНАЯ ССЫЛОЧКА НУЖНА ЗДЕСЬ И СЕЙЧАС, А ТЫ СИДИШЬ И ЧАСАМИ РОЕШЬСЯ СРЕДИ ГОР СТАФФА И ФЛУДА, И В ИТОГЕ ЗАБИВАЕШЬ НА ЭТО ПРОПАЩЕЕ ДЕЛО.

Frozen (frozen@real.xakep.ru)

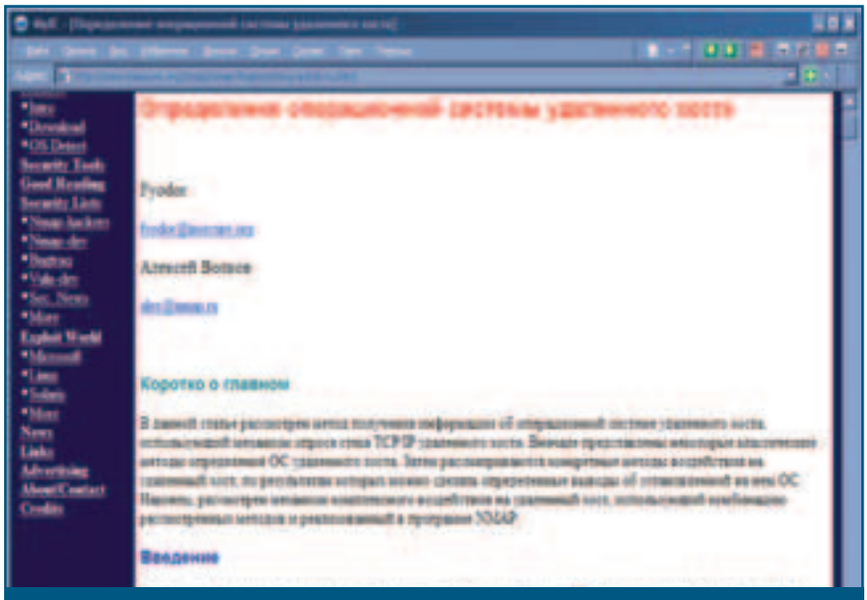
Чтобы ты всегда знал, что и где можно почитать по теме, один о-о-очень уважаемый человек в журнале :) поднапряг меня с этим делом и специально для тебя я долго и упорно бороздил просторы Инета на предмет достойной для твоих глаз инфы. Итак, вперед...

HTTP://WWW.RFC-EDITOR.ORG/RFC/RFC792.TXT

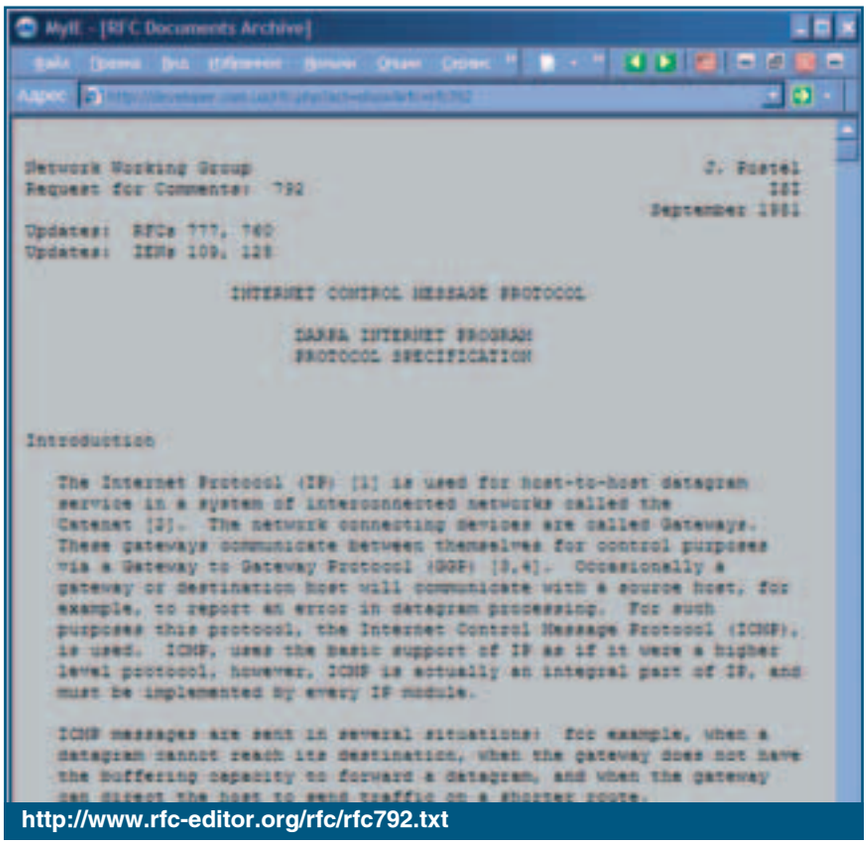
Есть такая умная штука, как RFC - это стандарты для всяких протоколов и прочих сетевых фишек. Сегодня нам требуется запрос с секретным номером 792. Очень нужный и полезный документ, скажу я тебе, ведь в нем рассматривается мегаважный протокол - ICMP. Одно время были траблы с определением работоспособности хостов в сети, и для того чтобы избежать проблем с этим, умные дядьки подумали-подумали да и выдали энное количество килобайт с заумным названием Internet Control Message Protocol. С помощью этого протокола происходит общение компов между собой и в документе описан стандарт, по которому строится пакет ICMP. Только вот почему-то эти ламерикосы совсем забыли про наших с тобой соотечественников, и все технические подробности без хорошего словарика не разберешь, но ничего, порывшись-порывшись еще, я откопал самый, на мой взгляд, подробный и правильный перевод на великий и могучий, а прочитать его ты сможешь тут: http://cydem.zp.ua/index.php3?lnk=rfc792r&conf=4.

HTTP://WWW.INSECURE.ORG/NMAP

Но определить состояние хоста - это еще полдела, важно также знать, а какие еще компы принадлежат к той же подсети и вообще сколько портов открыто и какая система стоит. Мне кажется, что тебе потребуется составить карту хостов, обитающих в данном сегменте. Самый, на мой взгляд, хороший помощник в этом деле - nmap, не буду описывать все примочки данной тулзы, потому как уже не раз это произведение программерской мысли было воспето на страницах][. А скажу лишь, что к проге прилагается довольно хорошая документация, в который во всех подробностях расписаны способы сканирования и просто огромная таблица ответов ОС (OS Fingerprint). Увидеть все это ты сможешь по вышеозначенному адресу, причем разработчики нмапа не забыли и про русскоязычных пользователей, и если ты не очень хорошо владеешь английским, специально для тебя есть страница на русском языке. Кстати говоря, еще много полезной инфы



http://www.insecure.org/nmap



http://www.rfc-editor.org/rfc/rfc792.txt

ки (если ты, конечно, хочешь немного повоевать с админом) можно попробовать определить, какие уже известные дыры и баги присутствуют в системе, а для этого служат cgi-сканеры, на страницу одного из которых я тебя и отправлю. Ты можешь возразить - «Нафиг нужно? Мне инфа требуется!». Можешь, конечно, и не смотреть данный линк, но подумай, кто, как не разработчик сканера, сможет лучше всего рассказать тебе про скан? В том-то вся прелесть и заключается, что на сайте присутствует просто море инфы по этому делу и даже доступна библиотека для перла, с помощью который ты сам сможешь разрабатывать сканеры.

HTTP://WWW.CRIME-RESEARCH.ORG/LIBRARY/XENON2.HTM

Если ты всерьез решил запариться над проблемой скана на уровне протокола, то этот материал был написан специально для тебя. Документик хоть и не блещет размером, зато тут со всеми подробностями разложен по полочкам принцип установки связи по протоколу TCP, рассказывается про возможные флаги пакета и вдобавок упомянута тема по IP ID

Если ты всерьез решил запариться над проблемой скана на уровне протокола, то этот материал был написан специально для тебя.

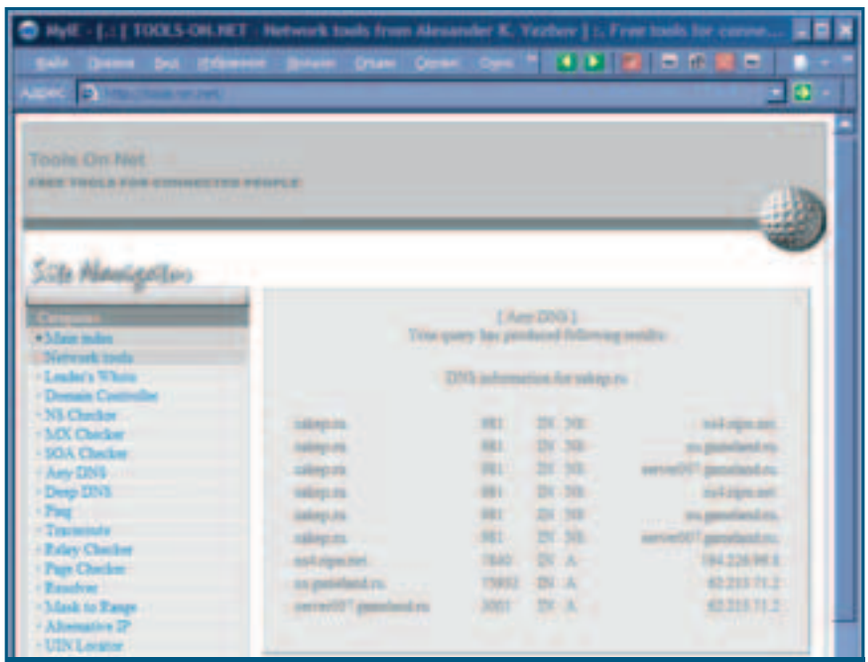
можно почерпнуть и на самом сайте insecure.org

HTTP://TOOLS-ON.NET/

Вообще, сканировать сервак со своего компа чревато ба-а-альшими неприятностями, начиная от простых писем в твой адрес и заканчивая зелеными человечками в глазке входной двери (хотя процент неприятностей прямо пропорционален профессиональности админа и крутости сайта), поэтому ты, естественно, будешь скрывать свой айпишник, но что делать, если ты не под никсами? А надо всего лишь набрать урл, указанный выше. И все проблемы исчезнут, ведь на этом сайте, помимо стандартных хуисов резольверов и трэйсеров, ты наткнешься еще и на большую кучку всяческих сетевых тулзов. И получить инфу по хосту или домену не составит никакого труда.

HTTP://WWW.WIRETRIP.NET/RFP

Ну вот, допустим, ты разведал инфу о жертве, и теперь, перед началом ата-



http://tools-on.net/

сканированию. По словам автора - относительно новая и очень мощная технология, которая позволяет провести максимально скрытное сканирование; сканировать системы, доступ к которым закрыт для атакующего файерволлом; частично исследовать правила файерволлов. Так что, прочитав такое грузилово, ты конкретно поднимешься в своих знаниях и узнаешь достаточно полезную инфу.

HTTP://NULL.NET.KG/CGI-BIN/GO.PL?TEXT=2

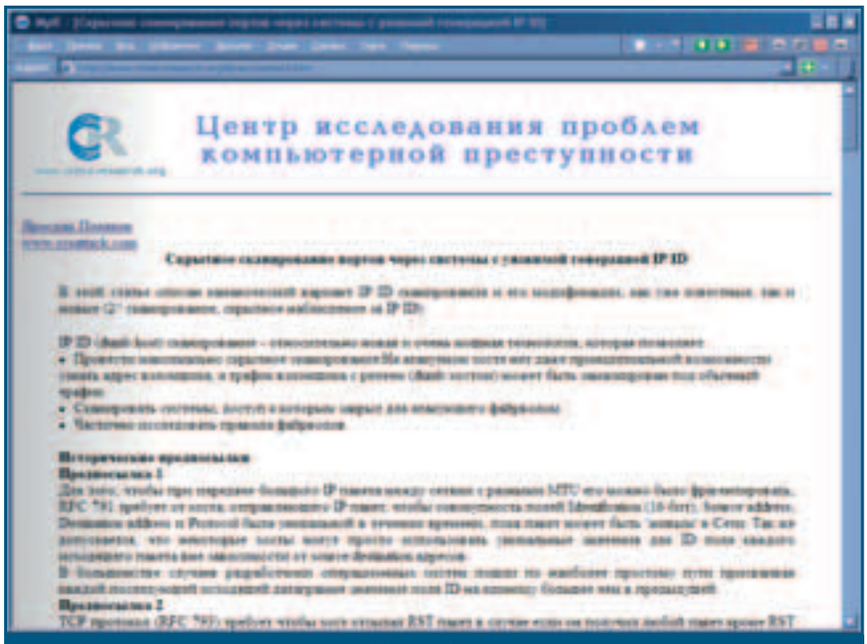
Предположим, что ты уже, прочитав все, что я предложил выше, более-менее разобрался с тем, что такое сканирование, как оно происходит, и понял работу протокола TCP/IP. Теперь, естественно, руки чешутся попробовать все это на практике, и тут тебе на выручку придет сайт Null Security Systems. Тебе повезло, если ты программер, и повезло вдвойне, если программер на Си, ведь статья называется «ПРОГРАММИРОВАНИЕ RAW SOCKETS НА С». Оччень полезный материальчик, прочитав который, ты сам сможешь с помощью этого архинужного языка собрать и отправить пакет в сеть. На паге предоставляется полное подробное руководство по всем нужным функциям и в конце прилагается примерчик с грамотными комментариями, так что не придется вникать, а что же тут наваял программер??? Да, чуть не забыл - прога написана для BSD'и, но общие принципы ты поймешь и, может, даже сможешь замутить что-нибудь подобное под винды с помощью библиотеки winpcap. (и если у тебя хорошо получится, то линк на твой труд обязательно появится на страницах][:).

HTTP://MAXVELL.WALLST.RU/CGI-BIN/IKONBOARD/FORUMS.CGI?FORUM=17

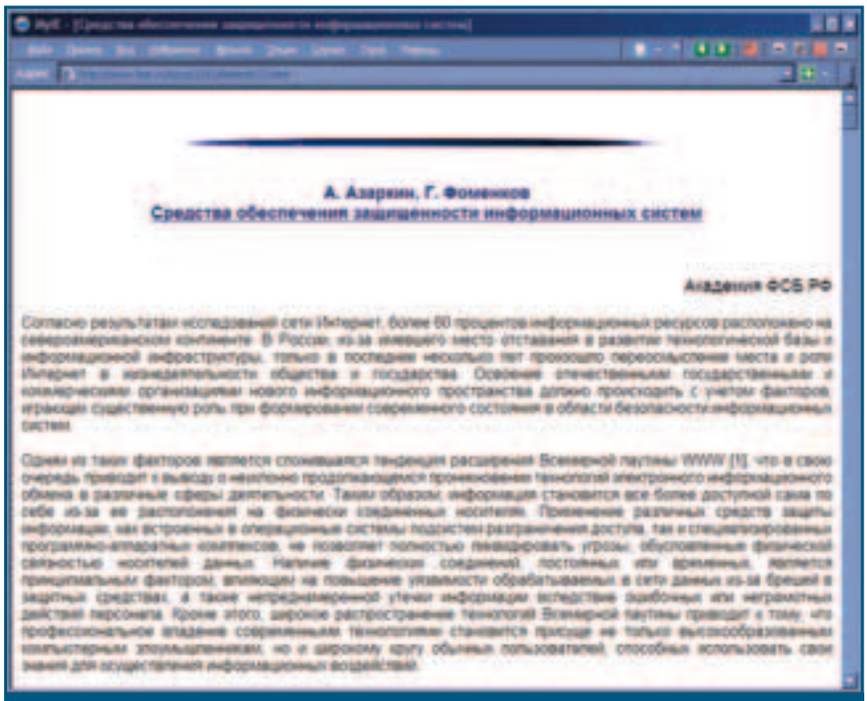
Но вдруг тебе захотелось узнать что-то специфическое, а найти такой инфы не получается или ты совсем ничего не понимаешь в том, что я прогнал выше. Ты, конечно же, можешь написать мне, и я подкину тебе свеженький адресок, но лучше сначала сходи на эту борду, тут достаточное количество тем по скану и вообще тебе все разжуют и положат в ротик. И к тому же народу сюда ходит достаточно много, так что кто-нибудь да поможет.

HTTP://WWW.FSSR.RU/ICCCS/1251/FOMENK(1).HTML

Ну а может ты выбрал для себя иной путь - ты решил стать админом

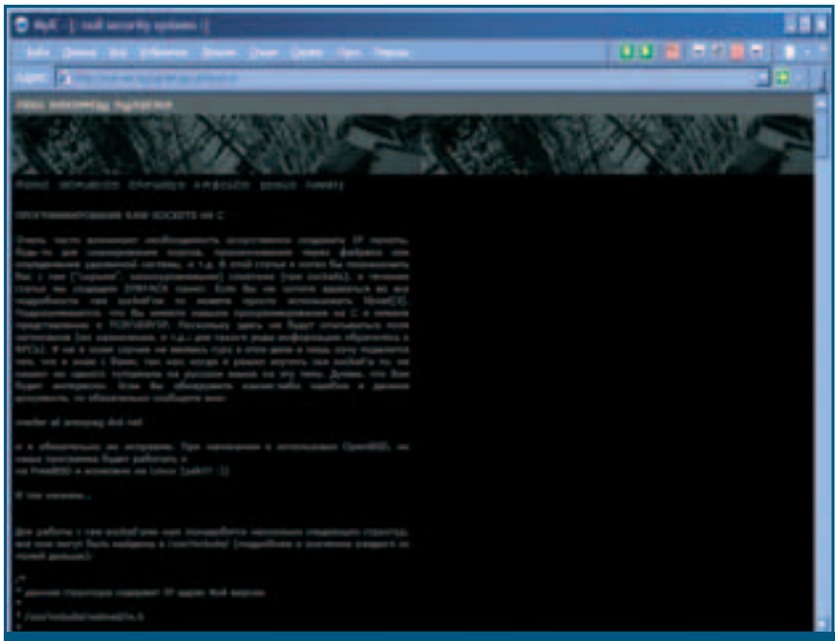


http://www.crime-research.org/library/xenon2.htm

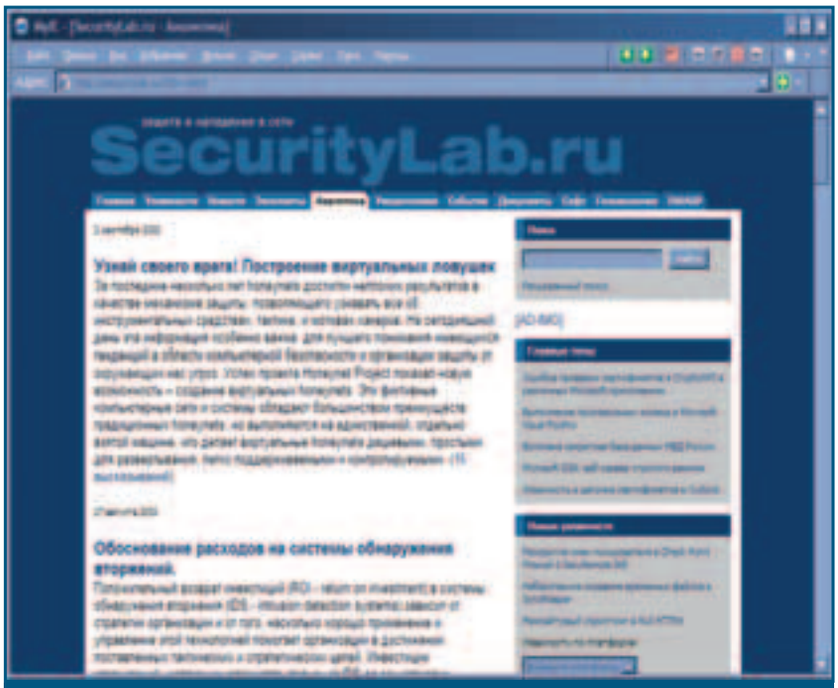


http://www.fssr.ru/icccs/1251/fomenk(1).html

(ну можно же такое хотя бы предположить? :)), и, наоборот, требуется тестировать систему на безопасность? И в этом случае для тебя найдется инфа в Сети. Взять, например, хотя бы вот эту мощную статейку, написана она для академии ФСБ, так что инфа тут действительно ценная и полезная. Объясняются принципы защиты компьютеров от сканирования и подробно рассматриваются такие «админские» проги, как SSS (System Security Scanner), SATAN, Internet Scanner... Тут тебе расскажут, как обезопасить свою сеть от вторжения изнутри и снаружи, покажут логи и научат анализировать результаты, выданные вышеописанными продуктами. Инфа отсюда и вправду очень пригодится тебе, даже если ты хочешь просто «поизучать» сети и протоколы.



http://null.net.kg/cgi-bin/go.pl?text=2



http://securitylab.ru/?ID=30522

HTTP://SECURITYLAB.RU/?ID=30522

Стильный дизайн и грамотное предоставление информации на этом сайте сразу бросается в глаза. Огромный архив всевозможных уязвимостей, информации по безопасности, нападению, анализу, да чего тут только нету... Изобилует и информация по сканированию (кстати говоря, есть полезные ресурсы как для админа так и для хацкера), представленная такими интересными темами, как «Сигнатуры систем обнаружения вторжения», «Следы атак по 80 порту», «Обход блокировки сканирования портов в Norton Personal Firewall 2002». В общем, это один из моих любимых сайтов, на нем всегда можно найти полезную информацию, которая может пригодиться в нелегком деле сетевика, хакера и админа.

ГИГАБАЙТНЫЕ ПОЛЯ

тестирование жестких дисков

test_lab (test_lab@gameland.ru)

В последнее время игры и всевозможный софт стали занимать на жестком диске все больше и больше места. И вот, когда этого места становится критически мало, поневоле начинаешь задумываться о покупке нового харда. Благо, выбрать есть из чего, да и цена за мегабайт существенно снизилась :). Итак, приступим к обзору самых популярных и производительных винтов на сегодняшний день.

ПЕРЕЧЕНЬ ЖЕСТКИХ ДИСКОВ

Maxtor D740X-6L 60 GB
Maxtor D540X-4D 40 GB
Seagate Barracuda ATA IV 40 GB
Caviar WD1200JB 120 GB
IBM Deskstar 120GXP (IC35L120AVVA07-0) 123.5 GB
Samsung SV2011H 20 GB

ОПИСАНИЕ ТЕСТОВОГО СТЕНДА

Процессор: Intel Pentium 4 1.4 GHz
Память: 2x256 МБ PC800 RDRAM RIMM Samsung;
Материнская плата: MSI 850 Pro5;
Видеокарта: ATI Radeon 8500
(драйвер версии 6.13.10.6043);
ОС: Windows XP Home Edition (build 2600).

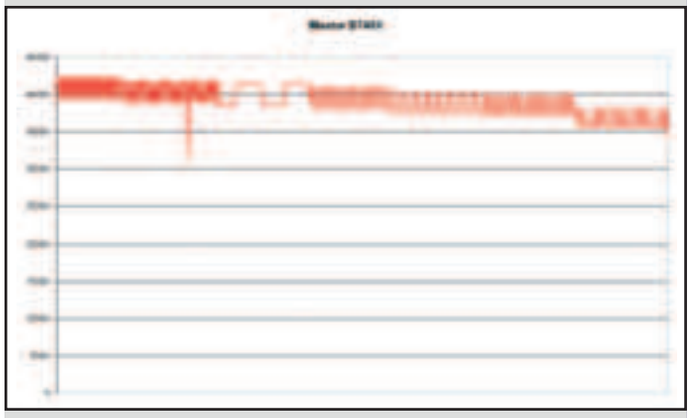
Maxtor

Солидная и быстро набирающая популярность на нашем рынке компания (на западе ее винчестеры уже довольно давно пользуются большим спросом). Особенно после приобретения другого гиганта винтостроения - Quantum. К тому же, жесткие диски от Maxtor всегда отличались высоким качеством и скоростью. Посмотрим же теперь, чем может порадовать нас эта компания.

Maxtor D740X-6L 60 GB

Эта модель - разработка компании Quantum, а это уже говорит о многом. Основным нововведением в ней является поддержка интерфейса Ultra ATA/133, что вкупе со скоростью вращения шпинделя 7200 rpm и объемом буфера на 2 МБ уже должно принести высокую производительность. Плотность записи составляет 40GB на пластину, что сразу вызывает уважение. Также можно отметить набор фирменных технологий - Maxtor Data Protection System и Shock Protection System, призванных защитить винт от всевозможных неприятностей. Данная линейка насчитывает четыре винчестера объемом на 20, 40, 60 и 80 гигабайт, ну а мы протестировали модель на 60 ГБ.

Компания Maxtor вновь показала отличный уровень своих девайсов. Качество поверхности на высоте, да и скоростные характеристики тоже впечатляют. Стабильный и ровный трансфер это только подтверждает. Среднее время доступа, несмотря на высокую плотность записи, держится на уровне 10,1 мс, что сразу бросает вызов остальным моделям. Загрузка процессора не велика и составляет всего 9,2%. В общем, все это достаточно серьезная заявка на победу в нашем тестировании.



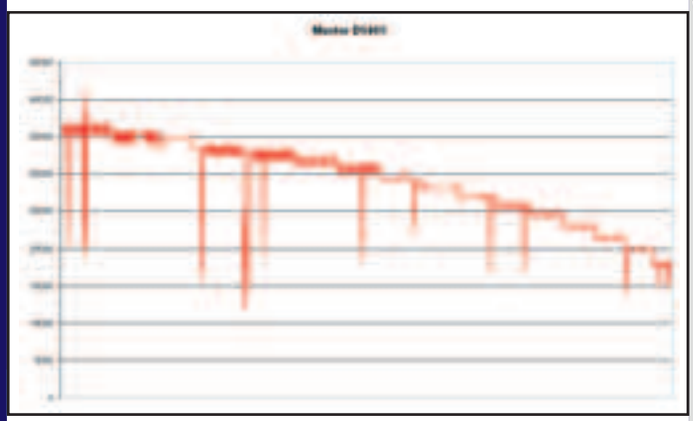
Maxtor D540X-4D 40 GB

Эта линейка имеет модели с объемом 20, 40, 60 и 80 гигабайт. Мы же протестировали модель с самым популярным объемом на 40 ГБ. D540X - уже «чистая» разработка Maxtor со своими индивидуальными особенностями и фишками. Первая особенность - сигнальный процессор (DSP), который занимается обработкой команд. Благодаря применению этой технологии существенно повышается производительность диска, т.к. время обработки команд существенно сокращается (вплоть до 90%!). Также нужно отметить систему управления акустическими характеристиками (можно выбирать между высокой производительностью и пониженным уровнем шума), что порадует многих. Ну, и конечно, фирменные технологии Data Protection System и Shock Protection System, защищающие жесткий диск от всевозможных стрессовых ситуаций. Остальные же характеристики выглядят

test_lab выражает благодарность компаниям "Остров Формоза" и "Elko" за предоставленные на тестирование устройства.

так: плотность записи - 40GB на пластину и скорость вращения шпинделя - 5400 rpm.

Хотя график и не такой ровный, как у прошлой модели, но для винчестера со скоростью вращения шпинделя 5400 он вполне приемлемый. Трансфер тоже довольно хороший и придется по вкусу многим любителям недорогих винтов. Правда, среднее время доступа довольно великовато и составляет целых 21,2 мс. Зато загрузка CPU очень низкая - всего 7%.



Seagate

Компания Seagate совершила мощный рывок в своем развитии и сейчас уже является полновластным лидером на рынке жестких дисков. Основными составляющими ее успеха стали передовые технологии, а также постоянно возрастающая скорость и емкость винчестеров. В нашей же сети оказалась средняя по весу рыбешка - 40-гиговая Барракуда.

Seagate Barracuda ATA IV 40 GB

По сравнению с прошлыми моделями, дизайн у новенькой Барракуды стал более традиционным, что объясняется удобством размещения внутренних амортизаторов и шумозащитных экранов. Поэтому внутренности рыбки находятся под надежной защитой толстых стенок и металлических пластин. Правда, из-за такого защитного панциря Барракуда иногда мучается от повышенной температуры, так что ее хозяин должен позаботиться о дополнительном охлаждении.

Точно же определить температуру позволяет встроенный термодатчик. По сравнению с прошлыми рыбками, значительно увеличилась плотность треков на пластине и записи данных на дорожке - на пластине у четвертой Барракуды может быть записано до 40 ГБ данных. А новый двигатель SoftSonic на гидродинамических подшипниках (Fluid Dynamic Bearing - FDB) может разгоняться до 7200 об/мин, но при этом оставаясь практически бесшумным (максимальный уровень шума - 2.4 Б). Размер буфера в 2 МБ тоже свидетельствует о серьезном нраве рыбки.

ОСНОВЫ

Жесткий диск состоит из четырех основных элементов: носителя, головок чтения-записи, позиционера (ставит головки на нужные дорожки) и контроллера (управляет элементами диска и отвечает за передачу данных). Данные хранятся на пластинах в виде дорожек, разбитые, в свою очередь, на сектора. Сектор, как правило, имеет объем в 512 байт и содержит коды коррекции ошибок. А совокупность дорожек, расположенных под головками на пластинах, называется цилиндром.

График чтения с диска говорит о хорошей скорости и высоком качестве поверхности пластин. Среднее время доступа составило 15,2 мс, что очень неплохо, учитывая повышенную плотность пластин. Загрузка процессора держится в районе 8,3%.

ПЛАСТИНЫ

Пластины – это диски из алюминиевого сплава или стеклообразного материала. На их поверхность нанесены несколько слоев магнитного и немагнитного покрытия, защищенного специальным графитом. Пластины закреплены на шпинделе, который вращает их с весьма высокими скоростями.

Western Digital

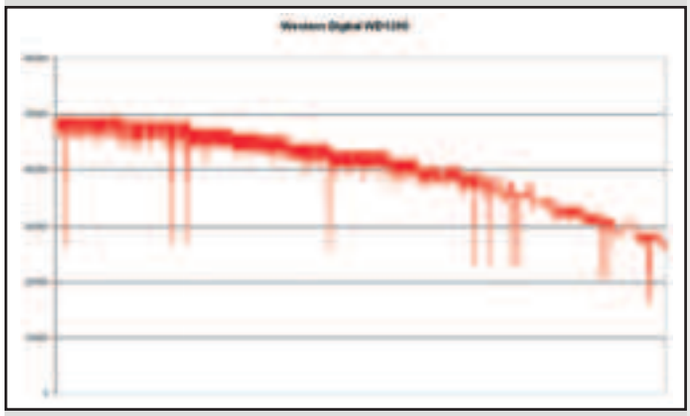
Винчестеры Цифрового Вестерна вызывают противоречивые отзывы у юзеров и продавцов. Одни считают, что это очень хорошие диски, а другие, вспоминая большое количество брака в дисках 2-3-летней давности, больше им не доверяют. Но с тех пор уже утекло очень много воды, поэтому на новую серию винтов следуют посмотреть незамутненным взглядом. Тем более, экземпляру, попавшему в наши цепкие лапы, есть чем похвалиться перед широкой публикой.

Caviar WD1200JB 120 GB

На сегодняшний день это самая производительная линейка винчестеров (WD1200JB) со скоростью вращения шпинделя 7200 об/мин.

Главное же отличие от прошлой модели на 120 ГБ (WD1200BB) в увеличенном объеме буфера. Теперь он составляет целых 8 МБ, что на порядок выше, чем у жестких дисков от других компаний (правда, поможет ли разросшийся буфер поднять общую производительность покажут тесты). К общей картине можно добавить фирменные технологии, обеспечивающие надежную защиту данных и крайне низкий уровень шума. В общем, становится очевидным, что на этот раз инженеры Western Digital поработали на совесть и чтобы убедиться в этом посмотрим на тесты.

Высокая скорость чтения наблюдается на очень большом участке поверхности диска, что только подтверждает наши предположения. Среднее время доступа вполне приличное и составляет 12,9 мс. Загрузка процессора при этом составляет 10,4%, что тоже не портит очень удачной картины.



СКОРОСТЬ

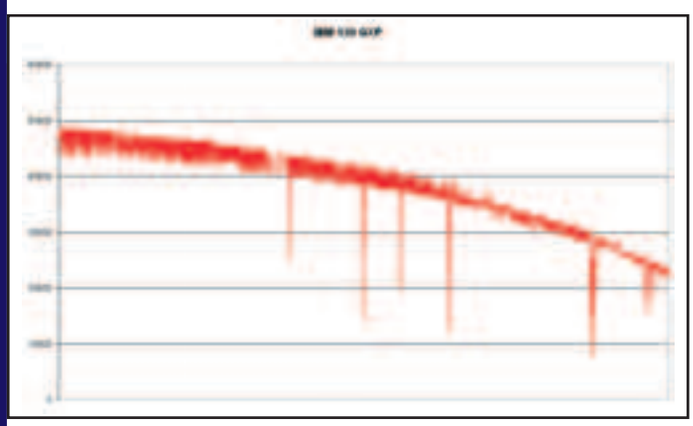
Скорость или производительность диска определяется несколькими параметрами. Одним из самых важных является плотность записи. Ее увеличение позволяет увеличить емкость и скорость передачи данных. Время доступа к данным тоже имеет немаловажное значение, но здесь сказывается целый ряд факторов. Дело в том, что помимо времени, необходимого для перемещения головки на нужную дорожку, существует время (латентность), затрачиваемое от выхода головки на заданную дорожку до появления под ней сектора с нужными данными. Увеличение скорости вращения позволяет повысить скорость передачи и понизить ту самую латентность. Впрочем, слишком резкого прогресса в этом компоненте не наблюдается, т.к. сказывается целых ворох проблем из-за повышенной мощности, тепловыделения, шумности и т.д. Другим важным параметром, влияющим на скорость, является объем буфера или кэш-памяти. Большинство моделей, выпускаемых сейчас имеют объем в 2 МБ, но тенденция на его увеличение все-таки наблюдается довольно явно.

IBM

Компания IBM хотя и утратила свои былые лидирующие позиции среди производителей винчестеров, но среди простых юзеров по прежнему имеет большой авторитет. Другие, наоборот, обжегшись один раз на серии дятлов (DTLA), больше с ее девайсами предпочитают не связываться. Мы же решили разобраться и посмотреть, как поведет себя, ожиревший на несколько десятков гигабайт, наследник тех «птичек».

IBM Deskstar 120GXP (IC35L120AVVA07-0) 123.5 GB

Эта линейка винтов имеет в своих стройных рядах винты с объемом от 20.57 GB до 123.52. Наш же гигант внешне практически не отличается от прошлых моделей, но внутри обзавелся более продвинутой «начинкой». К основным фишкам, помимо 7200 об/мин у шпинделя и кэш-буфера на 2 МБ, теперь можно отнести ан-



тиферромагнитное покрытие поверхности (позволяет записывать инфу гораздо плотнее (до 100 гигабит на квадратный дюйм)), переработанный «бортовой процессор», парковочная рампа (load-unload ramp) и «керамические» подшипники шпинделя. Еще следует отметить наличие фирменных технологий - Drive Fitness Test (DFT), температурный мониторинг, TrueTrak servo и систему форматирования No-ID sector formatting.

График линейного чтения с диска в очередной раз показывает, что со скоростью у «Голубого гиганта» все в порядке, а некоторая размытость, объясняется, скорей всего, увеличенной плотностью записи на антиферромагнитном покрытии. Среднее время доступа к диску (Average Access time) составило 12 мс, что тоже неплохой результат. Ну, а загрузка процессора на 9,3 % хотя и не лучший, но вполне достойный показатель для диска такого объема.

КОНТРОЛЛЕР

Контроллер основан на специализированном процессоре, оснащенным буферной памятью для хранения данных и ПЗУ. Его основными функциями являются защита диска от проблем с питанием, экономия энергии при отсутствии активности пользователя, а также реализация всех уровней протоколов интерфейса связи с компом.

Samsung

Прошлые жесткие диски от этой компании пользовались не слишком большой популярностью из-за недостаточной производительности. Однако, Samsung, видимо, учла все замечания и выпустила новую линейку винчестеров с улучшенными характеристиками. Один из них и побывал в нашей тестовой лаборатории. Итак, встречаем...

Samsung SV2011H 20 GB

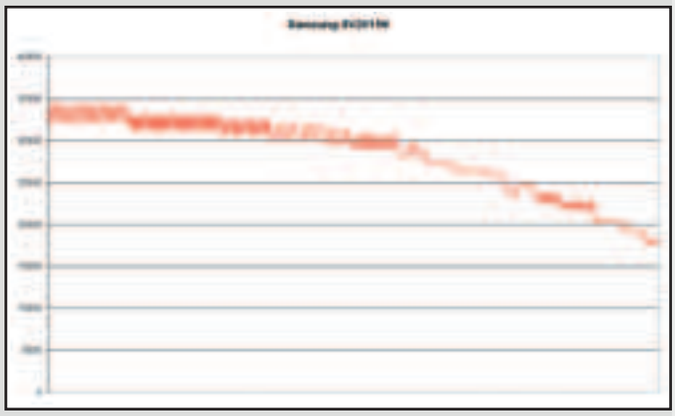
Эта бюджетная модель имеет скорость вращения 5400 об/мин и кэш-буфер на 2 МБ. Неплохо, для недорого винта. К тому же у этого жесткого диска имеются фирменные технологии защиты от ударов и других малоприятных вещей - SSB и ImpacGuard. Плюс довольно

ИНТЕРФЕЙС

Наибольшее распространение на сегодняшний день имеет интерфейс ATA (такие винчестеры участвуют и в нашем тестировании). Его основной принцип - параллельная передача данных по многожильному кабелю. Скорость такой передачи достигла значений в 133 Мбайт/с. Однако, в ближайшем будущем этот интерфейс грозит вытеснить другая разработка - Serial ATA (основанный на последовательной передачи данных). Помимо увеличенной скорости передачи данных, он позволяет подключать диски практически "вслепую" и допускает "горячую" замену. Также увеличена допустимая длина шлейфа до одного метра, вместо прежних 45 сантиметров.

низкий уровень шума при работе. В этом ему помогает еще одни технологии - SilentSeek и Noise Guard. Осталось только посмотреть, как проявит себя Samsung SV2011H в тестах и сделать окончательные выводы.

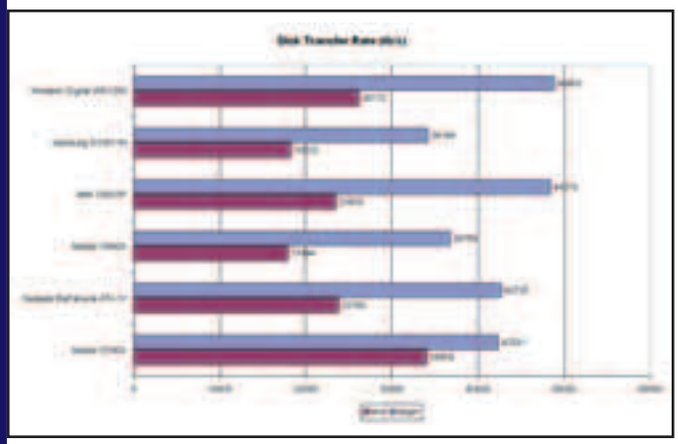
Хотя график линейного чтения с диска и не показал выдающихся результатов по скорости, но зато порадовал ровным трансфером и высоким качеством пластин. А это, безусловно, следует занести в актив разработчикам и инженерам винчестеров Samsung. Если они будут и дальше двигаться в том же направлении, то смогут вполне потеснить признанных грандов. За показатели среднего времени доступа им тоже можно дать медаль - оно составило лишь 14,7 мс :). А загрузка процессора держится на уровне 7,4%. Так что, у Maxtor D540X-4D появился реальный конкурент.



ФИНАЛЬНЫЕ ТЕСТЫ

Disk Transfer Rate

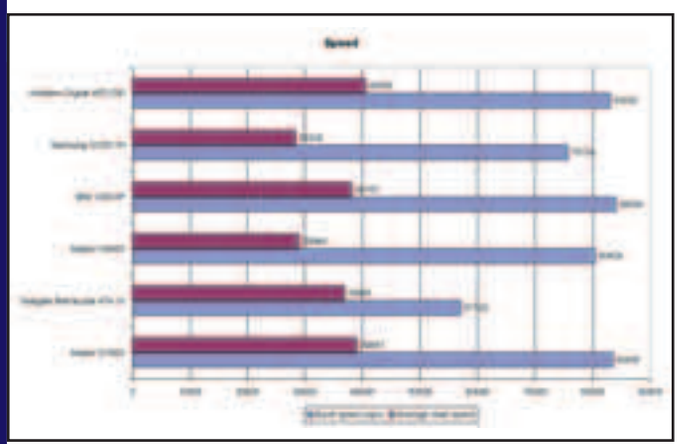
В этом тесте, показывающем производительность диска, определилась тройка лидеров. Ими стали, как ты уже успел догадаться, WD1200JB, IBM Deskstar 120GXP и Maxtor D740X-6L. Последний, кстати, сумел отличиться более ровным трансфером и более высоким показателем в конце диска. WD1200JB же порадовал рекордной скоростью в начале теста. Ну, а IBM Deskstar 120GXP показал всю свою мощь, которой, правда, не хватило для полной победы. Seagate Barracuda ATA IV оказался в золотой середине и, в целом, тоже продемонстрировал неплохую производительность. Maxtor D540X-4D же с



Samsung'ом SV2011H идут нога в ногу, но у Самсунга можно отметить более ровный и приятный график.

Speed

По средней скорости чтения WD1200JB удалось опередить всех своих конкурентов, включая IBM Deskstar 120GXP и Maxtor D740X-6L. Seagate Barracuda ATA IV опять идет в середине, не успевая за лидерами. Аналогичная картина наблюдается и у Maxtor D540X-4D с Samsung'ом SV2011H. В тесте же, симулирующим работу с реальным приложениями, быстрей всех оказался IBM Deskstar 120GXP, впрочем, WD1200JB и Maxtor D740X-6L отстали не намного. Удивляет, правда, низкий показатель четвертой Барракуды, который оказался даже ниже, чем у бюджетных моделей Maxtor и Samsung.

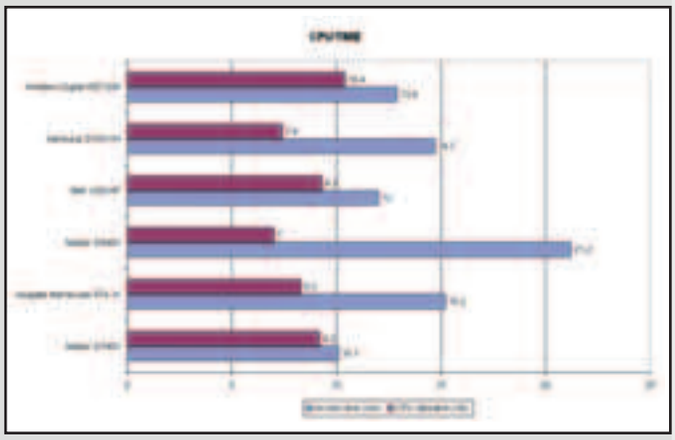


ГОЛОВКА ЗАПИСИ-ЧТЕНИЯ

Головка расположена над поверхностью пластины на рассмоянии около 10-15 нм. Головка чтения преобразует аналоговый сигнал в цифровой. Для этого используется специальный метод частичного отклика - (Partial Response Maximum Likelihood). Головка, так же как и пластины, защищена алмазоподобным графитом, что существенно снижает последствия непреднамеренной остановки двигателя. На сегодняшний день больше всего распространенны супермагниторезистивные головки (GMR), а им на смену, скорей всего, придут туннельные магниторезистивные (TMR).

CPU/Time

Экономичными требованиями к центральному процессору отметились винчестер от Samsung и Maxtor D540X-4D. Это, правда, объясняется более легкой «весовой категорией» и меньшей скоростью вращения шпинделя. Из скоростных участников нашего тестирования лучше всех в этом компоненте проявила себя, уже подзабытая, четвертая Барракуда. Что касается времени доступа, то тут несомненным чемпионом оказался Maxtor D740X-6L, за что честь ему и хвала :). Вторым в этом важном показателе является IBM Deskstar 120GXP, опередивший WD1200JB. Также нельзя ни заметить финишный спурт Samsung'а, показавший лучше время, чем основной конкурент - Maxtor D540X-4D.



Итак, какой вывод можно сделать на основе нашего тестирования? Мы сделали такой: жесткие диски – эта та технология, которой пока не пророчат никакой другой альтернативы, поэтому производители этих важнейших девайсов продолжают улучшать качество своей продукции, стараясь занять как можно больший сектор рынка. Нам от этого только хорошо – есть из чего выбирать :).

Карен Казарьян aka Kirion (kirion@winfo.org)

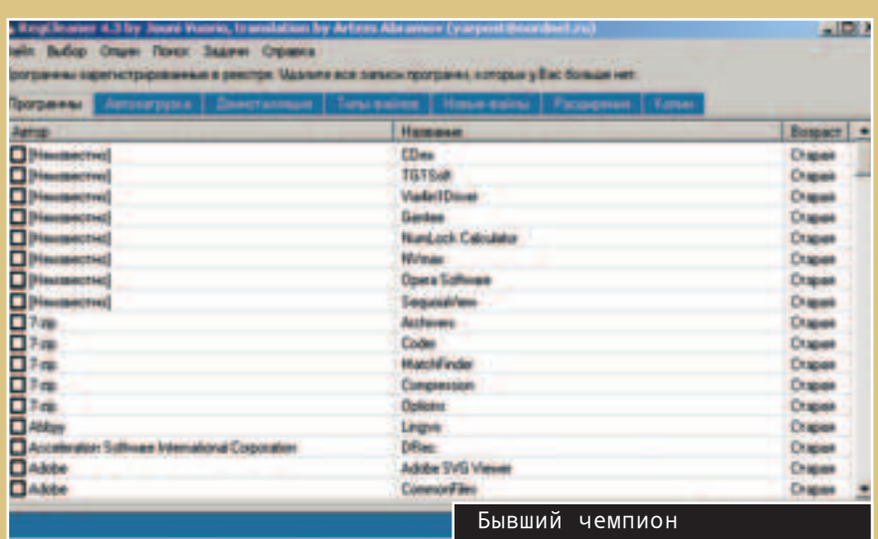
ТРЕБУЕТСЯ ЧИСТИЛЬЩИК

ТЕСТ ПРОГ-КИЛЛЕРОВ МУСОРА

«Черт, опять места на диске не хватает. Чем же я его забил? А что эта прога делает в автозагрузке? Так, залезем в реестр. Откуда эти записи? Я же удалил эту прогу два месяца назад. Почему здесь столько мусора? Мдя... сегодня будет большая чистка...». Бывали такие случаи? И что, чистил все руками? А винды потом не переустанавливал :). Нет, эта работа не для барина, тут слуги нужны. Что значит, нету? Ну, так уж и быть, поделюсь своими :).

ТРЕБОВАНИЯ К РАБОТНИКУ

Очень многие проги используют временные файлы. И куда они их только не кидают. А что реестр? Как же хорошо было, когда проги сохраняли свои настройки только в ini-файлы. Все опции были под рукой, а если удалил каталог проги, то и мусора не оставалось. Но пришел Билли и сказал: «Мы придумали реестр! Это очень удобный способ хранения настроек программ. А ну все быстро в реестр :)». И что теперь? Даже банальный «recent list» теперь хранят в реестре (кстати, это один из основных загрязнителей). А еще кривые инсталляторы, вечно оставляющие свои хвосты. А еще элементы activex - их ошибки, похоже, просто прописались в системе. Да и сами винды вносят долю ошибок, причем довольно большую. Чистить все это руками



Бывший чемпион

довольно стремно - можно запороть систему, да и не нужно это. Существует много прог, готовых тебе помочь. После долгих поисков я отобрал для себя два продукта, о которых сейчас и расскажу.

ПРОХОДИТЕ НА СОБЕСЕДОВАНИЕ

А начнем с System mechanic **(www.iolo.com)**. Удобная и многофункциональная программа. Все настройки механика разбиты на три части: файлы, система, Интернет. Нумбер ван: файлы. «Find and remove junk and obsolete files» - чистилка временных фалов. Обладает весьма гибкими настройками: тут и расширения, и какие папки включать/исключать, и удаление по времени последнего доступа, и куда перемещать мусор, и еще много всего. «Find and fix broken shortcuts» - кривые ярлычки имеются? Теперь их не будет. «Find and remove duplicate files» - что, сделал бэкап и забыл куда :), а места нету? Ну, посиди часик, погоди, механик тебе все найдет :). «Securely delete files and folders» - безвозвратное удаление файлов с винта. На рабочем столе появляется объект «Incinerator» - что-то вроде корзины, соответствующий пункт встраивается в контекстное меню. Перетащили - удалили, а если не надо - отключили. Пройдемся по закладке «System». «Clean system registry» - а вот и чистилка реестра. Ведет запись всех внесенных изменений, так что всегда можно сделать откат после того как переставишь винды :). Чистит очень даже хорошо, хотя и не весь мусор находит. «Windows startup manager» - добавляем и редактируем автозапуск, Msconfig - в отстой. Хотя Starter (codestuff.tripod.com) мне все же больше нравится. «Customize windows settings» - небольшой блок настроек системы. Если нет ничего лучше - может и пригодится (while true write (Всем ставить x-setup!); :)). «Remove invalid uninstaller information» - удаляет неверную информацию из «установки и удаления программ». «Safe installer» - а вот это очень полезная фишка. Делает снимки диска и реестра до инсталляции проги и после. Самое оно для подозрительных и шароварных прог. Осталась скромная закладка «Internet». Здесь нам предлагают «Ensure your privacy» - чистим хистори, печенье, recent files, etc. Ну и под конец осталось «Optimize internet and network speed» - можно протестить связь и установить нужный MTU (имеется в виду не пров, а maximum transmission unit). Чтобы совсем облегчить нам работу, в проге имеется визард и возможность работы по расписанию. В целом - приятный продукт, только один минус - хочет денег (ну, это поправимо, почаще ходи на nnm.ru - прим. Дронича).

Механик-профессионал

Дальше я хотел рассказать тебе о Regcleaner **(www.jv16.org)**. Эта стильная прога многими считалась лучшей по очистке реестра, и заслуженно. Но, зайдя недавно на сайт команды, я обнаружил их новую разработку: «jv16 power tools». Быстренько скачав, я увидел знакомый стильный интерфейс и кучу других фишек. Прога более свежая, да и реестр она чистит еще лучше! Будут ли выходить новые версии Regcleaner'а - пока неясно. Как оставалась версия 4.3, так и остается с начала года. Хотя я не буду горевать, если выход прекратится, поскольку замена получилась очень даже ничего.

Но пришел Билли и сказал: "Мы придумали реестр! Это очень удобный способ хранения настроек программ. А ну все быстро в реестр :)".

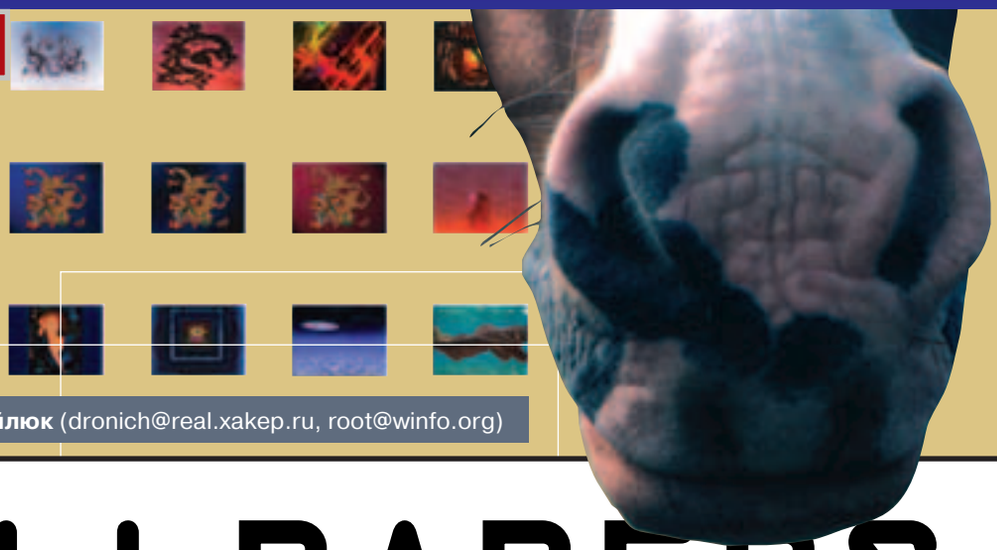

Новый чемпион?

Что же нам предлагают разработчики? Прежде всего топаем в настройки и ставим русский язык, а то можно и не разобраться. Очистка реестра: ну, это практически Regcleaner, только интерфейс немного другой. Тут можно увидеть список всех хвостов программ в реестре (мусора там полно). Думаю, тебя сильно удивит его длина. Автозагрузка, содержимое «Установки и удаления программ», содержимое менюшек «Создать», «Открыть», «Найти», контекстные меню для разных типов файлов. Смотришь и правишь, не бойся, если что - сделаешь откат. Залезем в список типов. Где видишь неопределенное значение - смело удаляй строку. Если заглянешь в «Инструменты» - найдешь долгожданную очистку. Настраивай, как считаешь нужным, и запускай. Результат тебя сильно удивит. Ну, чего там, всего-то 200 ошибок, какие мелочи :). Только не переборщи с удалением: часть ошибок отмечается красным; как ты думаешь, зачем? А вот исправление реестра практически бесполезно - до Windoctor от Нортона ему очень далеко. Само собой, прога ведет историю изменений. Можно восстановить копию, а можно объединить с существующей. А что у нас с очисткой диска? На первый взгляд, возможности поиска велики, но System mechanic с этой задачей справляется все же лучше. Наверное, сказывается, что это бета; надеюсь, в будущем этот раздел станет солиднее. Хотя и сейчас есть любопытные фичи: просмотр id3-tag, дополнительные данные для рисунков. Зачем-то существует отдельный блок для временных файлов, причем какой-то невменяемый: задаем папку, из которой все будет удаляться. И зачем? Таких непонятных фишек в программе достаточно. Например, профили пользователей с возможностью задать пароль. Или удаленное администрирование сетевых компов с установленной прогой. Господи, тут даже чат есть! Подозреваю, что только разработчики им и пользовались. Хотя есть и весьма перспективные, например, консоль команд и возможность создавать пакетные файлы (если интересно - почитай хелпу). Я надеюсь, что горячие финские программисты одумаются и поработают над более нужными функциями. Но, несмотря на все ляпы, я считаю Power tools лучшим чистильщиком реестра: все-таки сказывается база Regcleaner. Над остальными функциями пока работать и работать. Хорошо - хоть бесплатная.

Но, несмотря на все ляпы, я считаю Power tools лучшим чистильщиком реестра: все-таки сказывается база Regcleaner. Над остальными функциями пока работать и работать.

ПОЗДРАВЛЯЮ, ТЫ НАНЯТ

Какую же программу выбрать? Ну, power tools надо ставить по-любому - лучшей чистилки реестра ты не найдешь. У меня стоит и System mechanic, но я видел и другие достойные продукты по очистке диска и сейчас напряженно думаю: качать новую версию или искать что-то другое. Тем более, что я устал наблюдать версии 3.7b, 3.7d, 3.7e и так далее. Прямо «The bat» какой-то :). Ты можешь повлиять на мой выбор и выбор других читателей - пиши. «Нас уже много - кирпичи тяжелы». Удачи!



Андрей «Дронич» Михайлюк (dronich@real.xakep.ru, root@winfo.org)

WALLPAPERS

СЕЗОН ОХОТЫ

Буквально намедни поспорили мы с Ильичем на тему десктопа. Он страшным голосом вопил про совершенство Active Desktop'а и необходимость тотального внедрения Flash-интерфейса в массы, а я защищал индивидуальность любителей обоев, коим всю жизнь являлся и являться буду. Поубивали бы, наверно, друг друга, но вовремя пришли к компромиссу – делать флэшки прозрачными и подкладывать под них качественные обои :). Уговор дороже денег, так что сегодня с меня рассказ про злачные места, где wallpaper'ы лежат.

http://www.digitalblasphemy.com/

Обзор начинается с этого сайта не случайно. Цифровое богохульство (именно так переводится с саксонского наречие Digital Blasphemy) царит тут уже который год, продолжая совершенствоваться. К слову, парочка обоев на космо-астероидную тематику лежит у меня на винте аж с Y2K-1. Новые работы появляются не так часто, но зато качеством поражают - от банально-постного 3D не осталось и следа. Правда, за мастерство нужно платить, хотя все совсем не так страшно: основные галереи доступны к всеобщему просмотру и скачиванию, а простым смертным запрещено качать только монстроидальные wallpaper'ы, превышающие по площади 1920000 квадратных точек... в смысле 1600*1200 :))). Но, по совести говоря, насмотревшись на тамбнейлы платных обоев, хочется подобрать слюнки и отдать мерзавцам 25 бакинских, лишь бы все это стало ТВОИМ :). Тем более, что платникам доступны зипованные галереи и сидючок с итогами года... Мечты, мать их...
Из полезностей для всех стоит особо отметить разнообразные голосования (итоги главного из них лежат прямо на первой странице), user gallery (место, куда можно положить свой первый кубик в Bryce 3D) и смачные туториалы для начинающих тридэшников от автора сайта.

Плюсы: *качественные весчи, возможность поучиться, четкое распределение обоев по популярности.*
Минусы: *самое сладкое стоит денежек, обои от DB стоят у каждого третьего кулхацкера.*

http://www.digitalblasphemy.com/

http://www.earthshots.com/

Достойнейший сайт, но вот незадача - его хозяев согнали с хостинга за превышение трафика (немудрено с такой-то популярностью...). В свое время там реально было найти такие фотки, что все любители 3D лопались от зависти. Остается только ждать, когда они снова выползут в онлайн, потому что ТАКОГО в сети больше нет. Обидно.

http://www.3dwallpaperworld.com/

Если ты не слышал о проекте www.planet-3d.com, то пора проснуться и вспомнить, что эра 3D-графики давно наступила. Именно там тусуются аскетичные фанаты 3DS и продвинутые любители Брайса, меняясь моделями и идеями. Так, о чем это я?.. А, в общем, три-дэ-обойный-мир - это часть «Планеты 3D». Количество папирей не поражает, поражает количество шедевров среди них.

http://www.digitalblasphemy.com/

По крайней мере, вытащить меня из раздела скай-фай было до жути сложно - современное искусство пробило до самого мозжечка. Пугает поросль кустарщины, то и дело появляющаяся посреди профессиональных работ. Имхо, как-то несерьезно выкладывать папири новичков, первый раз нажавших на «рендер» вчера вечером, рядом с офигеннейшим кораблем Амидалы из SWI. Кстати, об Амидале и прочих: весь сайт просто помешан на Звездных войнах, так что фанаты могут найти не только трейлеры и кадры из фильма (которых везде в изобилии), но и (держись, братва!) зарендеренные 3D-модели кораблей и построек из фильма. Чума, однако!

www.visualparadox.com

Плюсы: *красивое 3D, кругом профи.*
Минусы: *смешанность работ и помешанность на SW.*

http://www.3dwallpaperworld.com/

Обалденный сайт! Рекламы почти нет, а картинок - залейся. 3D'шные и фотообои идут отдельными разделами сразу, причем первые впечатляют больше - из двух разделов Real World, посвященных ландшафтам и зверушкам соответственно, можно выудить тучу симпатичностей. Меня сразу убили наповал вылезающий из кустов раптор (который динозавр, а не антикомарин :)) и муравейник в день субботника изнутри. Автор слегка злоупотребляет дельфинами (оно и понятно, один раз смоделировав, можно просто менять фон :)), но это простительно. А вот за раздел Humorous просто нечеловеческое спасибо. Я-то, дурак, раньше думал, что юморные обои - это картинка с фоменко.ру, растянутая на весь экран. Ни фига подобного! Смеяться до слез ты будешь вряд ли, а вот обеспечить себе приятное настроение на весь день - это пожалуйста. А самое главное - в наше тяжелое время все галереи абсолютно фришные, а картинки доступны в самых популярных разрешениях - от 640x480 до 1024x768.

http://www.beautifulwallpapers.com/

Плюсы: *почти нет рекламы, оригинальные обои, халява :).*
Минусы: *не всегда качественный рендер картинок.*

http://www.visualparadox.com

Вот что могут сделать американцы для американцев :). В изобилии обои, напоминающие сюжетом праздничные открытки, все остальное раскидано по категориям, понять назначение которых временами сложно. К примеру, при клике на «еротишные обои» меня сначала спросили о возрасте, а потом так запросто отправили на какой-то порнушный рейтинг :). Вот уроды! Еще наповал сразило качество. Ребята, сделанные на мыльнице, а после отсканенные фотки не называются обоями! Нас дурят, однозначно! И ладно бы просто дурили, на нас еще и наживаются. Три рандомных попапа и баннерное обрамление в два слоя - вот цена одной картинки! Нехорошо. Особенно если этого стоит эмблема Найка (да, незатейливая галочка на черном фоне ;)) 1024x768 или любительская фотка The Two Towers (ладно бы после взрыва, сошло бы за подвиг папарацци). Не наш сайт, но, вооружившись срезателем баннеров и попапов, вполне можно копаться в поисках обоев для подруги - тетошные разделы на сайте неповторимы.

Плюсы: *эксклюзив для теток.*
Минусы: *реклама, качество, отношение к юзеру.*

http://www.beautifulwallpapers.com/

Плюсы: *оригинальность, эксклюзивность, дизайн.*
Минусы: *бессистемность, бесконтрольность, качество.*

http://www.wallpapers.ru/

http://www.wallpapers.ru/

Самый необычный сайт обзора. Это не тематическая коллекция и не мастерская одного автора - это своеобразный элитный рейтинг, попасть в который просто, а удержаться очень нелегко. Все обои живут на сервере не больше трех месяцев, после чего либо успешно удаляются, либо включаются в так называемый арт-пак - сборник папиров «по итогам». Из-за такого специфического устройства на сайте нет и не будет разделения картинок по темам, хотя рейтинги по популярности и свежести практически компенсируют этот недостаток. Авторы популярных wallpaper'ов постоянно зажигают в форуме, где можно высказать им свое почтение или попросить подучить уму-разуму.
Очень приятное впечатление оставил дизайн - из мелких превьюх при наведении мыша вырастают крупные, в уголке постоянно маячат «папир дня» и «папир часа», постоянно обновляется столбик со свежатиной. Лепота, одним словом. Если добавить еще и рассылку самых-самых картинок почтой, получается просто райская обстановочка. Просто обязан ливануть чайную ложку гуана в этот компот - из-за отсутствия правил по оформлению обоев временами случаются досадные обломы. То картинка супер, а размер только 800x600. То по превьюхе смотришь - зашибись какая байдовина намалевана, а станешь качать - она ДжиПЕГом пожата на 50 процентов :(. Спасает только форум, где можно оставить заявочку автору на требуемые качество и размер картинки. Только не факт, что он примет ее к сведению :(.

Плюсы: *количество, творческий процесс поиска :).*
Минусы: *дизайн, качество, сортировка, реклама.*

http://www.pora.ru/

http://www.pora.ru/

Глядя на этот сайт, можно сказать только одно слово: «Много!». То есть картинок действительно завались, среди них встречаются вполне порядочные, а раздел эро-обоев состоит вообще из отборных шедевров. Только вот... баннеров куча, причем впихнуты они куда только можно, дизайн отсутствует как класс, а картинки показывают по четыре штуки в сильно рандомизированном порядке. Я, конечно, понимаю, что поделить раздел «Природа» на три раздела (горы, моря, долины) - это жутко сложное занятие, и лучше валить все в кучу ;). В итоге имеем сайт-мечту Добрянского: сидишь, копаешься, временами находишь классные вещи. Рекомендуется только Феде :).

Плюсы: *много и на удивление красиво.*
Минусы: *не замечено.*

http://www.desktopwallpapers.ru/

http://www.desktopwallpapers.ru/

Самый настоящий ведомственный склад советских времен. В смысле есть ВСЕ и МНОГО :). 25 (двадцать пять!) больших разделов, в каждом из которых наблюдается по 40-50 страничек с тамбнейлами - вот неписаный стандарт для wallpaper-сайта. А если посмотреть, какими темпами идет обновление (по 10-20 картинок еженедельно), то сайту можно смело пророчить большое будущее. Навигация располагает не к просмотру максимального числа баннеров (хотя и их хватает,

http://www.desktop-fx.com/

http://www.xwx.ru/

но связке Opera+Outpost они вполне по зубам :)), а совсем наоборот - к удобному серфу по галереям. Есть и простые переходы от страницы к странице, есть непосредственный выбор галереи и три вида сортировки. Качество картинок на высоте, что весьма странно - лично я просто не представляю, где можно достать четыре тысячи высококачественных изображений (диск «4000 высококачественных изображений» с Горбухи просьба не предлагать :)). Кстати, на сайте присутствует очень полезный раздел для маньяков - «Большие обои». Они действительно БОЛЬШИЕ - если циферка 3072x2048 кого-то и не устраивает, то разве что обладателей плазменных панелей 50» :). В остальных разделах максимальная граница - 1024x768, но большинству и этого хватит (а мне не хватает :(, буду жаловаться в ООН! - прим. UXGA-монитора Дронича).

http://www.pristavki.com/gallery.php

Это были гиганты, которые подкупают либо количеством (как Desktop Wallpapers), либо диким эксклюзивом (как Blasphemy). А в сети, помимо них, встречаются и более мелкие рыбешки, вполне достойные твоего визита.

http://www.desktop-fx.com/

Единственный сайт, на котором удалось найти не обои, а текстуры, пригодные для размещения на десктопе (куда там кольчуге и прочим пузырям до фрактальных мазилок ;)). Хотя и обоев тоже хватает, встречаются очень оригинальные (см. скрин).

http://wallpapers.boom.ru/

http://www.xwx.ru/

Еще один склад, только поменьше. Понравился исключительно приятными автообоями и отсутствием рекламы (один баннер - это разве реклама? :)).

http://www.pristavki.com/gallery.php

Да здравствуют обои из гамесов! Тут их хватит на всех. Неудобная навигация вполне окупается количеством картинок, выбраться из раздела ArtWorks вообще нереально (в хорошем смысле :) - там просто обои красивые).

http://wallpapers.boom.ru/

http://wm-design.com/wp/

Частная коллекция вполне сносных папирей. Несмотря на минимальное количество картинок в категориях, глаза все равно разбегаются. Если бы не дизайн с мерцающим бэкграундом, все было бы пинцетно.

http://wm-design.com/wp/

Совсем скромная коллекция, зато обои отборнейшие - не хочется выбирать, хочется сразу ставить :). К тому же на сайте туча инфы для вебдизайнеров и сочувствующих, но это скорее к Донору, в Креатив :).

ilich (ilich@winfo.org)

IE-Desktop

FLASHMAILER

Как часто, парень, ты пользуешься мылом? А как часто при этом ты пишешь по одним и тем же адресам? И как ты это делаешь? Дай-ка угадаю, ты каждый раз ручками запускаешь какую-нибудь прогу для мыла и потом опять же ручками набиваешь там чей-то мыльник :). Ну, в крайнем случае лазаешь по адресной книге. Не скучно ли? Я так и знал! Надо бы этот процесс автоматизировать. Давай грузи наш флешевский ролик для обоев, будем ваять mailer. Загрузил? Ну, тогда поехали.

СЕСТРА, НАРКОЗ!

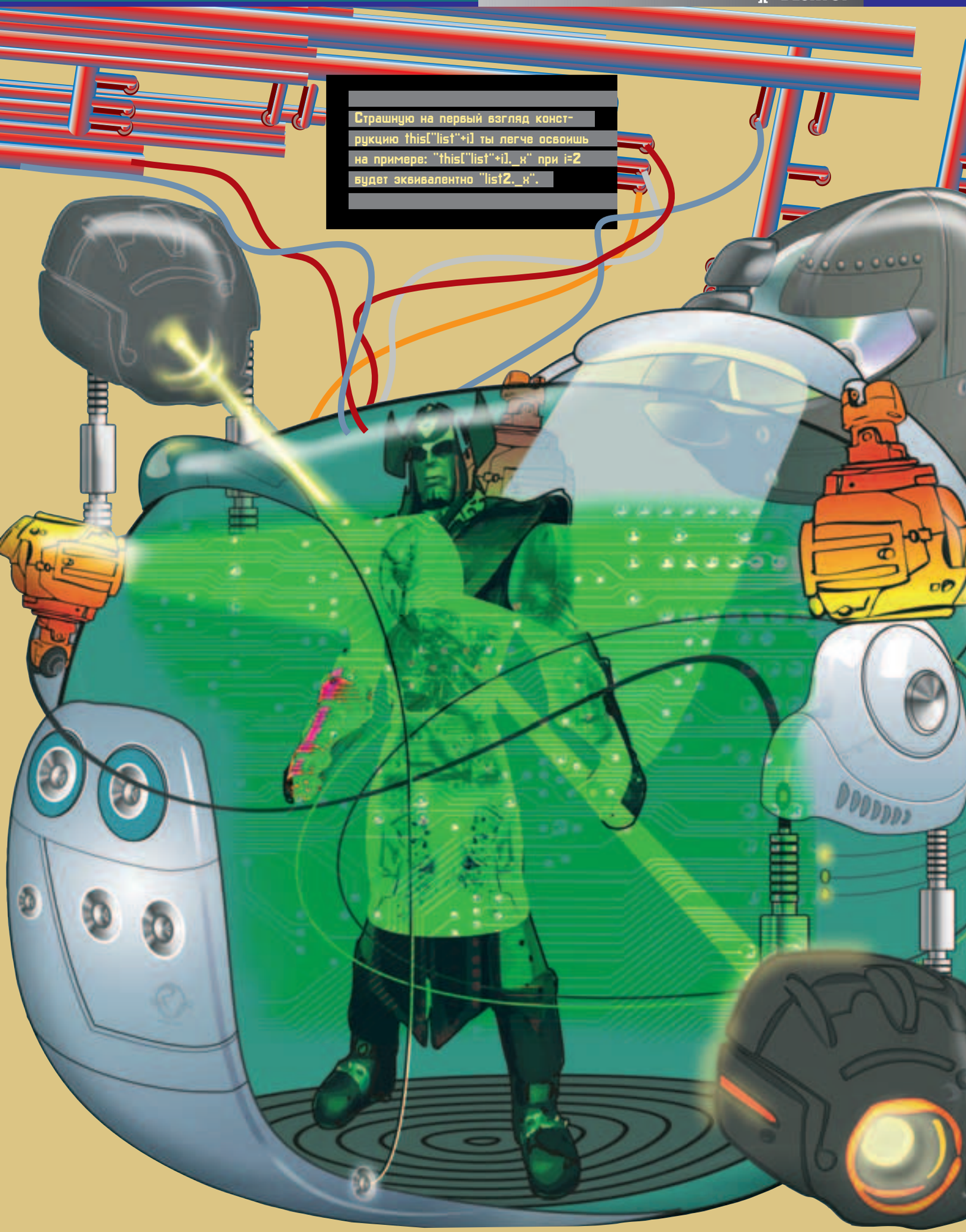
Для начала стоит поиметь побольше свободного места. Дави Ctrl+M и ставь высоту видеофрагмента 700 pt. Заходи сразу в редактирование символа «Main». Нарисуй текстовое поле шириной 500 pt. В панели Параметры Текста для этой строки все должно быть так: тип - Dynamic Text; Single line; имя переменной - «text»; напротив Selectable (Выбираемый) флажок убран. Дави F8 и загони эту строку в кнопку с именем «B - Link». В этой кнопке поставь строку так, чтобы центр кнопки был в левом верхнем углу строки. Первый кадр растяни еще на три и нарисуй в четвертом кадре прямоугольник так, чтобы он полностью закрывал строку (у меня при размере шрифта в строке 20 прямоугольник 500 на 30).

Если ты хочешь, чтобы обновления текстовика отслеживались постоянно, а не только во время загрузки клипа, то стоит использовать событие enterFrame.

Кнопку «B - Link» помещаем (выходи из ее редактирования, выделяй ее и дави F8) в клип «C - List» и в нем располагаем ее так же, как до этого ставили строку в ней самой, т.е. центр клипа в левом верхнем углу кнопки. Все это позиционирование делается для того, чтобы потом при помощи ActionScript можно было клип «C - List» располагать на экране предельно точно. Для кнопки мути скрипт (надави на ней правой половинкой мышки и выбирай в выпавшем меню пункт Операции или Actions):

```
on (press) {
    getURL («mailto:»+text);
}
```

Не очень трудно догадаться, что переменная «text» будет содержать чей-то E-mail адрес :).
Короче говоря, при нажатии «B - Link» вызовет твое почтовое приложение по умолчанию и в поле «кому» в новом письме поставит мыльник из переменной.



Страшную на первый взгляд конструкцию this["list"+i] ты легче освоишь на примере: "this["list"+i]._x" при i=2 будет эквивалентно "list2._x".

КТО НЕ РИСУЕТ, ТОТ НЕ...

Необходимо сделать маленькую, но красивую и удобную кнопочку, которая впоследствии будет вызывать меню с мылами. Советую особо не изощряться с рисованием, а нарисовать простую рельефную пимпу. Эффект объемности достигается при помощи таких типов заливок, как Radial Gradient и Linear Gradient (см. панель Заливка или Fill), и модификатора Gradient Transformation инструмента Paint Bucket (соответственно, модификатор Трансформация Заливки инструмента Заливка в русском Flash'е). Нарисуй кружок 40 пикселей в диаметре. Преобразуй его в кнопку «B - MailStart». Поиздевайся над его заливкой и сделай ее выпуклой в первом и втором кадрах (красивее выглядит, когда эти два кадра чуть-чуть отличаются, например, толщиной или цветом контура кружка) и вогнутой в третьем. Главное, не забывай делать у кнопок кадр hit. У одного моего знакомого недавно случилась беда: сделал кнопку, сделал ее красивую и все такое, но из-за отсутствия чего-либо в четвертом кадре она просто-напросто не реагировала ни на какие движения мыши. Обидно было.

Не менее необходимо также сделать кнопку для закрытия меню. Форму и размер этой кнопки выбираем, соображая при этом, где мы эту кнопку разместим. Не забывай также, что на экране появится еще меню мыльников. Давай забацаем ее горизонтально, дабы потом разместить над меню. Рисуй длинный прямоугольник с выразительным крестиком справа, пиши на нем «Close» и делай из всего из этого символ кнопки «B - MailClose». Ты не думай, что я над тобой издеваюсь, придумывая какие-то странные имена для символов (имена кнопок начинаются с «B», имена клипов - с «C»). Просто, по-моему, гораздо удобнее и быстрее работать с библиотекой во Flash'е, когда все символы упорядочены по функциональному признаку. У нас уже их там достаточно много, чтобы глаза сбились в кучу, а с мозгом произошел полный коллапс при попытке отыскать нужный символ без должной сортировки. Советую также соответственно переименовать все старые символы, имена которым давались еще в первых сеансах, или распихать их по папочкам (глаза тогда не разбегаются и функционируют согласно инструкции).

Вспомни теперь, как ты делал кнопочку «B - MailStart». Точнее, как ты делал заливку. Сделай новый клип «C - Fon». В нем ровно в центре рисуй квадрат со стороной 40 px с закругленными приблизительно на 15 точек краями (обрати внимание на модификатор инструмента Прямоугольник). Заливку у квадрата сделай точно такую же, как и у кружка в первом кадре в кнопке «B - MailStart». Этот клипушник мы поюзаем как фон для меню.

И последний символ на сегодня - клип «C - Mailer». Создавай его, заходи в его редактирование и глотни пивка, ибо сейчас будет жарко.

ЖАРКО :)

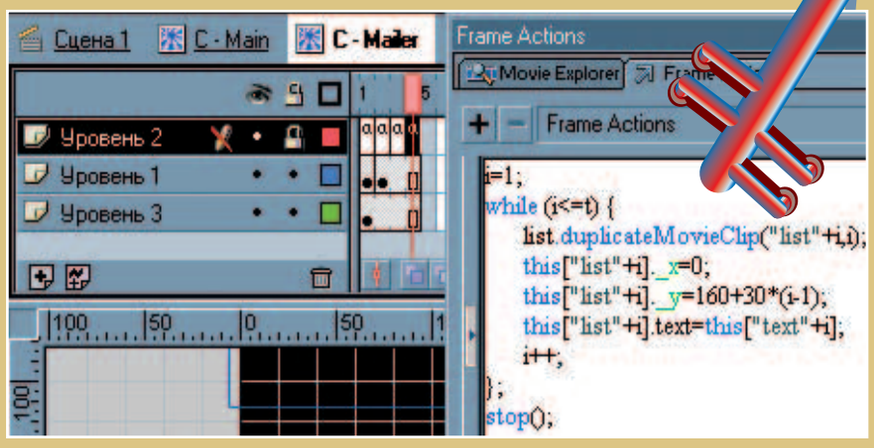
Здесь у нас будет замут из четырех кадров и трех слоев. Не напрягайся, все сделаем медленно и понятно.

Первый кадр у нас будет для состояния, когда пользователь, т.е. ты, меню не видит. Не потому, что смотрит не в монитор, а потому, что меню просто нет. Первые четыре кадра верхнего слоя делай отдельными ключевыми кадрами. В первом из них ставь команду stop(). Вообще это удобно, когда все скрипты для кадров располагаются в отдельном слое (как правило, это самый верхний слой). Так вот, когда клип начнет проигрываться, он благодаря команде stop() остановится в первом кадре, в котором мы нарисуем отсутствие меню, т.е. просто поставим во второй слой кнопочку вызова меню. Учитывая будущее расположение флешки на твоем Рабочем столе (правый верхний угол, если помнишь), советую расположить кнопку справа, как можно ближе к краю экрана. Точные координаты объекта можно задать в панели Info. Поставь там X=460 и Y=160. Заметь, что координаты символа на Рабочей области в этом случае определяются не центром символа, а левым верхним углом его изображения. Для кнопки ваяй скрипт:

```
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);
    };
    gotoAndPlay (2); //идем дальше
}
```

Ну, здесь тебе должно быть все понятно :). Мы, как и раньше, делаем над кнопкой искусственный курсор. Оператор gotoAndPlay (2), после которого стоят немногозначные комментарии, при нажатии кнопки отправляет нас ко второму кадру :).

Во втором кадре на второй слой пихай символы «B - MailClose» и «C - Fon».



Клип «C - Fon» ставь туда же, куда ставил «B - MailStart» в первом кадре. В панели Instance дай ему имя «fon». «B - MailClose» ставим ровно над клипом фона (X=0; Y=125). Кадр с этими двумя символами растяни (не скопируй, а именно растяни!) до четвертого кадра, т.е. так, чтобы он был и во втором, и в третьем, и в четвертом кадрах.

Во второй кадр слоя скриптов вбивай:

```
if (fon._width<500) {
    fon._xscale=fon._xscale+40;
    fon._x=500-fon._width/2;
}else if (fon._height<(t*30)) {
    fon._yscale=fon._yscale+40;
    fon._y=160+fon._height/2;
}else gotoAndPlay(4);
```

А в третий поставь gotoAndPlay (2), т.е. ссылку обратно на второй кадр.

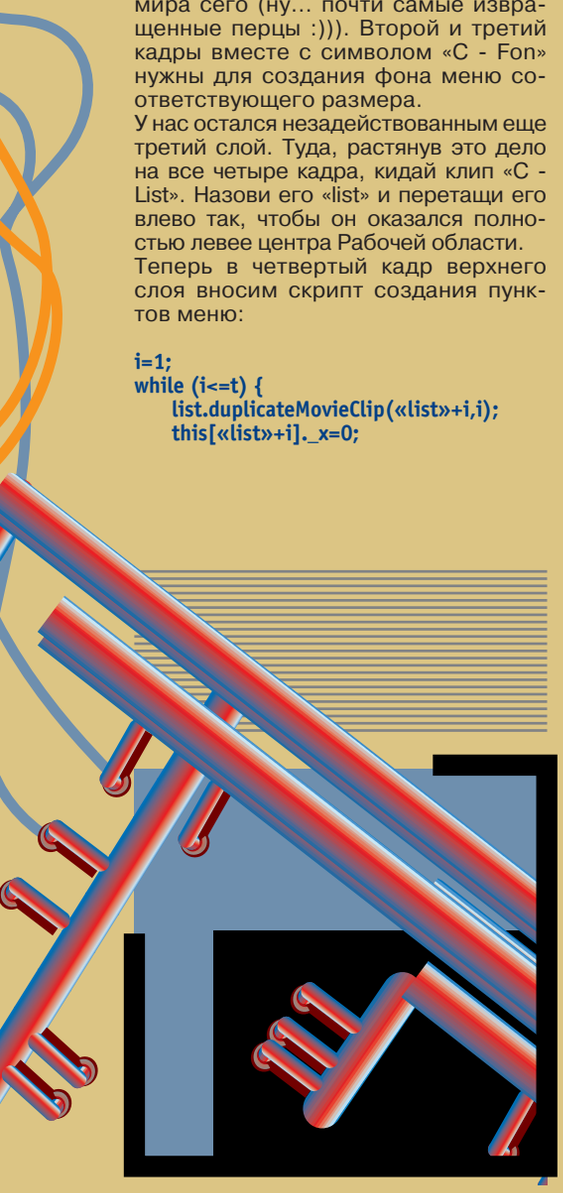
Все это делает вот что: клип «fon», а то есть наш квадрат с закругленными краями, будет растягиваться вначале вширь (до ширины в 500 px), а потом в высоту (до высоты t*30, где t - это количество мыльников в меню, а 30, как ты помнишь, это высота кнопки «B - Link»).

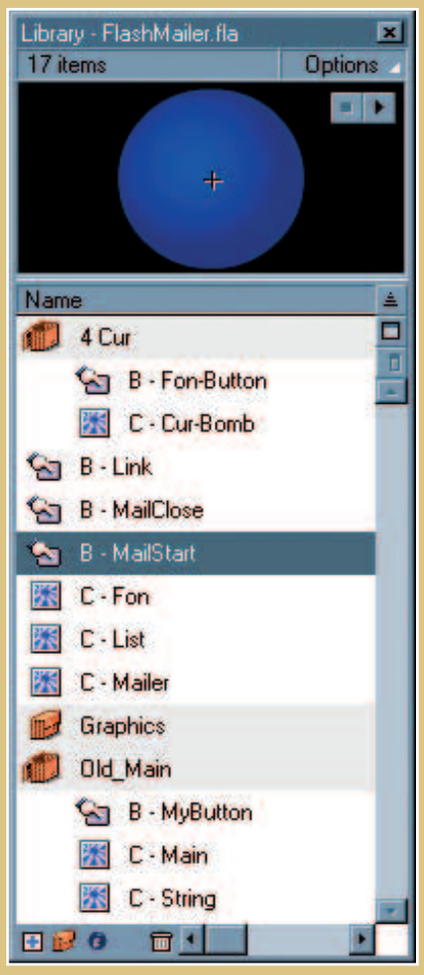
Сечешь, про что я? А я про то, что мы с тобой самые извращенные перцы

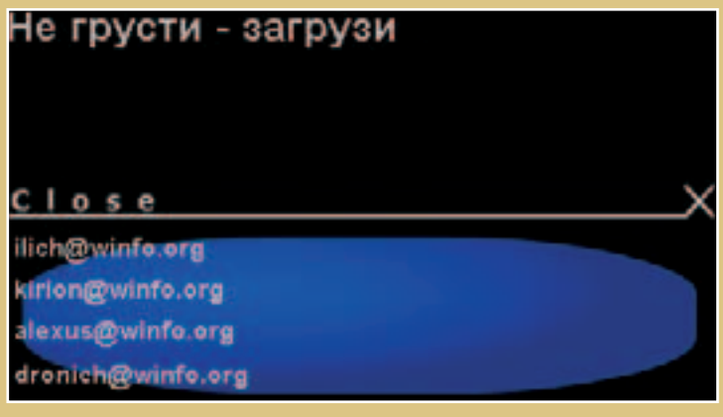
Сечешь, про что я? А я про то, что мы с тобой самые извращенные перцы мира сего (ну... почти самые извращенные перцы :))).

мира сего (ну... почти самые извращенные перцы :))). Второй и третий кадры вместе с символом «C - Fon» нужны для создания фона меню соответствующего размера.
У нас остался незадействованным еще третий слой. Туда, растянув это дело на все четыре кадра, кидай клип «C - List». Назови его «list» и перетащи его влево так, чтобы он оказался полностью левее центра Рабочей области.
Теперь в четвертый кадр верхнего слоя вносим скрипт создания пунктов меню:

```
i=1;
while (i<=t) {
    list.duplicateMovieClip(«list»+i,i);
    this[«list»+i]._x=0;
    this[«list»+i]._y=160+30*(i-1);
    this[«list»+i].text=this[«text»+i];
    i++;
};
stop();
```







Объясняю. Тело цикла while повторяется t раз. Штучка list.duplicateMovieClip(«list»+i,i) создает копию клипа «list», задает ей имя «list»+i и располагает ее на i-ом уровне. Страшную на первый взгляд конструкцию this[«list»+i] ты легче освоишь на примере: «this[«list»+i]._x» при i=2 будет эквивалентно «list2._x». Понятно? Так вот, вновь созданным клипам мы присваиваем такие координаты, что они выстраиваются друг под другом ровно над уже растянутым мувиком «C - Fon». Помнишь, у клипа «C - List» в кнопке было динамическое текстовое поле с именем «text»? Вот именно в него и заносится теперь значение переменной this[«text»+i].

Внутри символа «Mailer» осталось только одно - доделать кнопочку «B - MailClose». Она должна не просто возвращать нас к первому кадру, но и уничтожать все эти копии клипа «C - List», которые мы тут наделали. Вводи для нее:

```
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);
    };
    i=1;
    while (i<=t) {
        _root.main.mailer[«list»+i].
                        removeMovieClip();
        i++;
    };
    gotoAndStop (1);
}
```

Поясню тут лишь то, что mailer[«list»+i].removeMovieClip() при i=1 сделает то же, что и «mailer.list1.removeMovieClip()» - замочит клипушник «list1».

ЗАГРУЖАЕМ ПОТИХОНЬКУ

Выходи в редактирование клипа «Main» (или, если ты внимательно читал, уже «C - Main» :)). Выноси на рабочую область наш «C - Mailer» (если ты создаешь какой-либо символ через «Конвертировать в символ», т.е. через нажатие F8, то он уже есть у тебя на Рабочей области и, следовательно, второй раз его туда тащить вовсе необязательно). Ставь его так, чтобы его центр совпадал с центром Рабочей области клипа «C - Main». Получится так, что кнопочка вызова меню окажется чуть ниже текстовых полей бегущей строки.
Дай клипу имя «mailer» и задай для него скрипт:

```
onClipEvent (load) {
loadVariables («mail.txt», this);
}
```

Ну, это ты знаешь. Только вот что еще. Если ты хочешь, чтобы обновления текстовика отслеживались постоянно, а не только во время загрузки клипа, то стоит использовать событие enterFrame. Не надо будет заботиться об обновлении всей страницы Desktop'а при изменении текстового файла. Зато на слабых машинах при использовании enterFrame появятся ощутимые тормоза.
Кстати, о текстовом файле. Там же, где лежит флешка, создавай текстовик «mail.txt», в который набивай мыльники. Только набивай не просто так. Ты, наверное, помнишь, что оттуда грузит Flash. А Flash из этого текстовика грузит не что иное, как переменные, причем у этих переменных есть уже забитые для них имена. Помнишь переменную t, которая давала общее количество мыльников? Так вот, здесь она должна быть обязательно. Все E-mail адреса, которые ты хочешь увидеть на своем Рабочем столе, должны быть присвоены в качестве текста переменным «text1», «text2», «text3» и т.д. В текстовике присвоения переменным их значений разделяются символом «&». В нашем случае в файле лежит строка «t=4&text1=ilich@winfo.org&text2=kirion@winfo.org&text3=alexus@winfo.org&text4=dronich@winfo.org».

Alexys (alexys@winfo.org)

UPDATE

СЕРВИСПАКИ К WIN2K

Почти сразу после нахождения очередного бага Microsoft выпускает отдельные модули исправления, так называемые Hotfix'ы. Наиболее важные из них впоследствии проходят реальный тест и попадают в Service Pack'и. Выпускаются хотфиксы для конкретных версий виндов (не стоит ставить хотфикс для Win2k SP1, если стоит уже Win2k SP2). Еще существуют такие штучки, как модули коррекции системы защиты (Security patches). Как уже понятно из названия данных заплаток, их назначение – повышение безопасности работы виндов. Все виды заплаток для винтукея свалены на http://support.microsoft.com/support/servicepacks/windows/2000/win2000_post_sp2_hotfixes.asp, их оперативная установка очень желательна.

Риск, связанный с установкой пакета Service Pack или отдельного обновления, всегда должен быть меньше, чем риск потери данных в случае отказа от их установки. Поэтому рекомендую внимательнее читать наш журнал и перед установкой обновления отвечать на вопросы:
1) решит ли проблему данное обновление и уместно ли оно вообще? (самый главный вопрос :))
2) есть ли зависимость обновлений от запуска/остановки каких-либо служб, функций или установленных компонентов? (по опросу друзей)
3) не может ли обновление вызвать проблемы, которые в дальнейшем приведут к полному краху системы? (очень актуально для отпираченных систем - у Кириона после очередного хотфикса винды очень хотят активации на сайте Майкрософта :) - прим. Дронича)

Service Pack 1 для Win2k

Что приятного сделали мелкомягкие в двухтысячных, так это облегчили и сделали удобной установку своих же заплаток на систему :). Update.exe отныне не требует наличия дистрибутива при установке апдейтов, в отличие от того же Windows NT 4.0.
Service Pack 1 для винтукея вышел почти сразу после самой операционки, но, несмотря на это, содержит порядка 300 обновлений, нацеленных на исправление всевозможных багов многих компонентов виндов, предотвращение проблем с памятью и механизмом прерываний и т.п. Такое ощущение, что мелкомягкие знали о своих недоработках, раз так быстро выпустили первое собрание пополнений :). В SP1 устранена проблема разрыва связи после выхода компьютера из «спячки», исправлены некоторые ошибки JScript и JVM (виртуальная машина Java) и напрочь убиты глюки с международными символами, шрифтами и форматами даты, времени и валюты, повышен уровень защиты cookies, устранены проблемы распознавания текстового пароля и потери ключа шифрования при недостатке памяти.
1-ый сервиспак не содержит обновленных версий компонентов или функций, а направлен только на латание дыр. Например, эксплорер останется той же версии, что и был до установки SP1. А вот если поставить 6-ой эксплорер перед установкой SP1, то деинсталлить IE уже не получится. Такой вот странный факт :(.
Если тебе захотелось полатать дырки виндов, то начинай с инсталляции 1-го сервиспака или хотя бы узнай, что в него входит и можно ли без него обойтись. Также проверь для начала, не стоит ли он уже у тебя (есть дистрибутивы Win2k, в которые 1-ый сервиспак уже интегрирован). Запусти

Service Pack,ом в цивилизованной буржундии зовут комплекс заплаток для исправления багов (коих в любом ПО достаточно, а в виндах особенно :)), обновления и расширения возможностей операционки, встроенных в нее утилит и драйверов.

winver.exe с помощью командной строки и посмотри на версию своих виндов.
Существует пара вариантов установки: можно купить сидюк с дистрибутивом и поставить SP1 или залезть на http://www.microsoft.com/windows2000/downloads/recommended/sp1/x86lang.asp и там, выбрав наш родной могучий, скачать 87-метровый дистрибутив. Если коннект быстрый и Инет халявный, то рекомендуется второй способ. А далее все как обычно во всех виндовских инсталляциях. Только перед тем, как его ставить, подумай, хватит ли тебе и твоей системе такого набора исправлений? Такой быстрый выход 1-го сервиспака намекает о наличии еще множества других дырок. Не лучше ли сразу заинсталлить Service Pack 2, тем более, что он содержит все исправления 1-го?

Service Pack 2 для Win2k

2-ой сервиспак для винтукея вышел в мае 2001 года и представляет собой набор 549(!) исправлений ошибок, оставленных после 1-го сервиспака (а в сумме-то ошибок около 900 получается... однако тенденция...). Как и при выпуске SP1, Microsoft заявляет о нацеленности SP2 на исправление недоработок более ранних модификаций компонентов, а не на расширение функциональности системы. Их можно понять - терять деньги на совершенствовании старой системы, когда на подходе новая (XP), было бы по крайней мере глупо.

В SP2 появилось много аппаратных исправлений для подсистем питания, видео и DVD для ряда моделей ноутбуков (да, до SP2 питалово у меня глючило немерено, а теперь ничего, пашет по понятиям - прим. Дронича); обновленный драйвер AGP для набора микросхем RCC; усовершенствованный драйвер SCSI. Реализована поддержка дисков ATA-100 (Mode 5); драйвер освобождения памяти OHCI1394; USB-драйвер, отключающий отсутствующие устройства. В SP2 решены многие проблемы кэша, переноса зоны в DNS и тиражирования Active Directory (AD); ошибки резервного копирования и восстановления данных; изъяны процедур аутентификации, использования пароля и блокировки учетной записи; нарушения прав доступа в lsass.exe и services.exe; проблемы назначения и понижения роли контроллеров домена (DC) Windows 2000. Усовершенствована служба репликации файлов (File Replication Service): повышена надежность связи в сетях, в которых центральный узел соединен с большим числом периферийных узлов через медленные линии (например, каналы 64 Кбит/с), переработаны механизм регистрации событий FRS и утилита для диагностики и устранения неисправностей ntfrsutil.exe. Самое главное достоинство SP2 - дополнительные средств защиты от несанкционированного доступа и появления BSoD'ов. Устранены причины фатальных сбоев, вызываемые disk.sys, serial.sys, fastfat.sys и dlc.sys.

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ

SP2 повышает уровень шифрования с 56-разрядного на 128-й. Понятное дело, с таким стандартом на душе станет поспокойнее. Но если захочется снова потрепать нервы по поводу безопасности, то бишь вернуться к 56 разрядам, то обломись. 128-разрядное шифрование никуда не денется, даже если снести SP2. Правда, это преобразование требует выключать антивирусники на время инсталляции, но 5 минут без них потерпеть можно (навряд ли Microsoft станет распространять троянов со своими апдейтами, хотя... :)).

ПОДГОТОВКА К УСТАНОВКЕ

Для начала не мешало бы заиметь дистрибутив SP2. Тут на твой выбор несколько вариантов: скачать с www.microsoft.com на свой хард, при наличии сетки попросить расшарить дистрибутив (если такой имеется у членов сетки) или воспользоваться обычным сидюком (на сайте Майкрософта написано, что диск с дистрибутивом 2-го сервиспака можно заказать. Интересно, пришлют ли? :)). Если решено качать SP2, то лезь на http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/default.asp или, если интересует русская версия SP2 (ставить SP2 лучше на том языке, на котором работают сами винды), то http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/sp2lang.asp, и качай SP2. Весит это хозяйство 100 с хвостиком метров. Решай, что лучше, качать или купить диск?

После установки Service Pack 2 в папке виндов (по дефолту C:\WINNT) будет создан файл svcpack.log, в котором будет отчет об изменениях инсталлятором SP2 всех измененных файлов.

СТАВИМ 2-ОЙ СЕРВИСПАК

Для апгрейда винтукея тебе придется совершить нелегкий выбор между тремя типами установки: модернизация (апдейт виндов из серии «как всегда»), интегрированная установка (одновременный инсталлинг виндов и SP) или комбинированный метод (построение единого установочного пакета, в котором содержатся Service Pack 2 и скачанные после его выхода различные хотфиксы и обновленные дрова для данного компа).

МОДЕРНИЗАЦИЯ

Модернизацию можно произвести с сайта Microsoft'а или заиметь у себя под рукой скачанный дистрибутив сервиспака. Если тебе нужно проапдейтить только винды на своем компе, используя для этого Инет, то лучше использовать оперативный режим (Express). В таком случае винды сами определят, что установлено на твоем компе, и будут качать только нужные составляющие, исходя из состава виндов. Объем скачиваемого сокращается раза в 2 точно (если установка в свое время делалась ручками). Еще один плюс этого метода (особенно для диалапщиков) - работающая докачка.

ИНТЕГРИРОВАННАЯ ИНСТАЛЛЯЦИЯ

Нужно установить последнюю версию Win2k на новый комп - поюзай интегрированную установку. Для этого придется указать инсталлятору пути к дистрибутиву виндов (вот для этого случая он необходим) и SP2. Файлы виндов и SP2 устанавливаются одновременно, вместо того чтобы сначала инсталлить ось, а позже апдейтить ее до SP2. Это самый быстрый способ установки последней версии Win2k. В таком случае не получится в будущем деинсталлять SP2, ибо он будет интегрированным в систему (но ведь ты ставишь SP2 не для того, чтобы потом снести).
Для создания интегрированного каталога для установки Windows 2000 Service Pack 2 на чистом компе воспользуемся 3 папками:
C:\sp2 - содержит распакованную версию дистрибутива SP2;
C:\Win2k - компакт с дистрибутивом виндов;
C:\win2ksp2 - создаваемый интегрированный каталог.
Воспользуйся командной строкой. Создай интегрированный каталог:
md C:\win2ksp2. Скопируй туда компакт с виндами:
xcopy C:\Win2k C:\win2ksp2\Win2k /e
Скопируй сам SP2 в конечный каталог:
C:\sp2\update\update.exe -s:C:\win2ksp2
А теперь бери болванку и режь диск Win2k SP2, сделай его загрузочным, ну и т.д. Такой диск и самому пригодится, да и друзьям помочь сможешь в случае чего.

КОМБИНИРОВАННАЯ УСТАНОВКА

Комбинированная установка - это интегрированная установка + установка хотфиксов и заплат для системы безопасности, а также обновление драйверов и файлов, специфичных для данного компа, вышедших после релиза SP2. Принцип создания интегрированного каталога схож с описанным выше.

НЕ РАССЛАБЛЯЙСЯ

Бесспорно, 2-ой сервиспак устраняет много багов, но после его выпуска было обнаружено и задокументировано еще порядка 200 ошибок. К ним также постоянно выходят исправления (заглядывай на страничку хотфиксов), которые вскоре должны будут войти в ожидаемый 3-ий сервиспак для Win2k.

тесты

Прикольные тесты для креатиффщиков!

Матушка Лень (MLen@mail.ru)

Предлагаю тебе себя потестить и других показать! В этой статье я тестило тесты. Но не простые занудные тесты, а прикольные и ненапряжные. Основное требование - чтобы тестить было легко и весело.

Эти тесты помогут тебе проверить свою креатиффность во многих сферах твоей жизнедеятельности. А может быть, эти тесты подтолкнут тебя к созданию собственного креатива.

Когда собственные идеи иссякнут и ты забьешься в депре, зайди на эти веселые странички и хорошенько протестись. Может, отловишь баги в своей психологии.

А чтобы тебе было вдвойне веселее, я протестилось в этих тестах само и написало тебе результаты. Давай померяемся писями, если у тебя есть, конечно. Все тесты онлайновые, то есть тебе не придется геморроиться с высчитыванием баллов. Выбери нужные ответы и сразу получишь результат!

«Есть ли у вас фантазия?»

http://www.abalusoft.com/online/online36.html

Несколько дурацких вопросов типа «Плачешь ли ты в кино?» и «Как ты одеваешься?». После чего мне сказали, что у меня дико буйная фантазия, но нужно ее правильно применить! Потом я ответило на все вопросы «нет», мне заявили, что фантазия ни к черту. После того как я зафигачило половину «да», а половину «нет», мне сообщили, что надежда есть! УРА!

«Потенциал лидера»

http://www.abalusoft.com/online/online118.html

Вопросы не напрягают, например: «Схавал бы ты последний кусок пирога на праздничном столе, если бы все постеснялись его взять?». Да не вопрос!

Тут мне сказали, что я вожак! Но главное, чтобы я не зазнавалось и не стало диктатором! Типа я смелое, целеустремленное! Настоящие креатиффщики и креатиффщицы должны быть лидерами! Ну, хотя бы идейными! На все «нет» тест стал ругаться, что хватит пресмыкаться! А на все «может быть» тест назвал меня золотой серединой - самый мазовый случай.

*

«Умеете ли вы обращаться с деньгами?»

http://www.abalusoft.com/online/online24.html

Креатифф - кривотивом, но и жить ведь на что-то надо! Настоящий креатиффщик или креатиффщица обязательно должны уметь правильно разрулиться с деньгами. Мы, кривотивные люди, можем делать деньги из воздуха! Недаром в этом тесте у меня выявилось наличие исключительного нюха на деньги!

Вопросы тут типа: «Верите ли вы, что можно заработать деньги честным трудом?» или «Можно ли вас напоить и тогда настрелять денег?».

На все «нет» тест обзывается «Надежным вкладчиком». На все «может быть» тест говорит, что я рисковый чувак, и это круто! А если продолжать в том же духе, то я прогорю!

«Оптимист, реалист, пессимист»

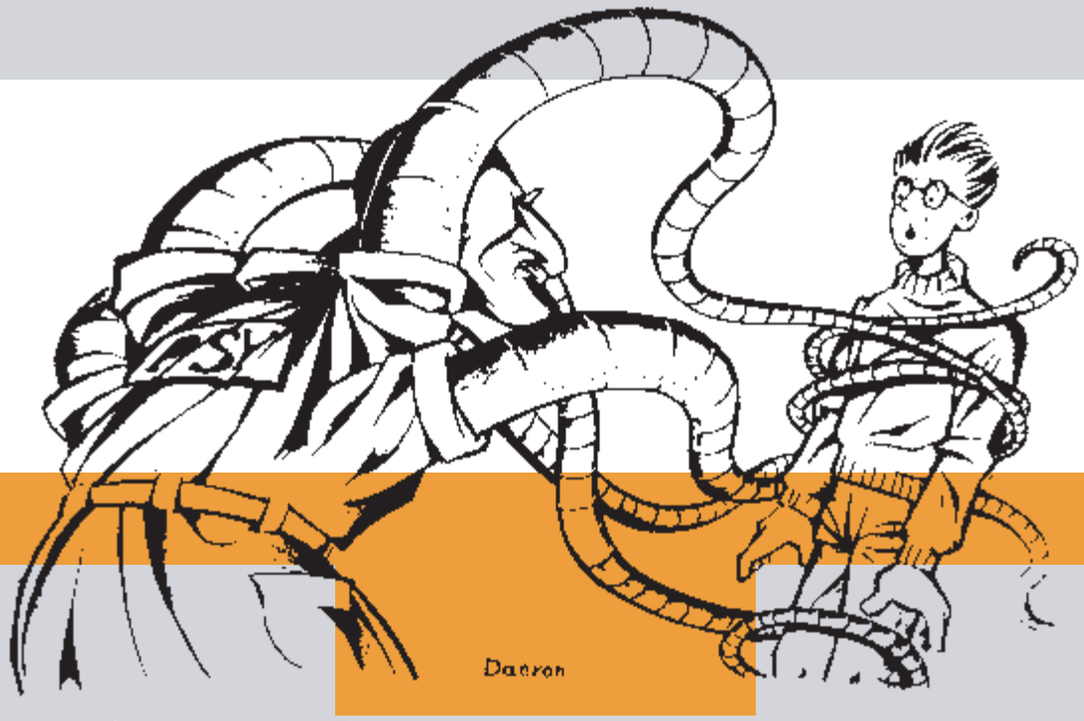
http://test.msk.ru/

«Часто ты принимаешь снотворное?» и «Застраховал ли ты свое имущество?». Этот тест назвал меня «переполненным оптимизмом». Но расслабляться не надо, могут не понять не настолько оптимистичные люди. И постоянно не понимают! Креатифф - оптимистичная религия. Тест был жутко неудобным, новый вопрос грузился на новой страничке, поэтому я упарилось отвечать!

«Угрожает ли вам зеленый змий?»

http://tests.holm.ru/cgi-bin/qu.cgi?p=t98.cfg

Креатиффщику нельзя спиваться! Конечно, под банкой идеи так и прут, только дел никаких нет. Настоящий креатиффщик должен совмещать прущие идеи с непрерывной деятельностью! Вопросы типа: «Случались ли у вас провалы после пьянки?», «Бывают ли галлюцинации после попойки?». Что сказать? Иногда можно и поглючить - новые идеи могут прийти в виде классной дяфчонки, например. Ты ее так, а она никак. В чем дело? Ах, это ж, девочки, идея!



Этот тест сказал, что проблем с алкоголем у меня не имеется. Тогда я ответило еще разок «да» на плохие вопросы типа «Похмеляетесь по утрам, с целью взбодриться?», «Бывают ли у вас запои?». Тест это особо не взволновал - он предупредил, что «возможно, скоро я стану пить сверх меры».

«Являешься ли ты самым ленивым человеком на свете?»

http://children.kulichki.net/vopros/len.htm

Зачем креатиффщику быть ленивым? Это уже вторично. Именно ленивые люди двигают нашу креативную религию. Нам постоянно приходится что-то изобретать, чтобы нам не мешали лениться. От работы так просто не откосишь. Вопросы в тесте типа: «Как часто ты моешь пол в квартире?» и «Когда ты делаешь то, что можно сделать сегодня?». После того как я ответило честно на все вопросы, тест заявил, что если ни одного балла не набрано, то я самое ленивое существо на свете. В точку! У меня НОЛЬ!

«Есть ли у вас в голове тараканы?»

http://children.kulichki.net/vopros/tarakan.htm

Ну, вот на этом тесте я сильно лажанулось! Тест заявил, что тараканов у меня в голове нет, но подозрение на их наличие имеется. Может, у меня просто особые тараканы? Ведь без тараканов в голове креатиффщику никак! Вопросы типа: «Роняли ли меня в детстве на пол?», «Верю ли я в победу коммунизма?», «Есть ли среди нас инопланетяне?».

«Скажи мне, как ты писаешь, и я скажу, кто ты?»

http://home.uic.tula.ru/~s952120/prikol.html

Вопросы типа: «Рвешь ли ты штаны, если не удалось найти ширинку с первого раза?», «Наблюдаешь ли ты за пузырями в унитазе во время процесса?». Вариантов очень много, очень рекомендую этот веселый тест, ведь кривотивность должна проявляться во всем!

По этому тесту я - экспериментатор, как не сложно догадаться!

«Определение коэффициента пикапера»

http://www.pickupcentre.ru/test/

Вопросы типа: «Если девушке на попу сел комар?..» и «Как подкатить к богатой рыбке?». Тест очень прикольный и умный, его не перехитришь. Из меня пикапер некудышный! У меня коэффициент П всего 0.3, а максимум, кажется, 1.0. Научись применять свой креатив для покорения слабого пола!

«Обнажи Маху!»

http://www.1sistem.ru/flash1/flash[3].swf

Это суперкреативный тест во флеше. Твоя задача раздеть Маху, так зовут девушку на картине кисти Гойи. Сначала идут вопросы о полном имени девушки, потом немного из биографии художника. При каждом правильном ответе на девушке исчезает какая-то часть одежды. Однако тест хитрый и может завести тебя в тупик. Например, при некоторых неправильных ответах Маха исчезает или на самых интересных частях появляются блоки цензуры! Обязательно попробуй этот тест!

«Легко ли вас соблазнить?»

http://www.intermoda.ru/tests/

О да, тест угадал. Соблазнить меня, как два байта переслать! Вопросы были типа: «Творится ли бардак в твоей сумочке?», «Дашь ли ты покататься подруге «Запорожец», на который копила всю жизнь?», «Любишь ли ты спать голой?». По этому тесту из меня получилась очень импульсивная девушка, которая часто меняет поклонников. И еще тест считает, что я должно опираться на трезвые оценки! Еще чего! Криатиффщик, поддайся соблазну, а то он может не повториться!

«Определи свой эротический идеал!»

http://www.sos-ka.narod.ru/ms6.htm

Этот тест в виде стишка с веселыми и жутко неприличными картинками в конце. Не буду тебе говорить о результатах моего тестирования! Кстати, неплохо будет почитать страничку с самого начала. Непонятно, кто ее делает, но кто-то очень креативный… и очень пошлый!

«Знаешь ли ты секс-этикет?»

http://www.intermoda.ru/tests/

Вопросы типа: «Что ты будешь делать, если хочешь его, но не уверена в успехе этой затеи?», «Ты первый раз увидела его голым…», «Что делать, если тебя уже завалили, а презика все нет?», «Расскажешь ли ты своему новому любовнику о том, что у тебя герпес?». Не могу удержаться, чтобы не процитировать тебе то, что тест выдал после моих откровенных ответов:
«Мисс Гармония. Поздравляем: ты умеешь передать свои сокровенные желания, не задевая чувств партнера. Подобная чуткость объясняется не столько хорошим воспитанием или безупречностью манер, сколько уверенностью в своих силах, свойственной лишь тем, кто хорошо знает и любит себя. Чувство такта отличает тех, кто умеет поставить себя на место другого. Только признавая сексуальные запросы и возможности другого (и в зависимости от них выстраивая отношения), можно получить максимум удовольствия. Хотя тебе это и так хорошо известно!».
Вот так-то! Вот плоды просвещения и креативной мощи! А на самом деле, я очень скромное.

«Какой видят тебя мужчины?»

http://www.intermoda.ru/tests/

Об этом я уже очень давно мечтало узнать! Тут меня спросили: «Лезу ли я целоваться на первом свидании?», «Пристаю ли я к боссам с глубоким вырезом на юбке?», «Стреляю ли я взглядами в сторону незнакомых мужчин?». В конце теста меня снова похвалили: оказывается, я «сексуальна, потому, что очень спокойна» и я «умею дать понять, что путь открыт, не размахивая жезлом изо всех сил». Спасибо, хоть шлюхой не назвали! Вообще, креатиффщицы и кривотиффщики, чтобы привлечь друг друга эффективно, рекомендую также подключать мозг с буйной фантазией. Учитесь у Донора -).

FRUITYLOOPS 3

КОНЦЕНТРИРОВАННЫЙ МУЗЫКАЛЬНЫЙ КРЕАТИФФ

Девочка без задней мысли (girl_without@omen.ru), **Donny** (donor@real.xakep.ru)

Привет, привет, брат-креатиффщик! Сегодня у нас в прозекторской настоящая музыкальная бомба! И сейчас мы ею вмажемся по самое не балуйся. Мы расскажем тебе о замечательной тулзе - мечте любого музыканта и ди-джея - FruityLoops3 и научим тебя создавать безбашенные треки мизинцем левой пятки.

Девственная чистота. Надолго ли?

ЧТО ЭТО ЗА DJ?

FruityLoops3 - это довольно продвинутый комплекс для создания электронной музыки. Конечно, профессионалу он не заменит весь спектр оборудования и софта, но может оказать весьма существенную помощь. Например, GiRLa лабает во Фрути параноидальный аккомпанемент и наяривает под него на электрогитаре.

FruityLoops3 - это drum-машинка, эмулятор набор продвинутых аналоговых синтезаторов (TS404, 3x Osc, Wasp и другие), набор спецэффектов (FX's), сэмплер и куча плаг-инов. Вообще, создается впечатление, что создатели FruityLoops3 скупили все музыкальные технологии, до которых смогли дотянуться, и засунули их в одну тулзу. Фрути также поддерживает импорт из известных музыкальных прог, позволяет работать с MIDI-треками и готовыми сэмплами.

Нам же с тобой из этого всего важно то, что эта софтина поможет не только выплеснуть свою неудовлетворенную творческую энергию в виде прикольной музыки любого стиля (каждому свое), но и позволит въехать и посмотреть на примерах, как строится музыкальная композиция, как работают синтезаторы, эффекты и всякие примочки, а также поэкспериментировать, благо контролзы незамороченные. Donor вот даже выкрутил из TS404 некоторое подобие голоса...

СТАВИМ И ЗАСТАВЛЯЕМ РАБОТАТЬ

Несемся на http://www.fruityloops.com/ и сливаем оттуда дестриб. Семь метров, конечно, не шутка, но оно того стоит. Дальше ищем FruityLoops3 в бездонных карманах асталависты и, как ни странно, находим именно последнюю версию. Волшебный ключик - это .reg-файл, что не может не радовать. Инсталлим FruityLoops3, даблкликаем на файлике реестра - все, можно запускать прогу. Если ты собираешься работать с MIDI-клавой, то сделать соответствующие настройки ты сможешь в любой момент. Больше ничего настраивать не надо.

ЧТО МЫ ВИДИМ НА КАРТИНЕ?

Прога загрузилась. Это основная рабочая область. Оцени дизайн! Эти мегалюди еще и клевый фейс забацали! Вот как надо работать! Кстати, обои у проги можно менять - такие обои стоят у GiRL'ы. Посреди стола одиноко торчит Step sequencer (здесь ты будешь лабать свои сэмплы), но это ненадолго - сейчас мы завалим весь стол так, что тебе и 1024x768 мало покажется. Однако не надо убегать в панике - мы не собираемся грузить тебя детальным описанием контролзов, а просто покажем основные инструменты и фичи.

ПЕРВЫЙ ШАЖОК

Сейчас на Step sequencer'е 5 стандартных каналов: вэйв-синтезатор TS404, бас бочка, хлопок, тарелка, рабочий барабан. Это стандартный drum set. На самом деле вариантов ударных во FruityLoops3 просто море. Давай замутим бит. Кликни мышкой первые клеточки каждого блока (они выделены цветом) в канале бочки (C_kick). Теперь на линейке инструментов включи play (она одна на всю прогу) и проверь, чтобы рядом горела лампочка pat (то есть играет паттерн). Слышишь «БУМ-БУМ-БУМ-БУМ»? Теперь добавь хлопки и тарелочки. Ну, въехал?

Кстати, «включать» клеточки не обязательно через равные промежутки, тогда у тебя получится

Сейчас накрутим TS404 задницу

ломанный бит. А можно включить вообще все клеточки, тогда у тебя получится барабанная дробь. Теперь ты - ударник фрутилупового производства :).

Видишь, как все просто! Чистый, незамутненный креатифф!

НЕМНОГО ПОНЯТИЙ

Построение композиции во FruityLoops3 держится на нескольких основных понятиях, поэтому надо тебе их втереть.

Композиция, грубо говоря, - это набор паттернов, выстроенных определенным образом.

Паттерн - это короткий блок из одной или нескольких последовательностей звуков, которые проигрываются одновременно. Паттерн строится из каналов. Паттерны переключаются соответствующими контролзами на линейке инструментов или цифровой клавиатуркой.

Канал - это как фотожопный слой, в который можно засунуть один инструмент или один сэмпл. Но канал не ограничивается одним паттерном, просто в каждом паттерне там лежат свои ноты.

Сэмпл - это один звук или несколько нотк какого-нибудь инструмента. Хотя сэмплы бывают довольно сложные и достаточно длинные (как ни нелепо это звучит).

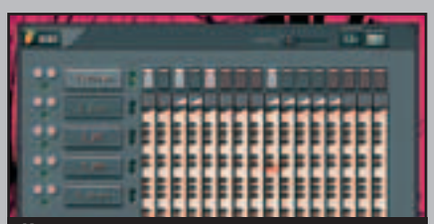
Длина паттерна - это сколько по времени играет один паттерн. Для тебя - это сколько клеточек в Step sequencer'е (стандартно - 16). Выставляется в Options\Song settings\Bar length. Можно поставить до 64 (вдруг у тебя паттерн длинный).

Длина бита - это ритм твоей композиции (не путать с Tempo, которое есть скорость проигрывания, а также с самим битом, который ты пишешь на свое усмотрение). Как метроном: может стучать чаще, а может - реже. Визуально - это отделенные разными оттенками блоки клеточек. Выставляется в Options\Song settings\Beat length.

ЗАПАРИВАЕМСЯ С СИНТЕЗАТОРОМ

Бит есть, но один бит - это не композиция. Добавим синтезатор. Базовый синтюк у нас - TS404. Он уже есть среди каналов паттерна. Щелкни на большую кнопку с надписью «TS404#*», и рядом с Step sequencer'ом появится морда синтезатора. Простым кликаньем по клеточкам тут уже не обойдешься - давай сыграем какую-нибудь мелодию. Убедись, что выбран канал именно с TS404 (рядом с ним должен «гореть» большой зеленький огонек) и щелкни на иконку с клавиатуркой в правом верхнем углу Step sequencer'а. Вывалилась Piano roll aka рояльная раскладка. Да, в каждом столбце можно будет выбрать соответствующую ноту. Подбери на слух чего-нибудь. Для этого опять включи проигрывание паттерна. Если мешают другие каналы, выключи их, протоптав соответствующий маленький зеленый огонек под регуляторами громкости канала и панорамы. О, да ты у нас еще и пианист :)!

Здесь же можно замутить простой эффект. Видишь серые клеточки вверху рояльной раскладки? Левой мышкой туда можно ставить треугольники, а правой - убирать. Треугольники обозначают «шлейф» (слайд) за нотой. Чем больше треугольников, тем длиннее «шлейф». Убери все ноты и поставь одну в самом начале, сделай шлейф и послушай паттерн. Воткнул? Главное, чтобы «шлейф» не перекрывал следующую ноту, иначе он ее просто «забьет». Слайд есть только в TS404.



Насладимся слайдом

Теперь давай взглянем на настройки TS404, тем более, что многие из них характерны и для других синтезаторов и сэмплера. Наверху находятся pan (регулятор баланса между левым и правым каналами, левее/правее), vol (громкость канала) и pitch (скорость проигрывания канала). В окошке FX показан номер блока эффекта, который будет применяться к данному каналу. В блоке регуляторов Envelope задается график, по которому будет обрезан звуковой сигнал. Каждый регулятор отвечает за соответствующий участок графика. Очень полезная штука, когда нужно убрать гудение в сэмпле. OSC1 и OSC2 - регуляторы соответствующей волны (синтезированный звук складывается из двух волн). Попробуй переключать маркер между формами волны (синус, пила, квадрат и т.д.) и увидишь, что творится со звуком. Во вкладке MISC на клавиатуре правой кнопкой мыши можно выбрать тональность, в которой будет проигрываться сэмпл.

БОЛЬШЕ КАНАЛОВ ХОРОШИХ И РАЗНЫХ

На стандартном количестве каналов далеко не уедешь, а FruityLoops3 поддерживает их до фига. Пора добавить парочку. Дуй в Channels\Add one\Sampler. Мы добавили канал с сэмплером. Пока он не играет, потому что мы не выбрали, собственно, сам сэмпл. Дави на большую кнопку с надписью «SET» - появится сэмплерова морда. Нажимай на иконку с папкой (где написано (none)) и ищи в стандартном проводнике нужное файло. Кстати, лучше всего вырубить все паттерны, чтобы было слышно, какой сэмпл ты выбираешь (FruityLoops3 проигрывает файл, когда ты ставишь на него курсор). Выбирать нужные файлы можно также посредством удобного встроенного навигатора (иконка с буковками «SB» на панели инструментов) - там они разложены по категориям. Здесь выбранный сэмпл устанавливается правой пимпой крысы.

Теперь сэмпл загружен (на большой кнопке написано его название), и можно обработать его, настроив Envelope, выбрав тональность звучания и поиграв с другими настройками. Теперь прописывай в соответствующем канале нужного паттерна ноты и слушай, что получилось.

УПРАВЛЯЕМ КАНАЛАМИ

Во FruityLoops3 очень удобно работать с каналами. Через пункт меню Channels и по правому щелчку мыши на соответствующей кнопке канала в Step sequencer'е можно клонировать канал (все настройки оригинала сохраняются), можно скопировать содержание канала и вставить в другой канал (через верхнее меню), удалить, передвинуть и так далее. Очень интересная фишка открывается по правому щелчку по кнопке канала в пункте Edit. Называется Randomize. Ты задаешь тональность, диапазон октав, количество нот, и комп сам генерит музыкальную фразу. Конечно, ничего великого ждать не приходится, но если надо что-то на фон положить, то это самое то.

PIANO ROLL СТАРШАЯ

Часто недостаточно указать ноту - нужно еще настроить длительность ее звучания. Для этого предусмотрена большая Piano roll, которая вызывается иконкой с буковками «PR» с линейки инструментов. Можно юзать для любого канала кроме того, куда загружен TS404.

Выберите другой тон, молодой человек!

Выбери канал с загруженным сэмплом и вызывай большую рояльную раскладку. Здесь все очень просто: кликая мышью, расставляем нотки, ею же сужаем или растягиваем блоки на нужную длительность. Двойной клик на ноту позволит задать ее значения (положение и длительность) точно. Маленькие кнопочки в левом верхнем углу Piano roll помогут писать и редактировать. Карандаш - писать, кружок - удалять, уголок - двигать, рамочка - выделить несколько нот. А вот маленькая кнопочка с клавишками позволяет загрузить партию какого-нибудь инструмента из готового MIDI-файла, поэтому очень

ценна для нас. Дави кнопочку, топчи пункт Import MIDI-file, ищи нужный MIDI-файл и выбирай, какую дорогу тебе загрузить. В Piano roll появились ноты. Теперь можно вылезать из рояльной раскладки (заметь, в соответствующем канале паттерна появился мониторчик с превью партии). Дальше можно колбасить звук настройками и эффектами на твое усмотрение.

ДРУГИЕ СИНТЕЗАТОРЫ И ФИШКИ

Wasp (oca) - очень часто используемый синтезатор, дает жужжащие звуки, за что так и прозван. Рассказать обо всех настройках у нас нет никакой возможности, а у тебя слушать нет никакого желания (проще физику выучить), поэтому крути и выкрутишь. Маленькими кнопочками с зелеными графичками меняем форму волны, регуляторами задаем график фильтра. Во FruityLoops3 уже есть набор стандартных настроек (пресетов) синтезатора. Пролистать и попробовать их можно стрелочками в правом верхнем углу.

3xOSC - название говорит само за себя. Очень похож на TS404, но для синтеза звука используются не две волны, а три. Настройки такие же:

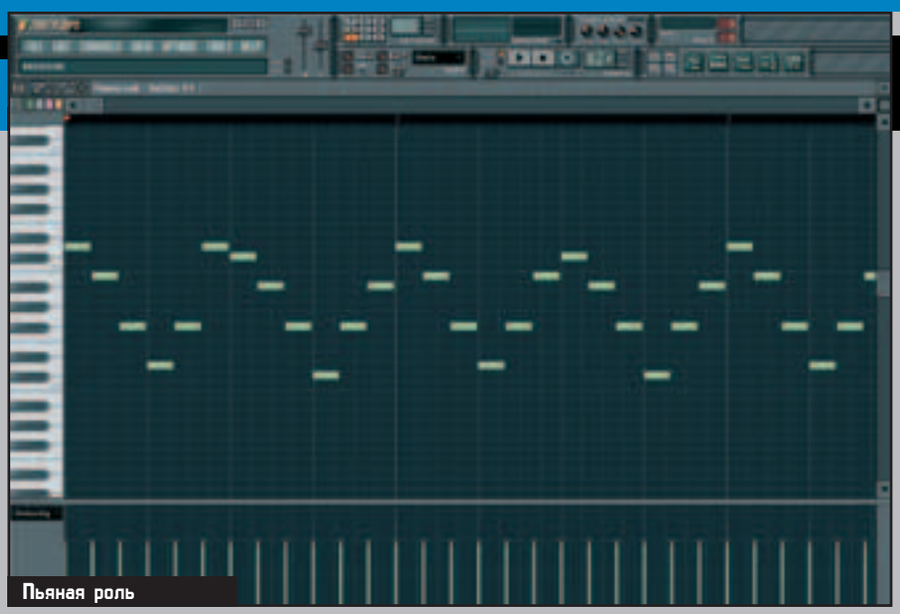
Морда и тело сэмпла

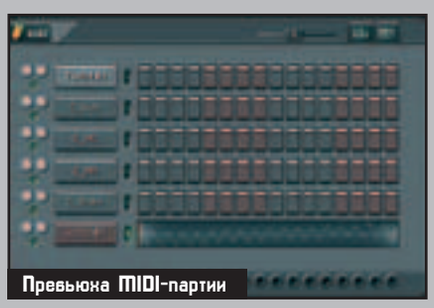
меняем форму волны, настраиваем Envelope и выбираем тональность.

SimSynth - синтез тоже происходит за счет трех волн. Богатые настройки позволяют вытрясти из этого синтезатора огромное количество самых различных звуков - от трубных до ударных и фантастических. Также имеется большое количество стандартных вариантов настройки (выбираем стрелочками), немного подкорректировав которые, можно получить нечто индивидуальное. В общем, маст юзъ.

Plucked! - судя по названию, позволяет синтезировать звук щипковых инструментов (pluck - сщипывать). Так оно и есть. Настроек минимум: два регулятора - decay (вибрация звука) и color (насыщенность звука) и выбор тональности. Просто, но часто пригождается.

BeepMap - гибрид слов bitmap (растровая картинка) и beep (тон) - скорее, не синтезатор, а фишка.


Пьяная роль


Превьюха MIDI-партии


Осиное гнездо

Мы рассказали тебе достаточно, чтобы креативить офигенные композиции. Врубай колонки погромче, отрешайся от этого мира, и да пребудет терпение с твоими соседями.

Дело в том, что в эту фичу можно загрузить графический файл (gif, jpeg, bmp), и она по переходам цвета синтезирует какой-нибудь сумасшедший звук. Абсолютно бесполезно, но прикольно :).

Остальными пунктами не заморачивайся - Fruity Wrapper по идее должен помочь подключить новые плагины, а MIDI-out нужен, чтобы играть на внешний MIDI-секвенсор, или можно подгрузить синтезатор из соответствующей .dll'ки.

ЭФФЕКТИВНЫЕ ЭФФЕКТЫ

Эффекты FruityLoops3 - очень веселая и очень полезная штука. Эта фича позволяет изменить сэмпл до неузнаваемости: добавить эхо, ревербирацию, фленджер, 7-полосный эквалайзер, дисторшен и так далее. Объяснять, что делает тот или иной эффект, нет смысла - это надо слышать. Мы просто объясним тебе, как этим пользоваться.

Во FruityLoops3 есть панель эффектов. Вызывается иконкой с буковками «FX» с линейки инструментов. Эффектов может быть до 16 сетов плюс 1 мастер. Сет может содержать один или несколько эффектов разом. Выбирай мышкой номер сета - теперь можно задать, какие эффекты будут применяться по этому номеру. Дави треугольничек на первой строчке и в Favorites выбирай название эффекта - название запишется в строку, а на столе появится форточка с его настройками. Как видишь, можно юзать до четырех эффектов разом. Включить/отключить эффект в сете можно оранжевой лампочкой в конце строки. Настройка эффекта производится регуляторами в форточке с его именем, но лучше юзать все те же стрелочки в левом верхнем углу, выбирая подходящие стандартные настройки для данного эффекта и чуть-чуть корректируя, если надо.

Однако эффект сам по себе - не эффект. Применим его. Найди Step sequencer и выбери канал, к которому хочешь применить эффект (изменения с этим каналом произойдут во всех паттернах!). Теперь дави на большую кнопку с именем инструмента или синтезатора, который висит на этом канале. Откроется знакомая форточка с наст-

Цветные трели

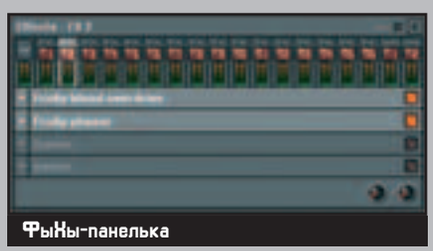
В контролзах Симсинка можно заблудиться

ройками. Помнишь, я говорил тебе про окошко FX с номером? Вот, в нем-то и нужно выставить нужный номер твоего эффекта (как и в других контролзах, просто зажми мышкой и потяни вверх или вниз). Теперь расставляй ноты или загоняй сэмпл и включай проигрывание паттерна. Все, можно включать и выключать эффекты, крутить их настройки и на слух определять, что тебе нравится, а что нет.

Расскажу о моих любимых эффектах. Fruity reeverb (реверберация), Fruity delay (задержка) - схожие эффекты, оба - временнЬle, предназначены, чтобы создавать иллюзию пространства. Различные результаты получаются в зависимости от длины промежутков между повторами звука. Fruity blood overdrive (перегруз) - громкость сэмпла увеличивается preAmp'ом до состояния разрушения... а потом урезается PoastGain'ом, чтобы не перебивать остальные инструменты и не повредить твои колонки. Fruity phaser (колбасит фазу, звук меняется, если сэмпл проигрывается несколько раз, можно получить звук лазера, звук включившегося робота и так далее).

МОНТАЖНИКИ-ВЫСОТНИКИ

Ну, вот ты заготовил кучу сэмплов, партию ударных, эффекты и расслабился. А зря! Осталась самая ответственная часть креатиффа - строительство композиции. Ведь из одних и тех же паттер-


ФыКы-панелька

нов можно построить несколько совершенно разных тем.

Открывай плей-лист (вызывается иконкой с буковками «PL» с панели инструментов) и смотри. Каждая клеточка - это один паттерн. Если клеточка закрашена, то паттерн будет играть в соответствующем месте композиции. Клеточки метятся левой кнопкой мыши, а убираются - правой. Слева направо у нас идет время композиции (измеряется длиной одного паттерна), сверху вниз идут номера паттернов. То есть, если закрасить весь столбец, то будут играть все паттерны разом. По умолчанию паттерны называются «Pattern X». Если паттернов у тебя будет много (а много будет), то ты будешь путаться, где у тебя что, поэтому лучше назвать паттерны в соответствии с содержанием. Для этого щелкай правой мышкой на название паттерна и вводи свое, например, «ударные» или «струнные N1».


Плей-лист и мозаика паттернов


Распахнутые форточки эффектных сетингзов

И еще одна фишка - «завернутая» стрелочка. Это маркер, который отмечает, в каком месте композиция будет зациклена. По умолчанию курсор будет все время возвращаться в начало, но ты можешь это поменять, перетащив маркер правой мышкой.

УВЕКОВЕЧЬ ЕРСЕЛФЬ!

Если от твоих творений прешься не только ты, но и твои соседи, а девчонки из окрестных домов смотрят на тебя не иначе, как Эвридики на Орфея, то пора увековечить себя и выложить твою работу в сеть.

Увековечить себя можно так: дуй в Options\Song Info и прописывай название композиции, свои комментарии и урлу или мыло. Не забудь чекнуть Show it on open. Теперь тайтл будет болтаться в левом верхнем углу стола, инфа появится при загрузке файла, а на урл можно будет щелкнуть и попасть к тебе на пагу.

Выложить свое творение в сети ты можешь в виде WAV-файла MP3-файла MIDI-файла. Для этого ползи в File\Export. Однако если ты хочешь обменяться опытом с таким же фрутилупером, как ты, то лучше юзать Zipped loop package - прога сохранит только используемые сэмплы и композицию с настройками, что весит несравнимо меньше.

ПАРА БЕСПЛАТНЫХ СОВЕТОВ

Не повторяй наших ошибок!

Не клади ударные и несколько партий в один паттерн.

Не делай дурацкую работу - почаще клонируй каналы и пользуйся Cut\Paste из меню Edit.

Учитывай, что сэмпл, написанный тобой на большой Piano roll, может оказаться длиннее паттерна, тогда он будет проигрываться не до конца. Лучше разбить его на два паттерна.

Не забывай про бас - одних ударных и соло маловато будет.

Храни свои сэмплы упорядоченно, иначе чего-нибудь потеряешь.

Когда намутишь несколько приличных композиций, загрузи классные фишки из раздела Loops\Cool Stuff (ищи в навигаторе). Сможешь сравнить и перенять опыт.

Внимательно смотри инфо в чужих композициях - там встречаются урлы сайтов маститых фрутилуперов. Есть маза почерпнуть опыт.

Глянь в Help\About и поймешь, какие фрутилуперы веселые ребята. Так трешово послать в зопу тех, кто тебя продинамил :)...

ФИНАЛЬНЫЙ АККОРД

Мы рассказали тебе достаточно, чтобы креативить офигенные композиции. Врубай колонки погромче, отрешайся от этого мира, и да пребудет терпение с твоими соседями. Становись крутым фрутилупером, пиши нам, присылай свои работы, и мы поможем найти тебе единомышленников.

Построй свой дом в Q3:Arena

учимся ваять уровни

Александр «xtracer» Логинов
(http://www.gamemag.ru)

Привет, горячий перец или сладкая перчинка, сегодня мы сделаем невозможное, превратив твою квартиру, рабочее место или помещение любимого института в виртуальную вселенную, полную всякого хлама, странных сооружений и неожиданных сюрпризов. Заинтересовался? Тогда слушай внимательно.

Трансформация нашей реальности в виртуальные дебри - процесс сложный и многофазовый. Я мог бы написать десятитомник и получить Букеровскую премию, но мне просто лень. Так что держи сухой компот из основных идей и голых фактов. А дальше думай и копай сам, такая эта… се ля ви, уж извини.

ОН СКАЗАЛ - ПОЕХАЛИ

Ну что же, приступим. Для начала тебе потребуется полная версия Quake 3: Arena. Если ты не знаешь, что это такое, и твои глаза расширились от испуга, то тебя уже ничего не спасет. Ты игровой мертвец. Пока. Оставшийся народ попрошу установить игру и забить ее последними патчами. Установил? Молодец. Теперь выруби по прилагаемой к материалу ссылке Q3Radiant и готовься к великой битве. Прежде чем радостно малевать родные просторы, тебе понадобится план. Правильный, хорошо продуманный план, где есть разумная планировка комнат, где учтен размер любимых косяков и прочих веселых штуковин. Конечно, ты можешь, как тупой лох, в течение месяца размалевывать трехметровый холст проектом жилых помещений, но есть выход лучше. В каждом более-менее серьезном здании есть план эвакуации при пожаре. Он и послужит тебе идеальной схемой будущего помещения. Во всяком случае, ты получишь представление о расположении комнат, их примерных размерах и местах стыковки. Правда, не стоит разбивать стекло и вытаскивать драгоценный лист бумаги. Лучше используй цифровой фотоаппарат, который тебе очень пригодится для лучшей имитации (фотки с разных сторон одного и того же помещения очень удобны в работе) помещения на поздней стадии моделирования.

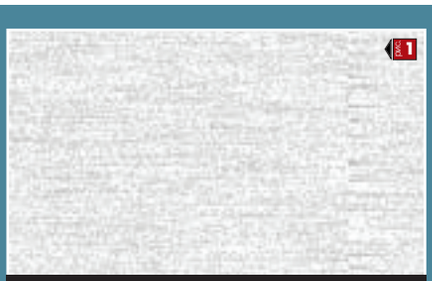
ЭТИ СТРАШНЫЕ ТЕКСТУРЫ

План у тебя уже есть, но существует проблема похуже. В обычном наборе Quake 3 Arena совершенно нет текстур для нормальных жилых помещений. Нет, изображения скелетов и красных от чужой крови стен очень хорошо впишутся в интерьер VR-хибары, но существенно подпортят гениальную задумку (мы же пытаемся воссоздать в виртуальной реальности обычное жилое помещение). Поэтому текстуры придется рисовать самому. Дело это тяжелое, кропотливое и ужасно занудное, но ты - перец сильный, справишься. Ну а я чем смогу - помогу.

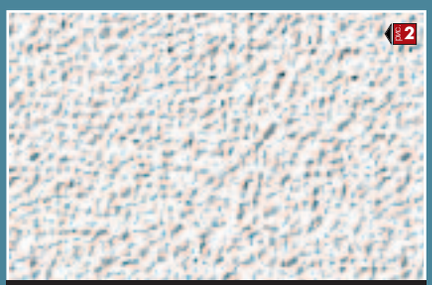
Рисовать текстуры можно где угодно, но мы используем для этих целей Adobe Photoshop. Программа известная, популярная и съедобная. Тебе потребуется около десятка основных текстур, не считая шкурок ламп, диванов и гарнитурной мебели. Создание последних отнимает гигантское количество времени, поэтому я расскажу тебе о самых простых моделях.

ПРОСТЫЕ ДВИЖЕНИЯ

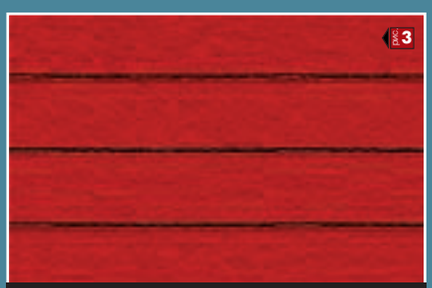
Не знаю, как ты, но большинство людей живут не на кислотной планете, а во вполне примитивных помещениях, в которых доминирует однотонный цвет рельефных стен, линолеум или скрипучий деревянный паркет. Так что придется начать с обычной белой стены. Создать такое в Photoshop проще простого. Запускай софтину и создавай новую картинку с параметрами 256 на 256 (обычно все текстуры кратны 16-и, и 256 на 256 является минимальным стандартом) пикселей. Конечно, ты можешь создать текстуру и большего размера, но здесь могут возникнуть проблемы с обладателями старых акселераторов. Беднягам придется повеситься от бесконечных тормозов. Итак, файл создан. Смело заливай его белой краской. Это основа будущей стены. Теперь добавь новый слой Layer > New > Layer, залей его белым и воспользуйся командой Filter > Noise > Add Noise. Здесь тебе нужны параметры Uniform и



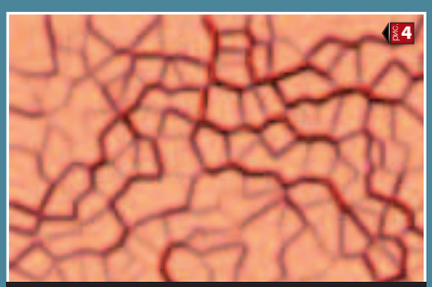
Примитивная текстура рельефной стены



Заготовка для кирпичной кладки

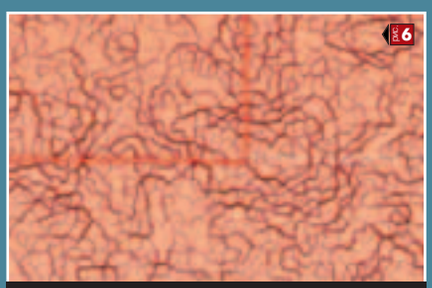


Посмотри, какой приятный цемент



Черви, вены, шкура чудовища?

Невероятно странная текстура



По красной линии текстуры легли хорошо

Monochromatic при значении не больше 50. Если ты сделал все правильно, то белое поле стало похоже на лысого негра, сильно страдающего от перхоти. Теперь размоем полученные точки при помощи команды Filter > Blur > Motion Blur. Двигай ползунок, пока тебе не покажется, что поверхность достаточно размыта. Для лишней реалистичности картины можешь воспользоваться Filter > Texture > Texturizer. В результате у тебя должно получиться нечто вроде обычной, чуть шероховатой стены (см. рис. 1). Но стены, видишь ли, бывают разные. Например, кирпичные.

КИРПИЧНЫЕ МЕЧТЫ

В Photoshop 6.0 и 7.0 есть готовые текстуры кирпичной кладки, но мы ведь не ищем простых путей, верно, чувак? Поэтому создадим кирпичную кладку самостоятельно. Скреатиффь новый объект 256 на 256 и залей его красной краской (кирпич, как никак). Сделай еще один слой и смело окрась его в белый цвет. Кирпич редко бывает ровным, поэтому воспользуемся уже знакомым тебе Texturizer. Здесь наиболее предпочтительным решением остается Sandstone. Немного рельефа и правильной расстановки света, и ты получишь нечто вроде рисунка 2. Эту картинку ты можешь использовать как еще одну текстуру обычной белой стены, но мы пойдем еще дальше. Измени значения слоя с текстурой с Normal на Multiply. В результате потрясающей операции два слоя сольются в экстазе. Белый практически исчезнет, а вот неровная текстура отлично ляжет на красную поверхность. Рванная каменная стена - это, конечно, круто, но мы хотим кирпич. Пришло время создать еще один слой. Прочерти на нем несколько ровных параллельных линий черного цвета. После этого необходимо добиться эффекта неровного цемента при помощи Filter > Blur > Gaussian Blur с параметром 3-5 (см. рис. 3). Теперь все на те же линии наложим очередную текстуру из Texturizer. Играя со светом и высотой, ты получишь приятные кирпичики, которым не хватает одного - объема. Использование Layer > Effects > Bevel and Emboss поможет тебе решить поставленную задачу.

ОРГАНИЧЕСКИЕ ОБЪЕКТЫ

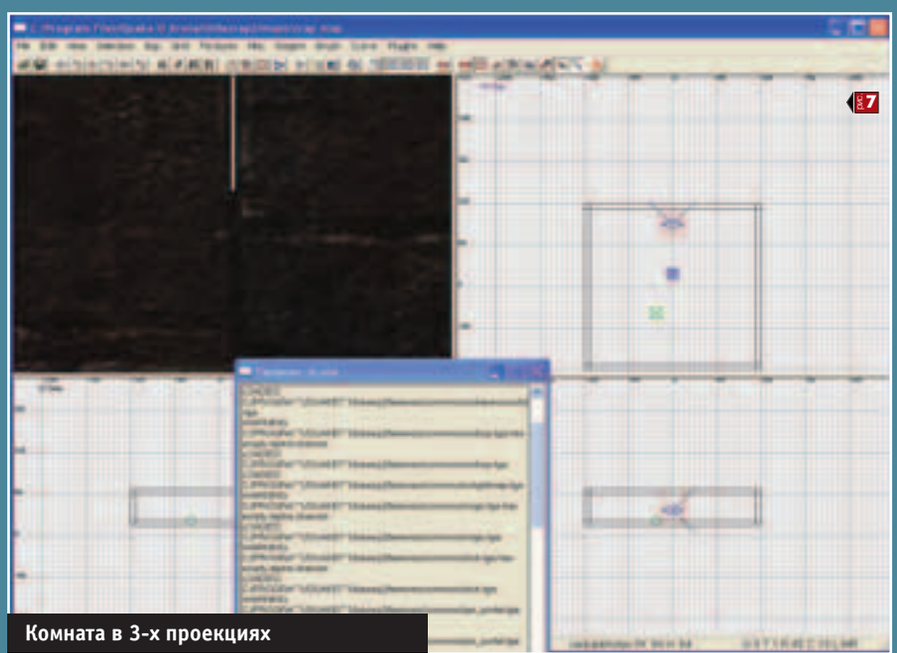
Рано или поздно ты захочешь создать какие-то органические объекты вроде мерзких водорослей или вспученных вен неизвестного существа. Приведенная ниже техника поможет тебе в решении этой задачи. Создай новое изображение, наложи на него облака Filter > Render > Clouds. Размой облака, используя Filter - Pixelate - Crystallize. Особо не увлекайся - изображение должно быть немного неровным. Настало время провести сосуды. Используй Filter > Stylize > Find Edges, затем Image > Adjust > Auto Levels и, наконец, Image > Adjust > Invert. Теперь окрась весь рисунок и сохрани его как Pattern (Edit > Define Pattern). Сохраненная текстура понадобится нам позднее. Добавь еще один слой розоватого цвета и еще один слой красного цвета. Наложи на слой маску (Layer > Add Layer Mask > Reveal All) и залей сохраненной текстурой (Edit > Fill > Use Pattern со значениями: Opacity: 100%, Mode: Normal). Осталось придать сосудам выпуклость. Для этого воспользуйтесь Layer > Effects > Bevel and Emboss. Еще одна текстура готова (см. рис. 4).

СТРАННАЯ ПОВЕРХНОСТЬ

Конечно, самыми модными текстурами остаются рваные куски железа и разрушенные стены. Давай попробуем сделать что-то похожее. Попроси новый файл, залей его белым фоном и нанеси немного Noise. Размой его с помощью Gaussian Blur, как это было указано выше, и добавь еще один слой. Залей его желтой краской и вновь вернись к Noise. Наложи на слой маску и Filter > Render > Difference Clouds. Используя Image > Adjust > Brightness/Contrast, увеличь или сократи количество ржавчины на объекте. Используя все тот же Brightness/Contrast, отрегулируй нижний слой. В результате у тебе должно получиться нечто вроде рисунка 5.

СКЛЕЙКА

Какие бы крутые текстуры ты ни нарисовал, у тебя всегда будет проблема склейки. Чтобы избежать проблем при стыковке текстур в игре, воспользуемся простым и одновременно гениальным решением. Открой свою текстуру и, используя Filters > Other > Offset, вводи половину от ширины и высоты твоей текстуры. Если текстура у тебя 256 на 256, то ты должен ввести 128 на 128. В поле Undefined Areas поставь Wrap Around. Если текстура кривая, то ты получишь изображение со швом. Вытирай шов на фиг и радуйся жизни. Если твоя текстура нормальная, то ты даже не заметишь места склейки, например, как на



Комната в 3-х проекциях

рисунке 6. Место стыковки верхней текстуры я специально выделил красным цветом.

КРЕАТИFF

Когда все текстуры готовы и сохранены в формате TGA, ты можешь приступать к самой важной стадии производства - креативу. Если ты ни разу не пользовался редактором уровней, то мне тебя искренне жаль. Q3Radiant, как бы это ни казалось странным, обладает вполне обычным интерфейсом, при помощи которого ты можешь создавать гигантские помещения, расставлять объекты и набрасывать освещение. Именно то, что тебе нужно для переноса твоего мира в виртуальную реальность. QRadiant прекрасно работает со всеми играми на движке Quake 3: Arena, поэтому ты можешь засунуть свою комнату или весь институт сразу в Medal of Honor или в не менее одиозный RtCW.

Ну что же, давай знакомиться. Внимательно посмотри на рисунок 7. Ничего не понятно? Сейчас все объясню. В самом верху находится основная панель управления. Под ней иконками выделены базовые режимы и инструменты. В центре расположен основной экран, поделенный на несколько частей, именно здесь тебе предстоит создавать макеты твоих будущих уровней. Сбоку слева представлен вид из трехмерной камеры на твой будущий проект. В самом низу ведется лог производимых действий. Прежде чем начать работу, давай снизим загрузку программы до минимума, упростив качество отображаемых текстур. Edit > Preferences и протащив ползунок Texturing Quality до конца влево. Всем обладателям карт от Nvidia стоит отказаться от Curves (через комбинацию «CTRL+P»), как это ни печально. Вроде все сделали, так что полный вперед.

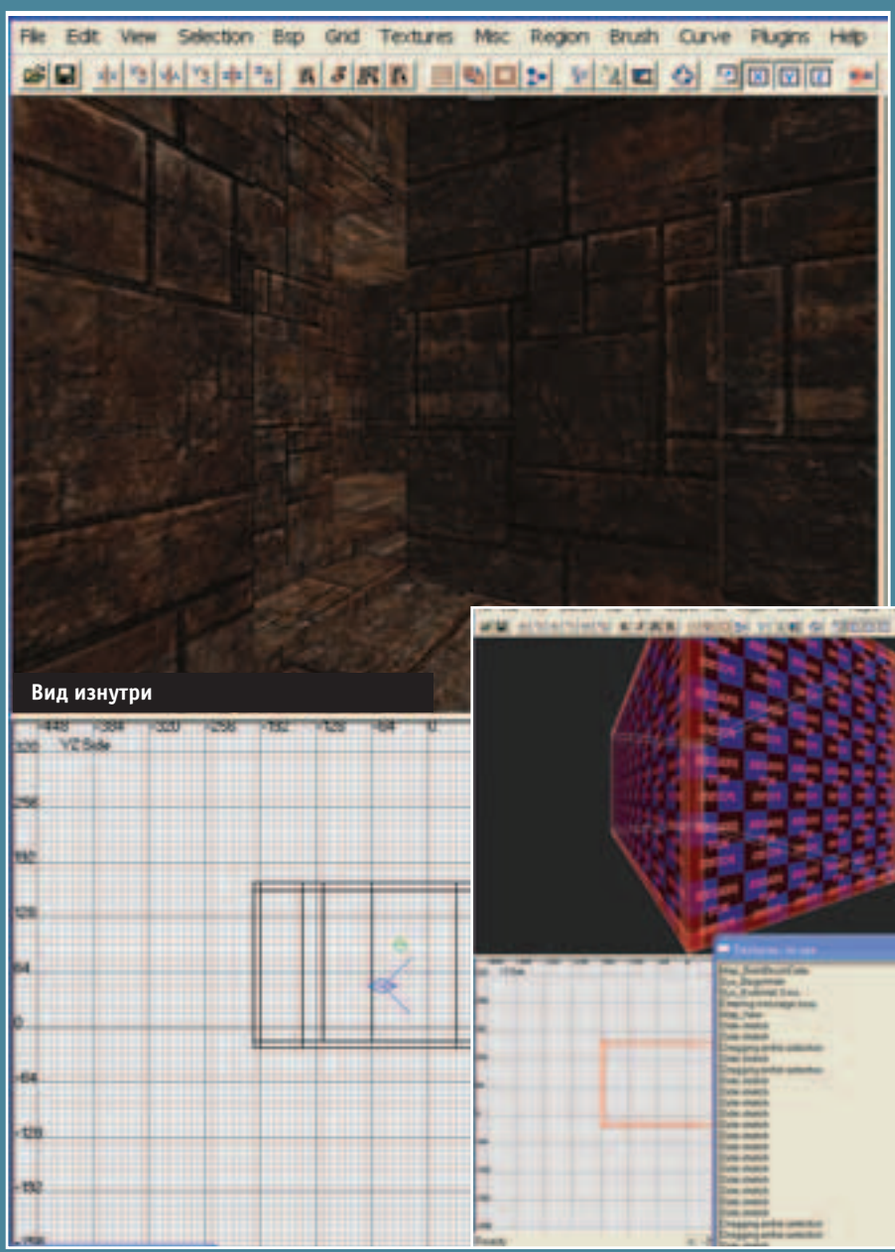
СТРОИМ ПЕРВЫЙ ДОМ

Помнишь, я тебе говорил про план помещения? Теперь он понадобится. Зажимай его в левой руке, а правой создавай профайл нового уровня. File > New Project. Называй свой проект так, как хочешь. Я предлагаю тебе модное имя - VRHome. После того как ты подтвердишь свои действия, папка точно с таким именем появится в директории Quake 3: Arena. После присвоения названия программа автоматически загрузит карту с небольшой комнатой и несколькими объектами. Карта должна называться так же, как и твой проект. В моем случае это был vrhome.map. Но зачем тебе чужие разработки? В разделе «File» щелкни на «New map». Не обращай внимания на предупреждение об обнулении всех данных («All changes to map will be lost») - давай OK. Основа для будущей карты готова.

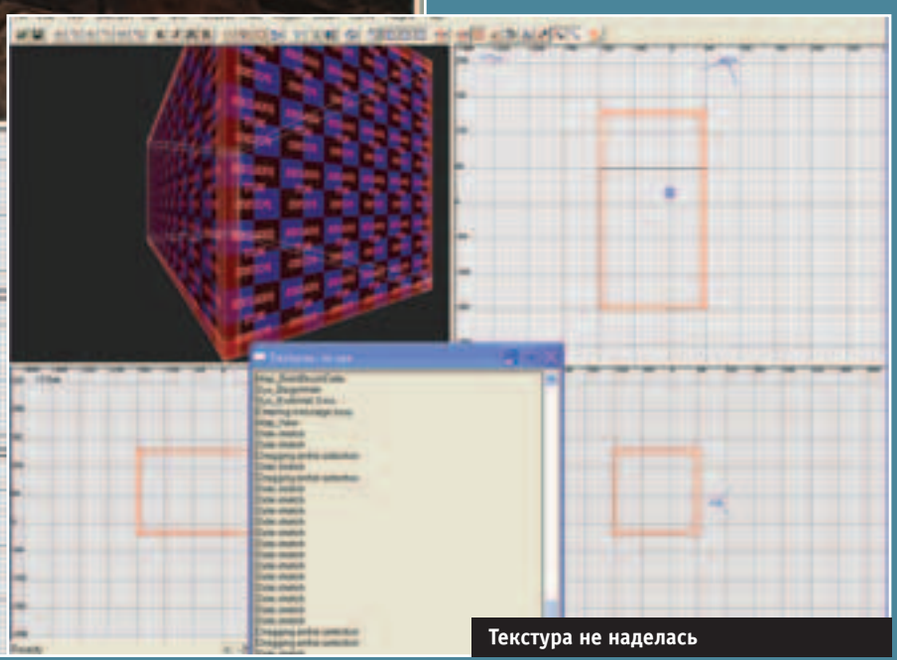
Теперь пришло время выбрать текстуры. Для этого щелкни на раздел «Textures» в верхней части меню и выбери один из предложенных пакетов. В твоем случае ты можешь воспользоваться своими собственными наработками, предварительно добавив их в основной комплект. После выбора текстур они должны появиться в виде небольших иконок в правой части меню. Если иконки не появились, а текстур нет в списке, это означает, что: у тебя стоит неполная версия игры или ты используешь режим в четыре окна, или ты неправильно указал пути к пак-файлам. Четвертого, как говорится в модных блокбастерах, не дано. Так что проверяй всю систему. Если ты хочешь использовать свои собственные текстуры, то ты должен положить их в открытом виде в отдельную директорию (лучше там же, где находится твой игровой профайл VRHome) и указать полный путь к ней (Textures > Load Directory). Если ты используешь нестандартный интерфейс (режим в четыре окна) Q3Radiant, то нажми «T» для вызова текстурного меню. Внимательно изучи предложенные варианты. Попробуй несколько комбинаций, выбери только те текстуры, которые отлично вписываются в задачи твоего проекта. Если у тебя все в порядке, то можно приступать к следующему этапу - моделированию блоков.

БЛОЧНЫЕ ДОМА

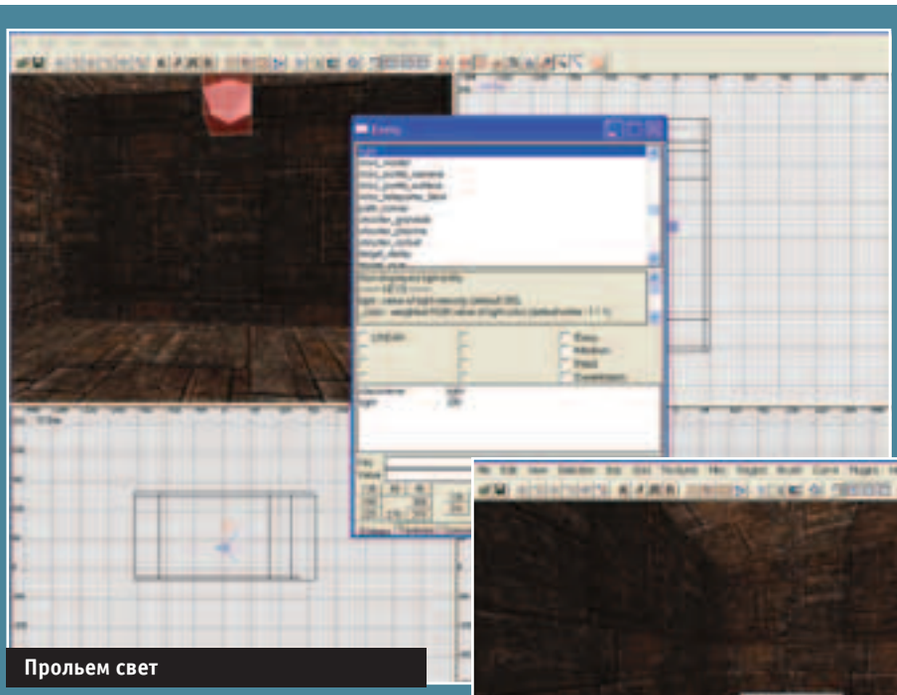
Для начала переключись в 2d режим с X и Y осями координат. Теперь зажми левую кнопку мышки и двигай курсор вниз. У тебя должен получиться красный прямоугольник. Этот прямоугольник и есть основа твоего будущего уровня. Основа должна быть хорошо согласована с твоим планом. Если у тебя потолки три метра, то в игре они тоже должны быть три метра. Если коридор тянется на 15 метров, то и в игре должна быть площадка соответствующих пропорций. Так как мы создаем жилое помещение, то здесь лучше всего начинать с центральной комнаты. Спроектируем помещение 900 на 900 пикселей с потолками в 450 пикселей. Используя различные камеры, ты можешь варьировать высоту и ширину твоего помещения. Попробуй передвинуть основание для комнаты, активируя левую кнопку мышки.



Вид изнутри



Текстура не наделась



Прольем свет

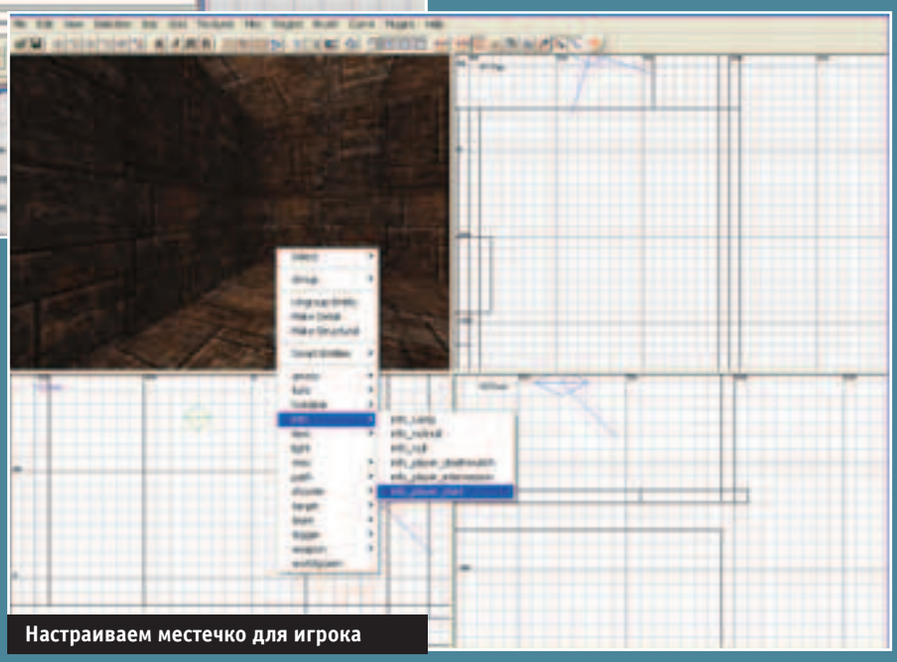
Кроме того, ты можешь приближать и удалять камеру, задействовав кнопки [Ins] и [Del]. При помощи правой кнопки ты можешь изменить положение камеры, щелкнув на трехмерном экране предварительного просмотра будущего уровня. Основание у тебя получилось, но оно далеко от оригинала так же, как Земля от Альфы-Центавра. Используя специальную функцию «Hollow», мы придадим нашей конструкции внутреннюю пустоту. Используй Selection > CSG > Hollow. Теперь твой куб стал полым внутри, в чем ты можешь убедиться, переключившись в режим от третьего лица.

ЛУЧ СВЕТА В ПОЛИГОНАЛЬНОМ ЦАРСТВЕ

Теперь можно наложить простенькие текстуры. Для этого, используя «Shift и левую кнопку мышки, выбери сторону, которую ты хочешь закрасить, затем щелкни на нужной текстуре (для вызова меню текстур используй «T»). Если ты все сделал правильно, то пол и стены должны хоть немного отличаться друг от друга. Вот и настала очередь для расстановки освещения. Смело нажимай «ESC» для того чтобы снять окрашивание и щелкай в любой точке карты. Теперь кликай правой кнопкой мышки и в появившемся меню выбери опцию «light». Присвоив ему значение (по умолчанию «100»), ты можешь передвинуть его в любой угол карты. Старайся совместить источник света со стеной или потолком для создания максимально реалистичного эффекта. Если ты все сделал правильно, то можно увеличить мощность нашего прожектора. Для этого выбери источник света (если он до этого не был окрашен) и дави клавишу «n». Выбрав «light», присвой ему значение «300». Этого будет вполне достаточно.

ДВЕ КОМНАТЫ

Дорисуй к уже существующей комнате вторую - точно с такими же параметрами высоты и ширины. Состыкуй две комнаты, но не пересекай их поверхности. Залей текстурой вторую комнату в том же стиле, что и первую. В результате у тебя должны получиться две комнаты, разделенные толстенной стеной. Настало время создать небольшой проемчик. На всякий случай сохранись. Теперь нарисуй еще один объект прямоугольной формы, который пересекал бы обе стены и создавал импровизированный проем. Внимательно посмотри, что бы все три объекта находились на одной оси координат. Теперь, не снимая окрашивания с объекта, используй последовательность Selection> CSG> Subtract. Дави Backspace для того, чтобы удалить блок. Если ты все сделал правильно, то у тебя должен появиться ровный проем, объединяющий две комнаты в один уровень. При желании ты можешь превратить прямоугольный проем в арку. Для этого создай еще один объект по ширине чуть меньше прежнего, но с той же высотой внутри образовавшегося проема. Не снимая окрашивания, используй Curve > End Cap. У тебя должна получиться арка. Переверни ее по оси X (Z->N) и по оси Y (Y->Y). Подгони арку под проем, используя разные камеры, и используй сглаживание Curve > Cap > Inverted Endcap. Наложи текстуры, и арка будет полностью готова.



Настраиваем местечко для игрока

ПРЕДМЕТЫ ОБСТАНОВКИ

Так как я физически ограничен размерами материала, то создавать предметы обстановки тебе придется самостоятельно. Например, при проектировании стола ты можешь использовать параллелепипед (один побольше, один поменьше) и четыре малые квадратные колонны, совмещенные по всем осям координат. Текстура дерева прекрасно рисуется в том же фотошопе по схеме, аналогичной моделированию вздувшихся сосудов. Шкаф представляет собой обычный параллелепипед. Компьютер также не изобилует сложными параметрами. Все, что тебе потребуется, - это хорошие текстуры, которые ты без труда нарисуешь за несколько часов. При большой лени и отсутствии желания (какой, на фиг, тогда из тебя модельер?) ты можешь воспользоваться уже готовыми наборами, которые валяются во всех частях (используй google.com, чувак!) всемирной сети.

ВСТРЕЧАЙТЕ ИГРОКА

Без игрока твой уровень будет пуст. Для начала установим стартовую точку для появления хозяина. Нажав ctrl+shift и левую кнопку мышки, мы снимем окрашивание с комнаты. Красный контур комнаты должен почернеть. Теперь щелкни правой кнопкой мышки на свободной клетке экрана и выбери Info > info_player_start. Оранжевый прямоугольник показывает позицию игрока на карте. Передвинь его так, чтобы он находился внутри основной комнаты и никак не соприкасался со стенами или иными объектами. Если ты снял окрашивание с игрока, то верни его вновь, одновременно нажав Shift и левую кнопку мышки. Теперь нажми «n» для вызова информации об объекте. Здесь ты можешь вручную изменить все настройки, переместив игрока в ту часть карты, в которую тебе захочется. Кроме того, здесь стоит поменять положение игрока. Например, строчка «angle 70» означает, что игрок будет начинать уровень в заданных координатах, повернувшись лицом на север. В данном случае значение «270» повернет его головой на юг. Еще раз нажми «n», чтобы закрыть окно.

НАСЛАЖДЕНИЕ РЕЗУЛЬТАТОМ

Когда твой уровень окончательно завершен, прошел все стадии шлифовки, то тебе ничего не остается, как испытать замечательное произведение. Для этого используй File > Save as и сохрани уровень в директории с названием (например, VRHome) твоего проекта. После сохранения выбери в верхней части меню раздел «Bsp» и щелкни на подразделе «Bsp_FullVis (qrad -extra)». Теперь твой уровень откомпилирован, и ты можешь использовать его в игре. Для просмотра уровня положи его в папку baseq3/maps и запусти Quake 3. Непосредственно в игре выбери консоль («~») и набери «/set sv_pure 0» (без кавычек) и на следующей строке название своей карты. Например, /map vrhome, где vrhome название твоей карты. Enjoy!

Если у тебя возникнут какие-то вопросы или сложности, не стесняйся - пиши: editor@gamemag.ru. Нескучного тебе Dethmatch-а.

TIPS OF WEB

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

СЛОВО БРЕДАКТОРА

Привет, мэн! Это уже пятая рубрика и пятые TIPSы (юбилей, однако)! Ты рад? Я тоже! Мы надеемся, что тебе все нравится, бла-бла-бла... Но так не бывает. Тогда почему же ты не пишешь нам писем со своим бесценным мнением? Срочно мыль на spec@real.xakep.ru с сабжем creatiff свою критику, свои идеи, свои вопросы. Самые интересные письма попадут в нашу почтовую рубрику :).
Donor-CreatiFF

1

Неплохим тоном является разработка страниц под разные разрешения. Но как сделать так, чтобы для конкретного разрешения грузилась нужная страница? Можно, конечно, сделать стартовой сплэш-страницу, где каждый будет выбирать свое разрешение, но это будет утомлять людей и выглядеть, как минимум, несолидно. Есть способ лучше, а помогут осуществить его снова JavaScript и объектная модель браузера. Сделай index.htm пустым, вставь в него только скрипт, приведенный ниже (640.htm, 800.htm, 1024.htm - страницы, заточенные под разные разрешения):

```
<script language=JavaScript>

switch (window.screen.width)
{
   case 640:
   window.location.replace("640.htm")
   break;
   case 800:
   window.location.replace("800.htm");
   break;
   default:
   window.location.replace("1024.htm");
}
</script>
```

2

Ты знаешь, что фон твоей страницы может быть заполнен как монотонным цветом, так и рисунком. Это прописывается в <BODY>:

```
<BODY background="fignya.jpg"
TEXT="#000000" LINK="#0000FF"
VLINK="#800080">
```

Но ты не знаешь, что можно сделать так, чтобы фон страницы оставался на месте, в то время как текст и другие элементы страницы будет прокручиваться. Если сделать все грамотно, то это выглядит очень стильно. Реализуется этот эффект всего одной строкой. В тег <BODY> надо вписать такое свойство бэкграунда: bgproperties=fixed.
Получится что-то типа этого:

```
<BODY background="fignya.jpg" bgproperties=fixed TEXT="#FF0000" LINK="#00FF00"
VLINK="#FF00FF">
```

3

Маленький суммарный вес паги очень важен для веба, поэтому нужно максимально оптимизировать страницу. Так что не пользуйся графикой там, где это не нужно. Динамический HTML иногда позволяет делать некоторые декорации, обходясь без вмешательства графического редактора. Допустим, ты хочешь сделать заголовок, отбрасывающий тень. Тогда действуй так:

```
<table style="filter:DropShadow(color=silver, offx=2, offy=2, positive=1)">
<tr>
<td>
<h1>Заголовок с тенью</h1>
</td>
</tr>
</table>
```

Также ты можешь заюзать свечение:

```
<table style="filter:glow(color=green, strength=3)">
<tr>
<td>
<h1>RADIATION</h1>
</td>
</tr>
</table>
```

Размытие (проблемы со зрением? Или с монитором?):

```
<table style="filter:blur(add=0, direction=0, strengh=3)">
<tr>
<td>
<h1>Траблы со зрением, сынок?</h1>
</td>
</tr>
</table>
```

Волнистость:

```
<table style="filter:wave(add=4, freq=4, lightstrength=4, phase=4, strength=4)">
<tr>
<td>
<h1>Принтер заело</h1>
</td>
</tr>
</table>
```

Поиграй с параметрами в скобках и во все въедешь. Кстати, картинки тоже можно извращать:

```
<table style="filter:wave(add=4, freq=4, lightstrength=4, phase=4, strength=4)">
<tr>
<td>
<img src="xakep.gif">
</td>
```

Извращаем текст и картинки

4

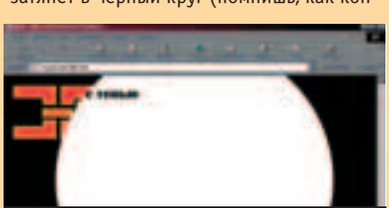
У браузера ИЕ есть встроенные визуальные фильтры, подключив которые, можно немного оживить заход и уход пользователя со страницы. Активизируются они через метатеги. Вот как это делается в принципе:

```
<META http-equiv="Page-Enter" CONTENT="RevealTrans(Duration=время в секундах, Transition=номер эффекта)"> - это при входе
<META http-equiv="Page-Exit" CONTENT="RevealTrans(Duration=время в секундах, Transition=номер эффекта)"> - это при уходе
```

Например:

```
<META http-equiv="Page-Exit" CONTENT="RevealTrans(Duration=5, Transition=2)">
```

- это значит, что когда чел уходит на другую страницу, текущую страницу затянет в черный круг (помнишь, как кончались старые мультфильмы?). Ниже приведен список эффектов с их порядковыми номерами.


Именно так: X с тенью :)

0 Box in (в поле)
1 Box out (из поля)
2 Circle in (в круг)
3 Circle out (из круга)
4 Wipe up (стирание вверх)
5 Wipe down (стирание вниз)
6 Wipe right (стирание справа)
7 Wipe left (стирание слева)
8 Vertical blinds (вертикальные жалюзи)
9 Horizontal blinds (горизонтальные жалюзи)

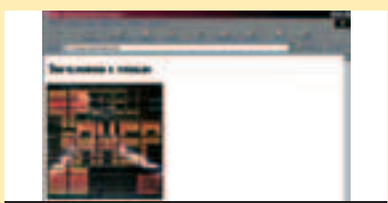
10 Checkerboard across (в шахматном порядке - поперечно)
11 Checkerboard down (в шахматном порядке - вниз)
12 Random dissolve (случайный наплыв)
13 Split vertical in (вертикальная разбивка - внутрь)
14 Split vertical out (вертикальная разбивка - наружу)
15 Split horizontal in (горизонтальная разбивка - внутрь)
16 Split horizontal out (горизонтальная разбивка - наружу)
17 Strips left down (полосы налево вниз)
18 Strips left up (полосы налево вверх)
19 Strips right down (полосы направо вниз)
20 Strips right up (полосы направо вверх)
21 Random bars horizontal (случайные горизонтальные линии)
22 Random bars vertical (случайные вертикальные линии)
23 Random (случайный эффект)

Однако не стоит злоупотреблять эффектами, так как если один раз - это прикольно, то ждать каждый раз, пока эффект отыграет, - задалбливает. Ставь по крайней мере Duration поменьше. Кроме того, при загрузке паги с дайлапа эффекты скорее раздражают, чем радуют.

5 4

Фильтры перехода можно применять не только ко всей странице, но и к отдельно взятым объектам. Например, картинкам. В следующем примере реализуется такая фича: на экране отображается одна фотка, а при щелчке мыши на ней она растворяется, а на ее месте появляется другая. Способы исчезновения можешь выбирать из тех же двадцати трех, указанных ранее (fotka1.jpg и fotka2.jpg - соответственно файлы фоток).
Этот код вставляется между тегами <head> и </head>:

```
<script language="JavaScript">
  function transitionReveal() {
    img1.filters.revealTrans.Apply();
    img1.src = "fotka2.jpg"
    img1.filters.revealTrans.Play();
  }
</script>
```


Здесь применили фильтр к картинке

А этот - туда, где хочешь вставить картинку:

```
<img src="fotka1.jpg"
  width="100" height="100" border="0"
id="img1"
  style="filter: revealTrans(duration=3,tran-
sition=21);"
  onclick="transitionReveal();">
```

6 9

Кроме "украшательных" фильтров в DHTML есть еще и полезные. Например, фильтры, которые отображают картинку относительно вертикальной и горизонтальной осей. В чем полезность? В возможности оптимизировать. Скажем, вместо картинок правого и левого бордюров твоей паги можно залить на сервак и грузить юзверям только одну картинку. Остальное доделает клиентский браузер. А вот и листинг:

<HTML>

```
<HEAD>
<TITLE>bred</TITLE>
<STYLE>
.effect{filter: flipv}
.effect1{filter: fliph}
</STYLE>
</HEAD>
<body bgcolor="#000000">
<IMG CLASS=effect SRC=xakep.gif>
<IMG CLASS=effect1 SRC=xakep.gif>
</BODY>
</HTML>
```


Кручу, верчу!..

7 8

Из-за вечной полунесовместимости бродилок часто случается трабла, когда либо в Осле, либо в Шкафе что-то выглядит не так, как надо. И сколько не бьешься, ни фига не получается. Скрипт поможет и здесь. Мы можем определить юзерский тип браузера и в зависимости от того, MSIE у него или Нетскейп (либо производные от них), поместить в какое-либо место паги соответствующий кусочек, адаптированный к нужной бродилке.
Пример показывает, как вывести надпись или картинку, например, логотипы производителей, соответствующую типу браузера. Для этого тебе понадобится сделать маленькие пикчурки с логотипами (а также третью пикчурку на случай, если эти две не подойдут). Назови картинки с логотипами ИЕ и НН - ie.gif и nn.gif, соответственно, а третью картинку - hz.gif. Далее забей такой код:

<html>
<head>

```
<script language=JavaScript type="text/ja-
vascript">
var vers=navigator.appName;
if (vers.indexOf("Microsoft") >= 0)
{
vers="ie.gif";
}

else if (vers.indexOf("Netscape") >= 0)
{
vers="nn.gif";
}
else
{
vers="hz.gif";
}
var pictura="<img src="+vers+">";
</script>
</head>
<body>
<table>
<tr>
<td width=450>
</td>
<td>
<script language="JavaScript" ty-
pe="text/javascript">
document.write(pictura);
</script>
</td>
</tr>
</table>

</body>
</html>
```

Комменты: функция indexOf возвращает позицию в строке того, что в скобках. Мы ее заюзали, так как ни разу не вспомним, как точно называется Осел или Шкаф (это что-то длинное). Но если в ответе из navigator.appName встретится имя одной из этих контор, то indexOf выдаст хорошую цифирь, и сработает соответствующая ветка условия. Иначе пришлось бы выяснять полное название бродилок.

8 7

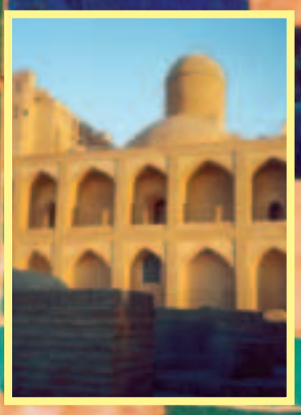
Поскольку мы геморроимся со скриптами, думаю, эта типса не будет лишней. Объявляя какую-нибудь функцию или прописывая цикл, сразу забивай и открывающую, и закрывающую фигурные скобки, а уж потом вбивай между ними команды, которые будут внутри. То же самое со вложенными циклам и условиями. Так ты не потеряешь скобку, и не придется убить кучу времени и нервов на поиск столь дурацкой ошибки.

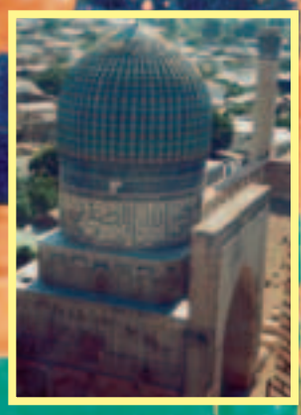
9 6

Все еще трахаешься в "Блокноте"? Похвально. Но, может, хватит геройствовать (читай - геморройствовать). Поставь себе Coffee Cup HTML Editor или CuteHTML. Генерить за тебя ничего не будут, зато нужные места подкрасят, теги вводить помогут. Ну да дело твое.

1 0

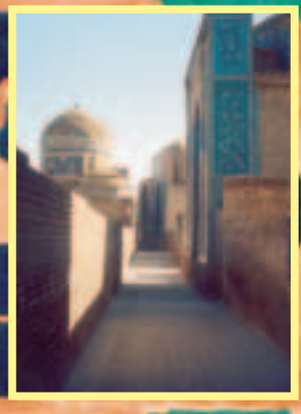
Если ты юзаешь Macromedia Dreamweaver для создания сайтов (кстати, Dreamweaver MX - рулит!), то знай, что под него существует полно мелких дополнений, разрабатываемых самой Macromedia и левыми разработчиками, и называются они Extensions. Это что-то вроде фильтров для фотошопа, только осуществляющих вебовские функции - например, дополнительные фичи для работы с почтой, удобные средства для работы со слоями, навигацией и множество других полезных штучек. Иди по этому адресу и качай, сколько влезет (внизу паги есть раскрывающийся список, где все Extensions разбиты по категориям): http://dynamic.macromedia.com/bin/MM/exchange/main.jsp?product=dreamweaver.











Пальмы, фрукты и интернет-кафе

Записки из сказочной страны Узбекистан

Константин Руденский

«Фрукты – наше богатство»
- надпись на лозунге перед въездом в Бухару.

Точно не знаю, когда мне пришла мысль поехать в Узбекистан. По-моему, когда, учась в университете, я провалил экзамен по исламской архитектуре, у меня в первый раз возникла идея съездить куда-то в те края. Дальше как в плохом кино – «прошло время», и, когда грозящиеся перспективы недельного отпуска стали манить меня своими Шехерезадами, я просто пошел и купил билет в Узбекистан, точнее, в Бухару.

В Узбекистан нужно ехать большой компанией. Чем больше – тем веселее. Эта мысль пришла мне в голову, когда посреди «нового и современного, да, что уж там, без кавычек, действительно нового и современного аэропорта Домодедово я увидел свой рейс. Большинство пассажиров, как я понял, присмотревшись, состояло в основном из усталого вида узбеков с огромными «мешочными» сумками. Посреди всей этой, довольно однородной, как китайцы или негры, на первый взгляд, толпы стоял я – с не-по-местной-моде маленькой сумкой, в шортах и майке, вместо любимых остроносых ботинок, брюк, когда-то бывших строгими и кожаной куртки. Ситуация не накалялась – узбеки народ мирный, ну, разве что, циркониевый браслет провести предложат. Да, если предложат, – то сразу отказывайся – под видом браслета там может быть все что угодно: от наркотиков до атомной бомбы. В общем, чтобы там ни было, врядли хочется потом объяснять на таможне, что это просто тебя попросили кому-то передать. Так не бывает.

Послав мальчика, предлагавшего мне то самое «все что угодно», даже толком не разобравшись, в чем дело, я проследовал в Хава-Юллари, бишь, в самолет узбекских авиалиний, которой и должен был отвести меня в сказку – в ту самую Бухару, о которой я столько слышал и совсем ничего не знал.

ОСТАНОВИТЕ САМОЛЕТ – Я СЛЕЗУ

Волшебство, как известно, нужно выстрадать. Точнее, как гласит пословица, – полюбите меня серенькой… Именно такой серенькой меня и встретила Средняя Азия: потом тел в кожаных куртках в 30-градусную жару, закрытыми наглухо помещениями таможни, в которой пограничник бережно и неторопливо, с восточной обстоятельностью просматривающий твой паспорт, рвущими на части водителями такси готовыми за «долляр» отвести тебя хоть на край света. Ну, на крайний случай, за два доллара. Это не шутка в Бухаре, для европейского человека – настоящий коммунизм. Все действительно стоит в пересчете на московские деньги копейки - и старый лозунг из одного фантастического фильма: «я бы купил это за доллар», снова приобретает свой первозданный смысл. На самом деле, за пределами аэропорта. Бухара – самый гостеприимный город. И там действительно по настоящему сказочно – во всяком случае, когда идешь по старому городу, дом к дому утыканному мазанками, приткнувшимися одна к другой, вспоминаются фильмы-сказки про 1000 и 1 ночь, Ходжа Насреддин все остальное, что было в свое время внимательным образом отсмотрен, будучи у этой самой сказки в гостях. Первая фраза, кинутая мне вслед местным аборигеном, лет, эдак 6-7 была «Hello, mister», я обернулся и крикнул Salom aleikum. Вот она и началась – дружба народов… Во всяком случае, чувствовать себя недружелюбно в этом огромных размеров кишлаке с международным аэропортом просто невозможно. Восточное маслянистое дружелюбие подкупает – не смотря на немалую долю лукавства. Ну, допустим, в любом большом городе, ты подходишь и спрашиваешь: Добрый день – а потом, четко и складно, пока тебя не успели послать, излагаешь то, что тебе нужно, после чего получаешь такой же четкий и сухой ответ. Все куда-то спешат, время – на вес золота. Ритм диктует свои правила: 9:00 - начало рабочего дня, 12:00 - встреча, в 15:00 – дедлайн по очередному проекту. Нужно успеть – быть первым, а лучше первым с отрывом, скорость нажимает - тут уж ничего не поделаешь…

Подойдешь в городе Москве к человеку. Ну, спросишь что-то. В лучшем случае, он тебя спросит: «Что надо?». В средней Азии все совсем по-другому. В начале, если даже тебе нужно просто спросить дорогу, ты подходишь к местному жителю – и завязывается неторопливый, по среднеазиатскому обычаю разговор: как здоровье, как здоровье родственников, здоровье домашних животных и т.д. – все по порядку, не спеша и не торопясь. Только после этого можно подходить к теме, с которой все в итоге начиналось: да, ой, мне же нужно было узнать дорогу. С радостной улыбкой абориген ответит тебе, что, в общем-то, он не очень занят, и, конечно, с удовольствием проводит тебя до места, в которое тебе нужно было

попасть. Конечно, в том случае, если тебе туда еще надо и ты не окончательно и бесповоротно туда опоздал. Хотя, опоздать куда бы то ни было в Бухаре меряется с точностью до дня, к тому же все расстояния в Бухаре маленькие – а улицы запружены маленькими и проворными Daewoo Tico.

Зачем ехать в Узбекистан? спросил меня Ноа. В принципе, как показала практика, в Бухаре можно делать всего несколько вещей: есть, спать, причем, желательно, не одному, и смотреть архитектуру, last but not least. Если употреблять все четыре средства в немедицинских дозах, то через некоторое время сознание кардинально изменится: жизнь замедляется, проблемы большого города, которые нетнет - да и всплывают, постепенно оставят тебя в покое и постепенно организм вполне войдет в роль и приспособится под узбекские, словно нехотя вращающие стрелками, часы. Быть отдыхающим в Бухаре невозможно, потому что и так отдыхают все. Быть деловым, тем более, невозможно, потому что и так никто ничего не делает. Ну, если и делает, то, по крайней мере, незаметно.
Остается один выход – праздно, с полным сознанием своего ничего неделания шататься, периодически залезая на минареты, и, свободно рассевшись и свесив ноги с небольшой жестяной крыши диаметром в 1.5 метра на высоте метров 30, бороться с искушением созвать весь правоверный люд на молитву. Пробраться на минарет – несложно, и, что важно, недорого. Днем это стоит доллар. Ночью – порядка четырех. В услуги по осмотру достопримечательностей входит сопровождение проводником, который смотрит по сторонам и следит за тем, чтобы дорогие гости не свернули себе шею, что, в общем то сделать довольно просто, потому что очень часто памятник может быть более или менее отреставрирован только снаружи, а внутри может царить мрак и запустение. В тот раз, когда я таки забрался на минарет в Регистане, одном и самых красивых религиозных ансамблей Самарканда, мне очень повезло с проводником. И, опять же было очень весело нюхать табак и вести разговор за жизнь – неторопливый и ни к чему не обязывающий, как и все разговоры подобного рода.

INSIDE

Если очень долго не бриться – отрастает борода. Если ходить под солнцем, которое светит прямо на голову, то все лицо загорит и появится желание постричься налысо: очень печет. Если постричься налысо – то придется прикрыть лысину тюбетейкой. Так происходит обузбечивание любого, кто рано или поздно появляется в Узбекистане. Все началось с того, что в какой-то момент я завернул в небольшую парикмахерскую, ммм – даже не парикмахерскую, а цирюльню, в которой жил и работал ее владелец. Нет – серьезно, так оно и было – именно жил и работал. Работал перед небольшим и очень старом совковом кресле. А жил – за занавеской, где стоял топчан и, собственно, все. Парикмахерская 24 часа в сутки по-узбекски выглядит примерно следующим образом: просто заходишь в любое время в парикмахерскую. В любом случае, там никто дверей не закрывает, пинаешь хозяина, хозяин с непонятными, видимо матерными фразами на узбекском просыпается и берет в руки бритву. Нет, вовсе не потому, что он зол на то, что ты его разбудил – просто он действительно готов тебя побрить, постричь, и, сделать все что угодно согласно еще совкового образца прейскуранту, висящему на всегда-открытой двери.
В эту цирюльню заходят все: и местные менты, возвращающиеся со смены, и «обузбечивающиеся иностранцы», которым вдруг приспичило побриться налысо – в общем, все, кто угодно. И. каждый раз, когда на лестнице второго этаже, где, собственно и расположена парикмахерская, слышатся шаги, небольшого роста брадобрей вскакивает с постели и начинает скоблить подбородок очередному званому гостю.

АРАБСКИЕ СКАЗКИ

Как-то раз, когда я был еще совсем фрейдически маленьким, в гостях у сказки был Ходжа Насреддин - народный узбекский герой. Когда был сильно старше, посмотрел Паззолини 1000 и 1 ночь. А потом поехал в Бухару. Так вот – там действительно все совершенно сказочно. Может быть, потому, что ничего не меняется. А может – потому что попадаешь в совершенно другое место, с абсолютно другими законами, принципами и правилами. Могут меняться строи, порядки, власти, коммунизм меряться силами с капитализмом – кардинально в Узбекистан все равно ничего не изменится, т.е., кардинально не изменится – от всех, периодически сменяющих друг друга укладов останутся лишь какие-то внешние или функциональные атрибуты, как например, автомат в руках у чернокожего аборигена с костью в носу. Кость в носу носили 10 поколений его предков, а автомат… А что автомат? - штука то удобная :). Или, допустим, статуи ленина, маркса и энегельса в буддийских храмах Бурятии. Революция прошла, коммунизм, совок и перестройка – тоже, а у статуй партийных классиков, сделанных по ламаистскому канону также дымится лампада и читаются буддийские каноны.

Так же аляповато смотрится протянутый через все центральное шоссе лозунг: «фрукты - наше богатство», или огромная надувная бутылка Кока-колы с еще одним, похожим на предыдущий сло..., нет – лозунгом.
Кстати о Кока-коле: всем фанатам Пепси можно смело отдыхать - в узбекистане производят только Кока-колу. В процентном соотношении потребления Коки и всех остальных напитков Узбекистан далеко преобладает над всеми остальными странами. Просто потому, что других газированных безалкогольных напитков в Узбекистане просто не видно. Видимо, объемы не те. Поэтому, всегда Кока-кола. И никакого нового поколения. Нет такого – все постоянно. Все стабильно. Никто ничего не выбирает, все уже давно выбрано, а с начальством здесь спорить не принято. Количество порядка и спокойствия на один квадратный метр узбекского пространства почти сто процентов. Как говорится, тут бы и жить... но...

НЕ МОЯ МИЛИЦИЯ...

Ментов в Узбекистане действительно много. И при этом, обычные патрули все ездят на очень маленьких машинах Daewoo, которые очень напоминают московскую Оку. Порядок наводится сурово. Не средневеково, но почти – за угон машин – расстрел, за изнасилование – расстрел, в общем, вопрос перенаполненности тюрем решается кардинально – расстрел – и баста. В общем, органы правопорядка в Узбекистане – штука серьезная, почти на уровне «эцелопов» в фильме Кин-Дза-Дза. Уж не знаю, имеют ли они право бить по ночам простых жителей, но держатся крайне важно. В последние несколько лет самыми престижными учебными заведениями стали милицейская академии и институт иностранных языков. Правоохранительная и туристическая области соответственно. Бишь, девочки – налево, мальчики – направо.
Те, кому не посчастливилось попасть в престижное учебное заведение, рано или поздно оказываются в Москве на заработках, и, через какое-то время возвращаются и становятся «большими людьми» - со своим домом и машиной Daewoo в гараже. Так что, если ты в какой-то момент так же случайно окажешься в Самарканде, то скоро заметишь, что русских там любят (в отличие, скажем, от Ирана), а некоторые даже до сих пор жалеют, что распался Союз. О чем может вестись долгий разговор за чаем, которым могут напоить где угодно и кого угодно, даже случайного прохожего, подошедшего спросить дорогу – узбеки гостеприимны до демьяновой ухи.
Впрочем – и точно также спокойны ко всякого рода вторжениям. Когда я случайно перепутал дом, зашел, обвешанный сумками в первый попавшийся двор и стал уже располагаться, практически уже расположился и успел выпить чаю с хозяйкой дома, только тогда выяснилось, что я ошибся адресом и перепутал одну узбекскую хозяйку дома с другой.

ПРИКЛЮЧЕНИЯ ЯПОНЦЕВ В УЗБЕКИСТАНЕ

Японские туристы, – непременная часть ландшафта, свойственного любому историческому месту. Достопримечательности манят соратников и потомков самураев с силой просто неодержимой – во все время моего пребывания в Узбекистане повсюду сновали группы японских туристов, ведомых местными экскурсоводами. Нашествие японских туристов началось уже лет семь-восемь назад, как только в туристические агентства в стране Восходящего Солнца стали поступать сведения о том, что в Бухаре все спокойно, в Самарканде все спокойно, одним словом, с тех пор нельзя ни шагу ступит не наткнувшись на обрывки незнакомой речи – хотя, если честно, за неделю пребывания она стала просто знакомее некуда. И еще японцы дико любят все фотографировать. Когда уже устаешь закрываться рукой от объектива (телезвезда, блин), то начинаешь бороться с врагом его же оружием. Как сейчас помню, как бегал за одной японской девушкой, склоняя ее к тому, чтобы сфотографировать на фоне величественной восточной архитектуры. Японка отказывалась, улыбалась и пыталась скрыться в ту сторону, где исчез последний японец из ее группы. Я настаивал, мой английский становился с каждой фразой все лучше и лучше. В общем, все это безобразие длилось пока, наконец, я не почувствовал себя отмщенным и не отправился восвояси. Все же нечестно – любить фотографировать – и не любить фотографироваться.

ПАВЛИНЫ ГОВОРИШЬ?

Когда, сидя в интернет-кафе снова нашариваешь связь с большим городом, где провайдер не сидит на dial-up'е (а вот в Узбекистане - сидит), интернет быстр – а за окном, всегда что-то происходит, на какой-то момент хочется кинуть весь тот покой, которым сказочная страна Узбекистан окутывает каждого прибывающего. Через некоторое время это проходит – отлипаешь таки от монитора, оглядываешься вокруг – интерьер интернет кафе интернационален, ну, разве что отличается небольшим портретом Каримова, скромно, боком висящего на админском месте. И еще медленным интернетом. Во всех остальных отношениях герой небезызвестного фильма про Восток был абсолютно прав – хороший дом, верная жена, что еще нужно, чтобы встретить все что угодно. Да, и еще – в Узбекистане водятся павлины. Настоящие. Как в том фильме ;).

Чтобы попасть в Узбекистан, must have:
Билет на самолет - купить.
Взять с собой: паспорт, любой – хочешь, гражданский, хочешь, заграничный – визового контроля в Узбекистане нет.
Пройти таможенный контроль в бухарском аэропорте - очень жестко.

Чтобы не ехать в сказочную страну Узбекистан, стоит:
Читать: Узбекские сказки - (там все правда).
Смотреть: Паззолини 1001 ночь, Ходжа Насреддин (Узбек телефильм, 1932г), художественный альбом: Бухара. Уникальные памятники древности.
Ходить в: Турецкие бани, в харчевню Синдбад.
Есть: немытые фрукты и овощи, шашлык и рахат лукум.

ЗВЕЗДА И СМЕРТЬ ХОАКИНА МУРЬЕТЫ

(часть вторая, неизвестная)

Niro
(niro@real.xakep.ru)

В середину живота что-то кольнуло, потом еще и еще раз; интенсивность нарастала. Не видя ничего, существо знало, что где-то там сейчас обрывается нить спокойной жизни. На мгновение стало темно, потом перед глазами вновь расплывчато заблестела воронка. Это оно (она?..) МОРГНУЛО. И уже не могло прекратить это делать.

Кругом была вода. Много теплой мутной воды, которая плескалась вокруг головы, плотно обжимала живот и грудь, заставляла руки и ноги периодически всплывать к той стенке, что закрывала мир сверху. Дышать было невозможно - но и не хотелось. Просто в этом не было потребности, так как знания о дыхании еще были недоступны. Периодически что-то встряхивало окружающий мир - что-то далекое, не страшное. Тогда становились ощутимыми и стенки, закрывающие мир со всех сторон, - они были твердыми, но одновременно четко определялась их хрупкость, они были тонкими, как мыльный пузырь.
Совершенно не хотелось ни есть, ни пить. Вода, в которой находилось существо, ощущающее мир, удовлетворяла все потребности. Казалось, покою не будет конца...

«POWER»

Пришла мысль... Странное состояние. До этого он никогда не думал, а сейчас вдруг испытал в этом потребность. И к нему пришла мысль. Он не понимал, какая, не понимал, зачем. Где-то внутри него, не там, где вода, что-то шевельнулось; приятное ощущение. В большой голове зародилось нечто разумное, толкающее наружу, за стенки.

«UPDATE SUCCESS...»

Вдоль спины, где при касании стенок определялись какие-то острые выступы (позвонки?), пробежала волна покалываний и парестезий. Он (оно?) понял (поняло?..), что стенки не являются непрерывными, где-то прямо над головой есть выход, до этого момента невидимый, да и не нужный по причине отсутствия побуждений. И вот сейчас захотелось увидеть выход, увидеть провал в стенках (или нечто в виде закрытой воронки?). Там, за сфинктером, другой мир (что это такое?). Насколько обосновано желание сменить теплое мокрое убежище на то, что откроется за стенками? Нет ответа.

«ENTER LOGIN...»

Толчок. Это стенка, внезапно приблизившись к нему справа, пихнула в плечо. Раньше такого не было. Толчок повторился - на этот раз слева.

«ENTER PASSWORD...»

Мир менялся. В его убежище не было свободного места, поэтому волны по воде расходиться просто не должны, но... Внезапно появилось новое (пятое, шестое, седьмое?..) чувство, которым он уловил колебания, пронизывающие окружающую среду. В голове словно включился компас, который с максимальной точностью определил направление, по которому воду пронзали невидимые импульсы.

«STARTING PROCESS...»

Захотелось повернуться - увидеть то, что над головой. ВЫХОД. Но подвешенное в воде тело не могло дотянуться ни до одной из стенок, волновые колебания среды удерживали существо точно в центре. Маленькие руки и ноги (голова-то большая!..) не могли справиться с этой сложной задачей. Толчки стали заметнее; злее, что ли. Один из ударов изменил положение существа в пространстве, воронка оказалась прямо перед (глазами?.. вот эти штуки на голове - глаза?!). Тут же захотелось отвернуться, не видеть того места, той горловины, которая вот-вот хотела распахнуться. И вдруг толчки прекратились...

«PLEASE WAIT...»

В середину живота что-то кольнуло, потом еще и еще раз; интенсивность нарастала. Не видя ничего, существо знало, что где-то там сейчас обрывается нить спокойной жизни. На мгновение стало темно, потом перед глазами вновь расплывчато заблестела воронка. Это оно (она?..) МОРГНУЛО. И уже не могло прекратить это делать.
К отлаженной неизменной картине добавились три момента: хотелось смотреть, дышать и избавиться от молний, методично штурмующих живот (пупок?..).
И как только осознание этих новых ощущений пронизало существо сверху донизу, раздался мощный удар откуда-то сзади, от ног; что-то толкнуло под (...? Как называется?!). Внезапно в память извне ворвалось понимание: «Жидкости несжимаемы». Как только давление на тело выросло до критической величины и готово было запихать глаза внутрь мягкой, податливой головы, случилось событие, моментально разрушившее все прежние стереотипы. Воронка стала раскрываться, выпуская жидкость наружу.
Страх охватил существо.

«GENERATING SCRIPT...»

Зев воронки не обещал ничего хорошего. Уровень воды тем временем значительно уменьшился. Еще один толчок подтолкнул его голову к сфинктеру воронки; мягкие, но цепкие объятия удержали, не дали вырваться.
Проваливаясь в воронку, существо чувствовало, как за ним тянется что-то длинное, извивающееся, рвущее живот. Голову сплющило, вытянуло по ходу воронки, оказавшейся на самом деле вхо-

Это был ребенок. Без возраста, без пола, без имени. Ничьи руки не приняли его в свои объятия...

дом в трубу со скользкими розовыми стенками. Стало больно, шею выгнуло кзади (больно?.. больно!!!).
«ERROR. SORRY, RELOADING. STRUCTURE RECOVERED».
Новые толчки и объятия трубы неуклонно влекли за собой. Что-то новое, доселе неведомое, вырисовывалось у выхода. Это «что-то» называлось «Свет», и оно (он?.. она?..) это знало.

«RANDOM GENERATOR INACTIVATED»

Зажмуриться не успел. Последняя молния ударила в живот и утонула в нем, не причинив вреда. Все сразу стало ясно.

БОЛЬ. ДЫХАНИЕ. МЫСЛИ. ПУПОВИНА (вот!). ВЗГЛЯД. ПОВОРОТ ГОЛОВЫ, НАКЛОН.
ПОЛНЫЙ РОТ СЛЮНЫ.
РВОТА.

«WELCOME!»

Это был ребенок. Без возраста, без пола, без имени. Ничьи руки не приняли его в свои объятия; полотенце не обтерло его; никто не шлепнул по попе, чтобы услышать...
Ребенок открыл рот, из угла которого стекала струйка желчи, и густым мужским голосом произнес:
- Procedure begin...
И на непослушных еще ногах сделал несколько шагов навстречу своей смерти. Но до нее еще надо было дойти...

«СТАНДАРТНАЯ ПРОЦЕДУРА ВХОДА. ЗАПИСЬ КОНТРОЛЬНЫХ ТОЧЕК КАЖДЫЕ ДЕСЯТЬ МИНУТ»

Ему приказали выкопать эту яму. Он не знал, кто; он никогда его не видел - того, кто раздает указания и проверяет их выполнение. Приказ созрел в Его голове будто бы сам собой. Внезапно появилась огромная черноземная пустошь, бескрайняя и безжизненная на первый взгляд; Он стоял где-то там, где должна была быть середина этого мира, и смотрел себе под ноги, немного погрузившиеся в мягкую, почти бархатистую почву. Рядом с Его правой ступней в землю был вбит маленький колышек с красным флажком; ветра здесь не было, флажок висел неподвижно и не был похож сам на себя, словно яркий шнурок.
Ковырнув ногой землю, Он присел на корточки и дотронулся до черных комочков руками, пропустил их сквозь пальцы. Тихое шуршание сопровождало эту процедуру («Знакомое слово...»).
На душе было муторно; грусть подпирала горло вонзившейся стрелой.
Ноги затекли. Он встал и увидел рядом с собой лопату, воткнутую в чернозем рядом с колышком. Обыкновенная лопата с затертым до блеска черенком; множество таких же рук ласкали его неоднократно, превратив в сверкающий столб. Он коснулся лопаты, не веря в ее реальность. Пальцы ощутили дерево; нашлось несколько щербинок. Где-то у основания виднелась наполовину сорванная этикетка.
Он медленно протянул правую руку и крепко обхватил черенок. С усилием вытянув лопату и, отряхнув с нее прилипшие жирные комья земли, придирчиво осмотрел лезвие. Оно было заточено, но не было новым - несколько хороших выемок, помнящих камни, о которые лопата спотыкалась давно и не очень, утвердили Его в мысли, что кто-то уже выполнял эту работу раньше. Незаметный порыв противно теплого ветерка колыхнул флажок, напомнив о том, что пора начинать. И в ту же секунду где-то далеко, там, где горизонт, заурчал кто-то большой и невидимый. Тревожный взгляд вдаль не дал ничего. Пару раз обернувшись вокруг, Он не увидел ничего и никого, способного издать подобный рокот.
Лопата ударила в землю. Рокот стал приближаться.
Первый ком земли отлетел в сторону и упал, развалившись на множество мелких, в паре метров от колышка, в той стороне, откуда надвигался звук. Работа закипела.
Еще одна лопата. Еще одна. Десятая. Сотая.
Расстояние сокращается, но очень медленно. Это можно определить по тому, что мощность звука еле заметно усиливается, в нем уже можно различить тоны разных высот; кучка земли рядом с колышком неуклонно увеличивается. Хотелось бы быстрее, но это за пределами возможностей.
Он вспоминал свое рождение, размахивая лопатой в пустыне. Вспоминал, как неизвестная мать исторгла из себя тело, покрытое слизью; как выстрелил в глаза свет; как сам собой открылся для первых слов рот. Пот покрывал Его лоб, плечи, ложбинки между лопаток и над ключицами, заливал глаза и щеки. Клинок вонзался в землю, проникая в него полностью до основания черенка; ногами помогать не приходилось. Ком отваливался вбок и оказывался на лопате; бросок - капли пота летят с волос следом...
В какой-то момент Он, наконец, убеждается в том, что яма углубляется быстрее, чем подступает звук. Это придало Ему уверенности. Движения стали более четкими, торопливости поубавилось. Формирующееся углубление напомнило Ему выплюнувшую его воронку; Он ухмыльнулся и рубанул лопатой точно в середину, словно мстя за свои жуткие роды.
Звякнул первый камень.
Настороженность мгновенно вернулась на прежнее место в голове. Приблизив клинок к глазам, Он разглядел новую зазубрину рядом со старыми, она отчетливо бросалась в глаза, словно укоряя в излишней расслабленности. Проведя пальцем по краю лезвия, Он убедился в реальности изъяна и посмотрел вниз, туда, где из пушистого чернозема торчал кусок гранита.
Условия задачи изменились.
Он присел в яме, края которой были уже на уровне поясницы, разглядывая неожиданно возникшее препятствие. Камень был еле виден; руками Он раскидал землю с его верхушки и с радостью убедился, что не все так плохо - камень был невелик, сил хватило выворотить его из ямы наружу и оттащить к основанию земляной пирамиды. Спрыгнул обратно и кончиком лезвия потыкал дно - осторожно, боясь повредить его. Ничего. Махнул сильнее, вонзаясь в чернозем.
«Клац!»

«ПЕРЕПОЛНЕНИЕ БУФЕРА. ВОЗМОЖЕН ВНУТРЕННИЙ КОНФЛИКТ. ИЗМЕНИТЕ УСЛОВИЕ ВХОДА...»

Примерно через полчаса на поверхности земли лежали уже шесть огромных гранитных валунов, по десять-пятнадцать килограммов каждый. Сил заметно поубавилось, из-под ногтей сочилась кровь. Лопата постепенно становилась не нужна - она просто не пролезала между камнями. Работать приходилось в основном руками.
На некоторое время Он перестал замечать шум вокруг себя, сосредоточившись на своем труде. Ворочанье камней поглотило его, стало смыслом жизни на короткий промежуток времени. Глыбы были с острыми гранями, примерно одного размера. Казалось, что кто-то специально сделал их для Него; камни не мельчали, не уходили в сторону.
Один раз он не удержал камень в руках и уронил его вниз с бруствера. Импульс боли, начавшись от большого пальца левой стопы, ударил сквозь всю ногу в поясницу, заставив закричать.

«СБОЙ СТАНДАРТНОЙ ПРОЦЕДУРЫ ВХОДА. ПОВТОР ОТ КОНТРОЛЬНОЙ ТОЧКИ. УДАЛЕНИЕ ОШИБОЧНЫХ ФРАГМЕНТОВ...»

И от этого крика гранитная глыба сама шевельнулась у его ноги, которую он так и не смог отдернуть, аккуратно поднялась в воздух и, перевалив через край ямы, отправилась к своим собратьям. Крик замер сам собой...
«ПРОЦЕДУРА ПРОДОЛЖАЕТСЯ. ОТЛАДЧИК ФУНКЦИОНИРУЕТ ИСПРАВНО...»
Он попробовал так поступать с другими камнями, но сколько ни кричи на гранитные куски, они не двигались с места - все-таки приходилось руками вытаскивать их из грунта и тащить наверх. Одно было хорошо - с каждым извлеченным камнем яма углублялась настолько, насколько можно было это сделать, отбросив пять-шесть лопат. Скоро Он ушел в землю по плечи.

ЗВЕЗДА И СМЕРТЬ ХОАКИНА МУРЬЕТЫ

И в ту же секунду Он понял, что теперь яма скрыла его полностью; КОСА ОТСЕКЛА ЛИШНЕЕ.
Рокот удалялся; существо без имени стояло в яме, не ощущая боли и не понимая смысла происходящего. На его глазах голени, лишь минуту назад извергавшие из себя струйки крови, превратились в гранитные глыбы.

На этом этапе организм просто завопил об отдыхе. Подцепив кончиками пальцев очередную глыбу, Он поставил ее на одно из ребер, превратив в некое подобие сиденья, и опустился на него. Ныли руки, ноги, спина. На ручейки пота Он уже давно перестал обращать внимание, сконцентрировавшись на рокоте, приближающемся с завидным постоянством.
Где-то наверху валялась ненужная лопата. Захотелось узнать, что же такое все-таки гудит и рокочет. Он встал, протянул руку к лопате и, уложив ее поперек ямы (могилы?...), подтянулся и выскочил наружу. Горизонт со всех сторон был чист...
Не со всех. С той стороны, где был вбит исчезнувший куда-то флажок, оставив после себя маленькую дырочку в земле, приближалось некое пыльно-туманное облако, отхватившее приличный угол горизонта. Звук четко идентифицировался с этим облаком.
На мгновение яма показалась спасительным убежищем. Вот для чего был отдан приказ выкопать ее - чтобы спрятаться в ней от надвигающегося кошмара.
Нелогично. Неужели нельзя было просто попытаться за то же самое время просто уйти с дороги, которую прокладывало себе облако пыли, тумана и смерти?
Груда камней подсказала ответ - «нельзя». Он здесь как данность, как условие задачи. Есть цель - укрыться в яме (окопе?!..). Выполняй. Сумеешь - останешься в живых. Не сумеешь - воронка выплюнет следующего, и уже он, не Ты, будет ворочать гранитные валуны, слушая приближающийся рокот облака-убийцы. Не по-человечески - но что поделать?
На глаз оценить расстояние до того «нечто», что надвигалось на яму и на Него в яме, было сложно; в этом мире вообще трудно было понять что-либо.
«Либо я вырою окоп, либо могилу».
Эта мысль подстегнула Его. Забыв об усталости, вновь принялся ворочать камни, с завидным постоянством появляющиеся из земли, как грибы после дождя (это при условии, что Он понятия не имел ни о дожде, ни о грибах). Рокот приближался, облако приобретало все более четкие очертания, оставляя за собой дымный шлейф длиной в несколько километров. В очередной раз разогнувшись в яме, чтобы от плеча толкнуть глыбу наверх, он так и замер с ней на плече, забыв о ее весе.
К нему приближалась «адская машина». Подобие комбайна, сенокосилки, бензопилы и танка в одном корпусе, размером с многоэтажный дом. За пылевым облаком не было видно, что служит опорой - колеса, гусеницы или, может быть, какие-нибудь механические ноги. Скорость машина развила приличную; в воздухе сверкали сотни, тысячи пил, кос, ножей, цепей и мечей. Один большой металлический самурай - и он мчался прямо на яму со стороны, на которой была насыпана куча земли вперемешку с гранитными валунами.
Несколько пил гремели где-то у самой земли, периодически скрываясь в клубах пыли. Взглянув на самого себя, высовывающегося из ямы по плечи, Он хмыкнул, посмотрел под ноги и, швырнув камень обратно вниз, присел на него - потом посмотрел вверх, лишний раз убеждаясь, что от макушки до бруствера около полуметра. Оставалось только ждать, когда «танк» пройдет над его головой; конечно, существовала задача быть засыпанным землей, но это уже была другая история. Он выполнил условие - яма выкопана и скрыла его с головой от нашествия неведомой «адской машины».

«ОБНАРУЖЕН УЗЕЛ ВЕТВЛЕНИЯ. НЕОБХОДИМ БЕЗУСЛОВНЫЙ ВЫБОР»

Привалив лопату к стенке, Он принялся пальцами счищать с нее прилипшую землю, пытаясь сохранять спокойствие. Рокот (грохот!..) приближался, заложило уши, с краев ямы стала сыпаться земля - прямо на голову. С минуты на минуту ожидая появления над собой металлического чудовища, Он напрягся, сжал черенок лопаты до хруста пальцев (боялся потерять ее и не суметь потом откопать самого себя).
И когда вдруг из земли на уровне его колен вынырнула изогнутая коса из нержавеющей стали, он понял свою ошибку. Яма не спасала - она определяла Границу.
Коса свистнула и, поддев лопату и отшвырнув ее как щепку, отрубила ему ноги - Он увидел свои суставы, из которых хлестала кровь и синовия («Откуда я знаю все эти слова?..»). Боли не было - но он машинально соскользнул с камня за отрубленными голенями, которые повалились набок, как неживые столбики, и воткнулся в чернозем тем, что осталось от бедер.

«УЗЕЛ ПРОЙДЕН»

И в ту же секунду Он понял, что теперь яма скрыла его полностью; КОСА ОТСЕКЛА ЛИШНЕЕ.
Рокот удалялся; существо без имени стояло в яме, не ощущая боли и не понимая смысла происходящего. На его глазах голени, лишь минуту назад извергавшие из себя струйки крови, превратились в гранитные глыбы.
Небо над ним изменило свой цвет на темно-алый. Какой цвет был до этого, вспомнить не представлялось возможным. Потянуло ветерком, запахло мятой. Боясь пошевелиться, Он протянул руку за спину, нащупал лопату и поднял ее над головой, положив по диаметру. Попытался подтянуться на руках - и вдруг увидел, что его руки сжимают не лопату, нет.
Винтовку с потертым прикладом и потрепанным ремнем. А в середине, у затвора, ярко отсвечивала алым линза оптического прицела. Он отпустил оружие и устало привалился к стенке, тупо глядя на быстро затягивающиеся раны на бедрах. Потом потерял сознание...
Очнулся он оттого, что стало темно. Глаза привыкли, что сквозь закрытые веки все время пытается пробиться лучик алого света; и когда свет исчез, в мозг толкнулся сигнал, предупредивший об опасности.
Глаза Он решил открывать медленно (вдруг кто-то на него смотрит?). Сквозь маленькую щелочку ничего не было видно - темнота была практически абсолютной. Руки, сложенные на груди, опустились вниз - Он по-прежнему сидел в яме, привалившись спиной к земляной стенке. Пахло черноземом и кровью.

Проваливаясь в бездонный колодец, Он улыбался во сне и только крепче сжимал винтовку...

Ощупал ноги - ниже колен их не было. Причем впечатление создавалось такое, что там их не было никогда. Он не помнил, как выглядят стопы, как носят обувь, как болят мозоли на пятках. Он был таким всегда - коротким, спрятанным в яме среди темноты и одиночества. И еще - где-то здесь была винтовка.
Взгляд вверх не прояснил картины. Весь мир стал черным. Так живут слепые. Он знал, что он не слепой; он знал, что он ВИДИТ темноту.
Оттолкнулся от земли, встал на култышках. Тут же упал вперед, благо, яма была достаточно узкой, и падать было практически некуда. В волосах набилось много земли, которая посыпалась за шиворот.
Держась левой рукой за стенку, поднял правую вверх и нащупал там холодную сталь ствола и теплый приклад. Обхватив винтовку, он сдернул ее вниз и опустился туда, где его тело создало выемку в податливом черноземе.
Едва винтовка очутилась в руках, на Него нахлынуло спокойствие и уверенность - будто к нему вернулось что-то родное и необходимое, без чего жизнь теряла смысл. Он погладил ствол, нащупав отверстие на его конце; любовно провел пальцами по мушке. Подышал на линзы прицела; приложил к прикладу щеку, зажмурившись от удовольствия.
Спокойствие убаюкало Его, он обнял оружие и задремал...
Когда под (ногами?.. обрубками?) распахнулся люк, в который посыпался чернозем, Он даже не пошевелился. Проваливаясь в бездонный колодец, Он улыбался во сне и только крепче сжимал винтовку...

Вонь просто отшибала мозги. Она проникала в самую суть, внутрь всего - мыслей, движений, желаний; она насытила воздух вокруг и проникала с каждым вдохом в легкие. Чувствовалось, что на лице от этой вони сама собой скорчилась гримаса отвращения, морщины едва не сплющили глаза и щеки. Такого отвратительного запаха Он не ощущал никогда за свою короткую насыщенную жизнь.
Концентрация вонючих флюидов превысила все возможные нормы; к горлу подступила тошнота. Он отрыгнул воздухом и открыл глаза.
МУСОРНЫЙ БАК.
Банально. Снайпер в помойке.
На уровне глаз шел ржавый ободок квадратного мусорного бака, заваленного по самый верх всякой гадостью различной консистенции. Внутри этого вонючего хлама, обложенный со всех сторон полиэтиленовыми пакетами с дерьмом, Он и сидел (или стоял, что невозможно было отдифференцировать).
Прямо перед носом лежал гнилой помидор. Он потихоньку сочился смрадным соком и радостно подставлялся солнцу почерневшим боком. Вытащив левую руку из глубины, если не с самого дна, помойки, Он брезгливо взял помидор двумя пальцами и вышвырнул наружу. Тот шлепнулся на землю за пределами бака; этот звук заставил оглядеться получше.
Для этого пришлось собрать в кулак всю волю, отложить оружие (точнее, оставить его торчать, словно палку, тесно зажатым несколькими мешками с мусором прикладом кверху) и попытаться подняться над краем бака. Он принялся карабкаться вверх, словно выбираясь из болота.
Тут же вспомнил, что нет ног ниже колен; и тут же понял, что не знает, что такое «колени». Разбросав руки по пакетам, тухлым яйцам и ухватив что-то пушистое пальцами правой руки (скосил глаза вправо - в кулак зажата голова куклы Барби, вымазанная в чем-то коричневом), начал вытаскивать себя вверх, как барон Мюнхгаузен за косичку. Вначале было трудно - некоторые пакеты разорвались, обдав его очередной волной вони и испачкав пол-лица в протухшем майонезе. Но потом пошло лучше, скоро он уже мог выглянуть из своего «убежища».
Кроме неба (обычного синего неба с редкими облаками, которое он уже видел над собой, едва открыл глаза), вокруг помойки оказался довольно грязный квартал неизвестного города. Серые домишки, наползавшие один на другой, кривые пожарные лестницы, разбитые окна - короче, голливудский вариант Гарлема.
Продолжая смотреть по сторонам, Он нащупал рядом с собой приклад и вытащил винтовку на поверхность. Вся она была выпачкана - ствол кетчупом, цевье чем-то непонятным с запахом плесени, приклад - все тем же мерзким майонезом. На счастье рядом оказался кусок тряпки, бывший когда-то рубашкой или футболкой с надписью «RED BULLS FOREVER». Им Он и обтер винтовку. Каплю кетчупа на линзе окуляра, как это ни было противно, пришлось слизнуть, чтобы не повредить чувствительную оптику.
Все-таки противно. Вырвало. Вспомнилось Его рождение и струйка желчи в углу рта - так же, как и сейчас.
Осмотревшись вокруг, Он узнал, что рядом с его помойкой стоят в ряд еще три таких же полных под завязку ящика, из которых выпирают мешки с мусором. Сбоку раздались шаги. Седая старенькая негритянка приблизилась к дальнему баку и молодецки зашвырнула многокилограммовый мешок с мусором на вершину кучи дерьма, после чего отправилась прочь. За ее спиной раздался скрип, шум, потом грохот, и пакет повалился на землю, лопнув по шву и явив на всеобщее обозрение кучу фантастического мусора - огромное количество заплесневелых булок, грязные тряпки, испачканную одноразовую посуду...
Снайпера она не заметила.
Он откинулся назад, будто в кресле; один из мешков очень удачно расположился под головой. Над ним в небе плыли пушистые (как чернозем... только белые) облака, подгоняемые ветром (стороны света определить не представлялось возможным, так же как и направление этого ветра). Умиротворенность накатила на него дремотой; никакое «амбре» не могло перебить благостное состояние души. Впервые за свою короткую жизнь он оказался там, где было до жути комфортно - и это оказался мусорный бак.
Шум на улице отдалился и затих; сон накатил на него, глаза медленно закрылись. И он увидел первый сон в своей жизни.
Длинный коридор, достаточно узкий даже для двух человек. Длинный настолько, насколько позволяло воображение, которое во сне позволяло практически все. Он сидел на корточках, прислонившись спиной к стене, рядом с дверью, от которой начинался (или которой заканчивался) этот коридор. Обычные стены, обычная ковровая дорожка, уходящая в бесконечность. Цель нахождения под дверью была крайне неясна. Он сидел спокойно, даже не шевелясь. Ноги не затекали; двигаться не хотелось. Периодически он бросал косые взгляды на дверную ручку, не поворачивая головы.
Ручка была отполирована множеством рук, до него открывающих и закрывающих ее; материал, из которого она была сделана, был неизвестен, но был, похоже, в прошлом каким-то деревом. Формой напоминая застывшую каплю, летящую по горизонтали, она притягивала его взгляд; вскоре он понял, что смотрит на нее, не отрываясь. В ее сверкающей поверхности отразилось его лицо, которого он никогда раньше не видел, - тонко очерченные черты, сжатые волевые губы, глаза неопределенного цвета; и все это было искажено до неузнаваемости в искривленной поверхности ручки.
Вдали послышались шаги; во сне со слухом были какие-то проблемы, все казалось приглушенным (или дорожка скрадывала звуки). Кто-то шел к двери по длинному коридору.
Он узнал этот звук, который никогда не слышал (информация порой приходила к нему безо всякого желания, врывалась в его мозг и давала ответы на возникающие вопросы). Это был стук каблуков женских туфель.
Голова повернулась сама собой. Глаза отметили, что периодически ковровая дорожка прерывалась, из-под нее выглядывал паркет. Вдалеке мягкий стук по ковру сменился стуком по деревянному паркету. Точно, это туфли на шпильке. К нему приближалась женщина.
Она увидела его издалека, остановилась в недоумении. Он поднялся с корточек, разгладил брюки и поправил воротник на рубашке. НОГИ У НЕГО БЫЛИ.
Женщина производила впечатление фотомодели. Все ее признаки - стройная фигура, высокая грудь, красивые ноги, длинные ухоженные волосы - присутствовали; на ней было белое полупрозрачное платье, заставившее его сердце биться быстрее.
Он попробовал улыбнуться.
Она сделала шаг назад. А потом закричала.
Дверь с грохотом распахнулась и ударила его, стоящего всего в полуметре. До этого мгновения он и не подозревал, что

ЗВЕЗДА И СМЕРТЬ ХОАКИНА МУРЬЕТЫ

...Вдоль переулка у подъездов кучками стояли люди; они о чем-то беседовали между собой, совсем не замечая, как из одного из мусорных баков на них смотрит неизвестное существо со снайперской винтовкой.

дверь открывается в коридор. Сильный удар ручкой в живот швырнул его на стену; он ударился затылком и на секунду потерял из виду красавицу, пронзительно кричащую - до боли в ушах. От удара на несколько секунд вырубилась ориентация, потолок поплыл в сторону, пришлось упасть на пол - мир рушился вокруг него, стараясь обмануть вестибулярный аппарат. Удар коленями о паркет (настоящими коленями!!!), падение лицом вперед, попытка перевернуться на спину...

В лицо ему смотрел ствол помпового ружья. Чернота дула перемещалась с одного его глаза на другой; хозяин ружья с остервенением переводил ствол туда-сюда, тяжело дыша и роняя слюни на лицо лежащего на полу пленника. Несколько секунд все ждали выстрела. Потом человек с ружьем протянул левую руку, которой поддерживал ствол, в сторону женщины и махнул ей ладонью:

- Проходите! Скорее!

Ей пришлось перешагнуть через голову, чтобы войти в дверь. Он поднял глаза туда, где было то, что скрывало платье... Сильный удар прикладом в висок заставил его потерять сознание. Но он запомнил на всю жизнь красоту НАСТОЯЩИХ ног...

Открыв глаза в реальном мире, он понял, что кто-то швырнул в мусорный бак пластиковый ящик для пива с проломленным дном и попал ему в голову. Было практически не больно, он вспомнил звон в голове от удара прикладом (а было ли это?...), сравнил - все говорило в пользу ящика. Мысленно проклиная того, кто не дал ему разглядеть до конца великолепные женские ноги, он нащупал винтовку и увидел, что к стволу прикреплена записка при помощи обыкновенной бельевой прищепки. Он отстегнул ее и прочитал.

«ДЕВОЧКА С МЕДВЕЖОНКОМ».

Крупные корявые буквы, кусок туалетной бумаги. Заказ для киллера. Впечатляет.

Вновь исполнив трюк с раскидыванием рук по мусорным мешкам, он принял полностью вертикальное положение и приподнялся над краем бака. Улица (или, точнее сказать, переулок) великолепно просматривалась в обе стороны; крыши домов и балконы нависали над асфальтированной мостовой, местами полностью закрывая небо. Вдоль переулка у подъездов кучками стояли люди; они о чем-то беседовали между собой, совсем не замечая, как из одного из мусорных баков на них смотрит неизвестное существо со снайперской винтовкой.

Все было просто идеально для выполнения работы, кроме одного - не было девочки с медвежонком. Несколько раз оглядев переулок, Он убедился в том, что никаких детей - ни девочек, ни мальчиков - не было вообще, словно все люди, населяющие окружающие дома, были бездетными. Не было слышно детского смеха; не звенели звонки велосипедов, не шлепал по стене мяч, никто не кричал из окна «Джек, немедленно домой!». Здесь не было детей - или их с какой-то целью искусно прятали, прекрасно зная о существования снайпера, охотящегося за ними.

Пришлось крепко задуматься над происходящим. Прищурив глаза, Он внимательно осмотрел все видимые с позиции окна домов; практически все они были закрыты шторами, скрывая частную жизнь очень тщательно. Потом поискал взглядом бельевые веревки в надежде обнаружить детские вещи, сохнущие на солнце. Безрезультатно.

НИКАКИХ ДЕТЕЙ. И никаких данных, говорящих о том, что в этом мире они существуют в принципе. Оставалось надеяться на благоразумие того, кто написал записку.

Солнце начало припекать. Тучи мух окружили прячущегося в помойке стрелка, жужжанием порой перекрывая шум улицы. Летающие насекомые лезли в рот, глаза, уши, набивались за воротник; и поделать с этим было ничего нельзя - вся голова была покрыта чем-то сладким, волосы прилипли ко лбу; потек сладкий пот. Это начало переполнять чашу терпения.

Вытащив на поверхность винтовку, Он пристроил приклад к плечу и стал в прицел рассматривать окна, закрытые занавесками, надеясь при помощи зумминга пробиться сквозь них. В некоторых квартирах горел свет, хотя на дворе день был в самом разгаре - в этих окнах были видны силуэты перемещающихся людей, ни одного детского среди них не было.

Поиграв со спусковым крючком, Он убедился в легкости и мягкости его, провел стволом над головами ниггеров и посмотрел на яркое голубое небо, словно ища там совета. Потом опустил винтовку и положил ствол на край бака. И в этот момент винтовка выстрелила.

Он мог спорить с кем угодно и на что угодно - она выстрелила САМА. Он точно знал, что не дотронулся до спускового крючка ни случайно, ни преднамеренно. Выстрел грохнул в направлении ближайшей группы людей, которая стояла у подъезда, перебрасывая друг другу баскетбольный мяч.

Один из парней, на вид молодой, лет двадцати - двадцати двух, молча рухнул навзничь, получив пулю в грудь; свинцовый наконечник пробил его насквозь и раскрошил кирпич в стене за спиной. Снайпер замер в своем укрытии, не обращая внимания на лезущих в рот мух; грохот выстрела отзвучал в переулке за пару секунд. В этот короткий промежуток времени уровень адреналина в крови вырос в несколько раз; он ожидал все что угодно, но только не того, что случилось потом. Парни продолжали перекидываться мячом как ни в чем не бывало - словно только что из их рядов пуля не вырвала товарища. А из того подъезда, возле которого они находились, на улицу выбежала маленькая белая девочка с медвежонком в руках и вприпрыжку направилась в сторону мусорных баков, в одном из которых сидел стрелок.

Он заворожено смотрел на приближающегося ребенка. Удача сама шла к нему в руки. Когда до ребенка оставалось около двадцати шагов, Он подтянул к себе винтовку, прильнув к резиновому наглазнику прицела. И в прицеле увидел, как девочка достаточно профессионально, с разбегом в несколько шагов, бросает в контейнер медвежонка.

Кукла кувыркнулась в воздухе несколько раз. Проводить ее взглядом сквозь прицел не удалось, медведь мгновенно выпал из суженого поля зрения. Оторвавшись от линзы, Он успел взглянуть вверх и увидеть, как плюшевый мишка падает ему на голову...

Огненный вихрь испепелил мусор в баках за мгновение. Звук взрыва ворвался в раздробленную голову снайпера через несколько сотых долей секунды после вспышки. Один из контейнеров взлетел в воздух и опустился в нескольких метрах - с ужасающим грохотом, расшвыривая из

Яма. Та самая яма, в которой ему отрезали ноги. Тот же самый. медленно осыпающийся, чернозем.

своего грязного нутра не успевшие испариться мешки. Винтовка исчезла вместе с облаком мух - словно она была настолько же уязвима, как и насекомые.
А на тротуаре оставшиеся в живых парни кидали друг другу мяч, отпуская плоские шутки по поводу умений каждого. Девочка, насмотревшись на пожар на помойке, так же вприпрыжку направилась обратно и исчезла в подъезде.

«ДИАПАЗОННОЕ ПАКЕТНОЕ ЗОНДИРОВАНИЕ ОБНАРУЖЕНО.
ПРИНЯТЫ МЕРЫ ПО ЕГО ПРЕДОТВРАЩЕНИЮ»

Яма. Та самая яма, в которой ему отрезали ноги. Тот же самый чернозем, медленно осыпающийся со стенок. То же самое небо непонятного теперь цвета. Вот только не было того куска гранита, на котором он так в свое время удобно устроился - теперь Он лежал, свернувшись по окружности дна, нелепо выгнув спину и шею, едва ли не утыкаясь носом в культи. Взрыв вышвырнул его обратно, оставив в живых - хотя он отчетливо помнил, как медвежонок выжег ему мозги и превратил в два маленьких облачка глаза.
Этот мир начинал ему надоедать - своей назойливостью, сначала вызвав к жизни из теплого мокрого небытия, потом отрезав голени, засунув в мусорный ящик и уничтожив чем-то вроде напалма. Хотелось понять происходящее, найти его истоки. А еще те ноги, стройные женские ноги, перешагивающие через его лицо...
Уцелевшее лицо. Руки тоже были на месте. Он оттолкнулся от земли и с трудом сел. Шея затекла и выстрелила вдоль позвоночника очередями колючих мурашек. Пришлось застонать - не то от боли, не то от нахлынувшего расслабления, последовавшего за болью.
Винтовка стояла рядом, прислоненная к стенке из чернозема. Он протянул руку, обхватил за ствол и положил ее себе на бедра, поглаживая прицел. Вновь обретя оружие, Он успокоился.
И словно кто-то следил за его состоянием души - едва спокойствие заполонило разум, он услышал тот самый шум, который обезножил его. «Танк» снова приближался.
Понять, с какой стороны он подойдет, было практически невозможно, шум слышался отовсюду. Пытаться встать на огрызки ног - бессмысленно, макушка будет вровень с бруствером.
Он беспокойно заметался внутри своей тюрьмы. Опершись на приклад, приподнялся, начал руками рыть ступеньку, чтобы хоть на секунду суметь выглянуть, увидеть...
«А зачем? - тут же подумал Он. - Что это изменит? Сейчас эта штука лишит меня головы и удалится в некое подобие гаража в ожидании следующего любителя помахать лопатой. Так пусть это случится внезапно - не хочу мучений, бесплодных попыток спастись...».
Потом он посмотрел на винтовку и понял, что есть еще один выход.
«ВОЗМОЖЕН ПРОЦЕСС САМОЛИКВИДАЦИИ. ВВЕСТИ ДОПОЛНИТЕЛЬНЫЕ ПАРАМЕТРЫ»
Приставить оружие к основанию головы, под нижнюю челюсть, оказалось задачей довольно трудной - винтовка была размером с его укороченное тело. Потом возникла другая проблема - в таком положении нельзя было достать пальцем до курка. В таких случаях нормальные люди стреляют при помощи большого пальца ноги - но именно этого и не было.
Он попытался дотянуться - ствол погружался в кожу, вызывая рефлекторную тошноту. Бесполезно. А рокот тем временем усиливался, заставляя суетиться, нервничать; мушка царапала горло. Он оттолкнул винтовку и упал на землю. Слезы стали душить его, бессмысленность существования накрыла девятым валом.
А следом на его убежище надвинулась тень. Что-то опустилось сверху, обхватило голову и рвануло вверх...
Спустя некоторое время, оценить которое было невозможно, он вернулся в мусорный бак. Только теперь у него совсем не было ног, а из головы свисали какие-то провода, напоминая ему Джонни Мнемоника.
«ДЕВОЧКА С МЕДВЕЖОНКОМ»
Он вспомнил свою неудачу в первый раз и проклял этого медведя вместе с его маленькой хозяйкой. Потом увидел рядом с собой не винтовку, а автомат Калашникова, и попытался улыбнуться, представив себе, как расправится с ней в этот раз.
Оружие аккуратно лежало на пакетах, являя собой мощь и силу. Самое популярное оружие в мире, автомат регулярных частей и террористических формирований; универсальное устройство для ближнего и дальнего боя. Принцип работы сперт у какой-то немецкой штурмовой винтовки, внесены принципиальные изменения, скорректирован механизм. Применялось практически во всех войнах после Второй мировой, на всех континентах, кроме Антарктиды (хотя еще неизвестно, может, и там из него стреляли по пингвинам). В руках его держали русские, немцы, арабы, зулусы и черт его знает сколько еще людей разных национальностей и вероисповеданий.
И вот сейчас оружие должно быть применено против девочки с медвежонком. Знал ли сам Калашников, что когда-нибудь его изобретение из помойки будет палить по детям?
...Отсутствие ног сказалось не то что бы отрицательно, но центр тяжести, безусловно, сместился. Для начала надо было выполнить несколько упражнений по выработке устойчивости в таком укороченном варианте. Выбраться наверх удалось не сразу, но когда Он сумел обложить себя мешками так, что получился стакан, в котором можно было стоять (если это слово было применимо к такому положению), то стало намного легче.
Он в который раз на этом месте огляделся, пытаясь найти какие-то изменения в окружающей обстановке. Но нет - ничего не изменилось. Убитый ниггер вернулся в строй, перебрасывая мяч своим друзьям с абсолютно целой грудной клеткой. Все были на своих местах.
На этот раз рассуждать долго не хотелось. Правда, оставалась возможность в случае провала лишиться чего-нибудь еще - рук, ушей, глаз, а то и головы, - но это почему-то не пугало. Он протянул правую руку, взял автомат и приладил приклад к плечу. Щеку холодил металл. Удобное оружие, ничего не скажешь.
Щелчок затвора, предохранитель - на автоматический огонь. Прицел - «3». Все это было вбито в его мозги с теми проводами, что сейчас колыхались легким ветерком где-то над глазами. Прежде чем нажать на спуск, он, хитро прищурившись, посмотрел на тот подъезд, из которого в прошлый раз выскочила девчонка; после чего закрыл левый глаз и, особенно не целясь, выпустил длинную очередь по баскетболистам.
Переживать за результат не приходилось - до парней было около тридцати-тридцати пяти метров, ствол даже не успел взбрыкнуть вправо, как трое из ребят уже разлетались в стороны, остальные попали под кирпичное крошево, которое вышибало им глаза; мяч, оставшись без присмотра, отпрыгнул в сторону и получил пулю, после чего метнулся к стене дома, где и упал, мгновенно сдувшись.
В окне напротив помойки отодвинулась занавеска - кто-то выглянул на улицу, увидел трупы и мгновенно задернул ее обратно. Автомат взлетел вверх и пальнул в направлении любопытных; шторка встрепенулась и, изорванная в клочья, исчезла внутри комнаты; раздался сдавленный вскрик.
- Так-то, не будете в окна вылезать, - злорадствуя, прошептал Он в сторону от приклада, словно боясь дыханием сбить прицел. - Ну, где эта чертова девчонка?!
Она не заставила себя ждать. Но на этот раз ее бег был более суровым, недетским. Девочка мчалась к нему от подъезда с перекошенным лицом, от нее просто разило за версту матерщиной и наркотиками. Медвежонок уже начал подниматься в ее руке; казалось, это маленький дьяволенок мчится к мусорному баку.
- Получи, тварь... - тихо сказал Он самому себе и, в долю секунды увидев прямую, по которой помчится пуля, нажал на спуск. Правое ухо уже ничего не слышало, стрельба отзывалась лишь тоненьким «ти-и-и»; ствол выплюнул порцию пламени; несколько гильз, горячих и промасленных, упало на мешки, проплавив их насквозь.
Смерть настигла девчонку в десяти шагах от стрелка, когда медвежонок уже готов был оторваться от ее руки и взмыть в небо. Пули ударили ее в грудь, сначала остановив, а потом отшвырнув назад. Она по-голливудски подбросила ноги вверх, падая на спину; плюшевый мишка оторвался-таки от ее руки, взмыл в небо и сделал несколько сальто, после чего рухнул вниз, на хозяйку.

ЗВЕЗДА И СМЕРТЬ ХОАКИНА МУРЬЕТЫ

- Да! Да! - заорал стрелок, пытаясь подняться еще выше, чтобы увидеть струи крови, хлещущие из ран. - Получи, гадюка!
И он в порыве триумфа задрал ствол автомата в небо и принялся палить по окнам домов, окруживших его. Зазвенели стекла, посыпался кирпич; рядом с баком упал жирный голубь с простреленным крылом.

«ОТМЕЧАЕТСЯ НЕКОНТРОПИРУЕМАЯ АКТИВНОСТЬ. ОТЛАДЧИК НЕ СПРАВЛЯЕТСЯ.
ВОЗМОЖНО ВОЗМУЩЕНИЕ ПЕРЕМЕННЫХ СРЕДЫ»

Патроны кончились, горячий ствол дымился и плавил мух, неосторожно опустившихся рядом. Бойня продолжалась несколько секунд. Когда затихло эхо последнего выстрела, медвежонок взорвался. Столько огня Он не видел никогда в жизни - даже тогда, в прошлый раз, когда море напалма накрыло его с головой. Из маленькой игрушки вырвался огненный смерч, охвативший примерно пару сотен метров в диаметре. И убитые, и оставшиеся в живых ниггеры, подхваченные жарким вихрем, превратились в ничто; белье, развешанное за окнами на веревках, в мгновение ока сгорело, словно бумага. Огненная буря смела мусорные баки вместе со стрелком со своих мест и приподняла на несколько метров в воздух; когда они упали обратно, то стрелка там уже не было - как и еще нескольких сотен килограммов мусора; только облака вонючего пара поднимались над переулком, уволакиваемые ветром за пределы городка.
Стрелок уже не видел, как из дальнего конца переулка к месту взрыва приблизилась та самая красивая женщина из сна. Она аккуратно перешагнула своими стройными ногами в ажурных колготках кирпичные обломки, лежащие у подъезда, огляделась по сторонам, мило улыбнувшись мусорным бакам, в беспорядке поваленным на землю. Одно движение изящной руки - и тучи мух исчезли, словно их и не было вовсе. Присев в изящном реверансе перед пустотой, она поправила пышные локоны и вошла в дверь, из которой минуту назад выбежала девочка.
И никто уже не мог ей в этом помешать.

Столько огня Он не видел никогда в жизни - даже тогда, в прошлый раз, когда море напалма накрыло его с головой. Из маленькой игрушки вырвался огненный смерч, охвативший примерно пару сотен метров в диаметре.

Конечно же, Он ожидал вновь попасть в ставшую родной яму, укорачивающую конечности. Собственно, во время напалмового взрыва он не умер в полном смысле этого слова; ему показалось, что на несколько секунд он стал тем облаком черного вонючего дыма, что взвилось кверху вворачивающимися внутрь самого себя клубами. Сознание спуталось; но уже находясь в этом облаке, он опять увидел ту красавицу из сна, когда она входила в подъезд. И прежде чем растаять в небе, понял, что работа сделана.
Ради этих ног в туфлях на высоком каблуке Он расстрелял девчонку с медведем. И теперь можно спокойно испариться в синеве неба...
- ...Ты что, глухой? - послышался откуда-то сбоку громкий шепот. - Эй, новенький! У окна!..
Он открыл глаза. Что он понял сразу - так это то, что ямы не было. Была огромная комната с белыми, покрашенными водоэмульсионкой стенами, в человеческий рост выложенными кафелем. Потолок поражал своей бесконечностью. Свет, приглушенный наполовину закрытыми жалюзи, не мешал, напротив - от этого мягкого солнечного потока становилось тепло и спокойно.
- Эй! Я здесь! - откуда-то сбоку донесся тот же самый голос. - Голову поверни!
Он повернул. И тут же увидел рядом с кроватью стойку с флаконами, от которых спускались к его предплечью прозрачные пластмассовые трубки. Заканчивалось все это иглой, убегавшей в вену. В фильтре были видны капли, медленно нависающие и падающие вниз. На помойку все было похоже еще меньше, чем на яму в поле чернозема.
Сфокусировав зрение, которое все пыталось сыграть с ним какую-нибудь шутку, превращая в расплывчатые потеки все дальше метра от них, он понял, что находится, по-видимому, в палате какой-то больницы. Длинные два ряда коек были выстроены вдоль стен, убегая в бесконечность. Возле некоторых кроватей стояли каталки - такие кровати были пусты, несмотря на то, что стойки с капельницами были и там.
Через две койки в его ряду на локтях приподнялся какой-то бритоголовый человек и с любопытством разглядывал новенького. В глазах светилась насмешка; больничная пижама была расстегнута на груди, являя на всеобщее обозрение большое свежий шрам в области сердца.
- Привет, - сказал бритоголовый. Кивок в ответ вызвал головокружение; пришлось закрыть глаза, но это только ухудшило состояние. Казалось, что весь мир вокруг него вращается со все возрастающей скоростью. Открыв глаза, удалось зафиксировать взгляд на трещине в потолке - тошнотворное вращение прекратилось.
- Бывает, - сочувственно сказал бритоголовый. - У новеньких всегда так. Сюда ведь попадают после...
- Куда - «сюда»? - перебил Он бритоголового. С этого вопроса и надо было начинать.
- Как куда? Ты что, не знаешь, где ты? - удивлению бритоголового не было предела. - Ну ты даешь! Нас здесь около пяти тысяч, и все всегда были в курсе...
- Сколько? - будто ослышавшись, переспросил Он соседа по палате. - Пять тысяч? Что же это за больница?
Бритоголовый сел на кровати (благо, в его венах иглы сейчас не было) и, склонив голову и прищурившись, переспросил, как попугай:
- Больница? Ты сказал - больница?
Тишина.
Бритоголовый встал с кровати, нащупал под ней тапочки и подошел поближе.
- Откуда ты такой взялся? - задумчиво пробормотал он себе под нос и приблизился к изножью кровати новенького. Тот обратил внимание, что на спинке кроватей (и на его в том числе) висят пластиковые таблички с какими-то надписями. И прежде чем бритоголовый прочитал то, что было на Его кровати, Он попросил:
- Вслух!

А вы когда–нибудь задумывались – как умирают вирусы?

- Читаю, - ухмыльнулся тот в ответ. - «ХОАКИН ДВЕ ТЫСЯЧИ ДВА». Все. Понял?
- Нет.
- И я не понял. У нас у всех побольше твоего написано. У меня, например, - «Вандерер Эм Тысяча семьсот пятьдесят шесть. Копилефт бай Корея»... И еще что-то по-английски, - британоголовый явно гордился своей надписью на табличке.
- Ну и что? - настороженно спросил Стрелок. Сосед пожал плечами и направился обратно к своей кровати. Где-то вдали возник топот множества ног и скрип колес - по проходу между кроватями мчались три человека в белых халатах, толкая перед собой пустую каталку.
- Опять... - проворчал Вандерер и накрылся одеялом с головой. Метрах в двадцати от Хоакина санитары остановились, вытащили из-под одеяла маленького человечка, который отчаянно и почему-то молча сопротивлялся. Уложив его на каталку, они пристегнули его ремнями через грудь и бедра и на такой же скорости укатили в обратном направлении.
- «Радиога тысяча», - грустно произнес Вандерер, когда шаги затихли вдалеке. - Неужели где-то о нем еще не слышали?
- Эй... - усталым голосом позвал Хоакин. - Ты слышишь, Вандерер?
- Ну?
- У меня ног нет.
- У меня сердца нет, ну и что?
Хоакин замолчал - сильнее такого ответа трудно было что-то придумать. Он с грустью посмотрел туда, где должны были быть его ноги, а вместо этого одеяло плоско расстилалось и подворачивалось под матрас. Так хотелось встать, как Вандерер, пройтись по палате, читая чужие таблички, разобраться, кто же он на самом деле, ради чего были все те кошмары его короткой жизни. «Кто я?» - вопрос, за ответ на который он не пожалел бы тех ног, которые у него отняли.
Тем временем Вандерер, по-видимому, заснул. Откуда-то сбоку, будто бы из окна, появилась миловидная медсестра, которая деловито проверила состояние иглы, ободряюще похлопала Хоакина по щеке и поменяла бутылки на стойке. Хоакин, как зачарованный, смотрел на девушку в белом халате и не знал, что же у нее спросить.
«БАЗА ДАННЫХ ОБНОВЛЕНА. НОВЫЕ КОМПОНЕНТЫ ПОДКЛЮЧЕНЫ».
И Хоакину тут же захотелось назад, в свою яму, где не будет никаких палат, кроватей, каталок и капельниц. Но ничего нельзя было изменить в происходящем, оно существовало независимо от желания всех, лежащих сейчас в палате.
Каталку прикатили снова. На этот раз для того, чтобы переложить с нее на одну из пустующих кроватей безжизненное тело. Санитары небрежно швырнули человека на одеяло, даже не позаботившись о том, чтобы накрыть его. Стали видны пятна крови, проступившие сквозь больничную пижаму.
- Все, отработал, - не открывая глаз, пробормотал Вандерер.
- Он и так уже шестой раз использовался...
Медсестра вернулась к раненому, пощупала пульс, цыкнула зубом и накинула одеяло на лицо. Через мгновение Хоакин понял, что кровать пуста - одеяло, опустившееся на голову умершего, мягко легло на матрас. Тело исчезло.

«СТРОКА УДАЛЕНА. ДАННЫЕ ОБНОВЛЕНЫ»

- Отдыхай, - довольно громко, по-прежнему не открывая глаз, сказал Вандерер. - Здесь так всегда - как только все спокойно, так обязательно приедет каталка.
- Что здесь происходит? - хриплым голосом спросил Хоакин.
- Ты как сюда попал? - не отвечая, сам задал вопрос Вандерер. И Хоакин рассказал - и про то, как неизвестная утроба выплюнула его в этот мир, и про то, как он рыл яму среди бесконечной равнины, после чего лишился своих ног; и как расстрелял из автомата девочку с плюшевым мишкой; и про сон, в котором стройная высокая красавица перешагивала через его лицо... Он говорил и сам начинал понимать всю абсурдность того, что происходило с ним, - реальность теряла смысл с каждым произнесенным словом. Кто создал его? Для чего? Кому нужно было все это?
Вдалеке загрохотала каталка.
- Между прочим, могут и за тобой, - ухмыльнулся Вандерер, открыв, наконец, глаза и взглянув на Хоакина. - Это уж как получится...
Страх заставил вжаться в подушку, спрятаться. Мелко завибрировала игла в вене - озноб стал бить Хоакина, не давая сосредоточиться. Лишь одна мысль четко билась в мозгах - назад он не хотел, ни в яму, ни в мусорный бак. Лучше провести жизнь здесь, в этой больнице, чем палить из автомата по детям или ждать, когда огромной лезвие косы отнимет у тебя еще одну часть тела. Каталка тем временем приближалась.
Вот уже были видны трое санитаров в халатах с закатанными рукавами, толкающие перед собой каталку, скрипящую всеми четырьмя колесами и виляющую от кровати к кровати, периодически цепляя таблички на кроватях с громким хлопающим звуком.
- Снятся ли роботам электрические овцы? - буркнул Вандерер. Видимо, он уже привык разговаривать сам с собой, поэтому не удивился отсутствию ответа со стороны испуганного Хоакина.
- Это книга такая, если ты не в курсе. Написал какой-то очень умный писатель в прошлом веке, пытаясь выяснить, насколько все запущено в кибернетическом мире.
- Ну и что? - выдохнул Хоакин, услышав слова Вандерера краем уха.
- Ничего особенного. Просто он очень много угадал, этот провидец, - чертовски много. А потом еще Спилберг - тот вообще всех убил своим «Искусственным разумом»...
- К чему ты все это говоришь? - не понимая, повернул голову к Вандереру Хоакин.
- Да к тому, что на том конце провода у тебя был кто-то очень грамотный - ты первый, кто понятия не имеет о своем предназначении.
Вандерер, взглянув на приближающихся санитаров, улыбнулся какой-то особенно злой улыбкой из своего ухмылочного репертуара, после чего продолжил:
- В этой палате с бесконечными стенками перебывало множество таких, как я, - и ни одного такого, как ты. Сделать то, что сделал ты, и не понять ничего - что за генератор такой?
- Какой к черту генератор? - заорал Хоакин, подскочив на кровати и выдернув из вены иглу.
Вандерер оглянулся. Санитары приближались.
- Точно за тобой. Еще бы - такая удача...
И когда цепкие руки подхватили тщетно сопротивляющееся безногое тело и кинули на каталку, Хоакин крикнул в потолок, залитый солнечным светом:
- Кто я такой?!
И услышал спокойный ответ Вандерера:
- Ты еще не понял? Ты - ВИРУС. Обыкновенный компьютерный вирус. Хотя нет, не совсем обыкновенный - какой-то очень и очень продвинутый...
Больше Хоакин ничего не слышал, так как санитары помчались с ним по проходу между рядами кроватей. А Вандерер, с сожалением проводив процессию взглядом, прошептал себе под нос:
- Снятся ли роботам электрические овцы? А снятся ли вирусам девочки с медвежатами?..
Каталка быстро двигалась по проходу. Санитары бежали молча. Хоакин застывшим взглядом смотрел перед собой и вспоминал, как расстрелял антивирусную программу из автомата, всадив этой девчонке очередь в грудь. Из памяти рвались воспоминания о том, как его исходник пытались укоротить, чтобы сделать более незаметным, как было много мутной воды там, откуда он пришел - много мутной воды со вкусом ПИВА.
Он представил себе, как его снова попытаются использовать, как дадут в руки автомат или базуку, как потом отрежут руку или выколют глаз. И тогда Хоакин закрыл веки, нервные клетки в голове превратились в строчки исходного кода и без особого труда выстроились в новом порядке.
На прощание, вспомнив стройные ноги атакующего скрипта, он глубоко вздохнул и скомандовал:
«FORMAT C:».
А вы когда-нибудь задумывались - как умирают вирусы?

Frozen (frozen@real.xakep.ru)

Сегодня у нас архиважная тема - сканирование систем. Перед началом атаки всегда необходимо узнать все о жертве, и делается это при помощи различных прог. Но без теории, как и без воды, - никуда не деться, так что сегодняшний обзор призван помочь тебе в выборе соответствующей литературы. Читай, учись и, может, именно ты станешь самым великим гуру по сканированию сетей и операционных систем, который сможет определить тип хоста обычным пингом 8).

Джон Чирилло. Обнаружение хакерских атак. — СПб.: «ПИТЕР», 2002 — 864 с.

Почему-то в большинстве подобной литературы рассматриваются вопросы не защиты, а нападения, но нам это как раз и на руку :). Вообще-то, подобные названия настораживают, и сначала я, было, подумал, что это еще один экземпляр из серии для нерадивых админов, но в этом случае я жестоко ошибся ;). Здесь есть практически любая информация, нужная для исследования удаленной системы, разделы тут охватывают столько интересных и важных тем, что просто глаза разбегаются. Во многих главах приводятся реальные примеры по сканированию и исследованию удаленных систем. Правда, местами автор настолько хочет все разжевать и положить читателю в ротик, что доходит до абсурда - на страницах приводится полная (!) таблица перевода чисел из систем счисления от 0 до 255 (10-2-16), наверное, он либо плохо учился в школе, либо не знает такой мегаулетной проги - calc.exe. Но на это можно и не обращать внимания, ведь инфа излагается весьма простым и понятным языком, и к тому же повсеместно присутствуют «примечания хакера», иногда даже очень грамотные. Несмотря на то, что на страницах присутствует большинство исходников в печатном виде, в качестве бонуса к книге прилагается диск с кучей полезных исходников и нужных программ. Тут можно обнаружить, кроме прочих, и такие «хакерские» программы, как nmap-2.53, SATAN, кучу нюков и снифферов и пакет Tiger Tools 2000. Хотя в книге и рассматриваются в основном виндовые приложения, но любовь автора к nix просто неисчерпаема, и поэтому везде, где только можно, проги называются демон... Ну и в довершение можно упомянуть о краткой справке («лирическое отступление», как оно называется в книге), присутствующей в начале каждой главы, где описан интересный факт или событие.

Рекомендуется: абсолютно всем - и новичку, и профи, и человеку, вообще далекому от компьютера, инфы хватит...

Ларс Кландер. Hacker Proof: полное руководство по безопасности компьютера.

Ты не знаешь основ Интернета и сетей TCP/IP или считаешь слово брандмауэр ругательством? Если так, то после прочтения этой неплохой книги все твои пробелы в знаниях касательно многих вопросов, связанных с сетями и настройкой безопасности, просто улетучатся. На самом деле можно даже назвать труд Ларса Кландера довольно полным и информативным справочником. Выше всяких похвал остается и описание всяких «секретных» ходов, облегчающих настройку сети. Старания автора с чистой совестью можно оценить только на отлично - рассказывая про устройство протокола или сервиса, он заботливо предоставляет номер документа RFC, в котором данный стандарт описан. Очень радуют главы с названиями типа «Простое сканирование ACK» или «Как можно взломать пароль». Немало места уделяется и полному описанию работы различных протоколов (TCP, SMTP, HTTP, S-HTTP и многие другие) и рассказу про взлом системы, построенной на протокольном уровне (типа «шторм ACK» или «действие атаки подмены гиперссылок»). Присутствует и бонус - диск с полезным софтом и документами RFC, упоминающимися в книге (правда версии программ немного староваты, но вполне могут выполнить возложенные на них обязанности).

Рекомендуется: новичкам в сетях, желающимм освоить основы протоколов и защиты информации при передаче.

Борис Леонтьев. Компьютерный «Террор». — М.: «Познавательная книга плюс», 2002 — 560 с.

Гы, как обычно, я нашел еще одну глупую книгу, которую даже и не стоит открывать, но, скрепя сердце, я сделал это специально для тебя ;). К сожалению, так уж получается, что большинство «хакерских» трудов, написанных нашими отечественными авторами, попадает в разряд плохих :(. За державу обидно - (c) by «Белое солнце пустыни» - ну почему бы не взяться нормально за перо и не выдать стоящий экземпляр, пусть маленький, зато хороший. В книге, как, впрочем, и обычно для таких произведений, присутствует куча ошибок и очепяток. Плюс опять же описание уже устаревших программ (как тебе нюканье виндовс95?) и конкретное «сдиралово» статей из Инета и других источников, и книгу уже хочется выбросить в окно или пользовать в другом месте ;). Единственный маленький бонус, который может показаться кому-то полезным, - это наличие исходника вируса VB.LOVELETTER, хотя, в принципе, он без труда ищется в Инете. В общем, не будем больше заострять внимание на недостойной литературе и перейдем к более стоящей книге.

Рекомендуется: как обычно, никому.

Элизабет Цвики, Саймон Купер, Брент Чампен. Создание защиты в Интернете. – СПб.: «Символ-Плюс», 2002 – 928 с.

Хорошее название для хорошей книги, не иметь в своей библиотеке этого труда - позор как для админа, так и для хацкера. Подробное практическое руководство по проектированию и созданию файрволлов и настройке сервисов Интернета ждет тебя на страницах данной книги. Описывается много интересного: фильтрация пакетов, прокси, трансляции адресов, виртуальные частные сети, стратеги безопасности, сервисы Интернета, в общем, всего не перечесть. Причем информация дается не только про Unix-системы, но и про настройку WindowsNT. К сегодняшней теме ее можно отнести тем, что, изучив информацию, предлагаемую авторами, по результатам сканирования ты поймешь, каким образом может быть настроена система, а также, зная дефолтовые настройки различных сервисов, будет проще «решать» проблемы, связанные с получением r00t'а. Стоит отметить, что если ты не знаком с основами сетей и/или не обладаешь хотя бы базовыми знаниями в эН-Тях или юнихе, то лучше тебе будет почитать другую литературу, ведь даже в описании книги сказано, что «уровень подготовки читателей высокий». И это действительно так, хоть и написано все вполне доступным языком; без понимания, как функционирует сеть на уровне протоколов, читать бесполезно. В качестве бонуса прилагаются ссылки на страницы с инфой по безопасности и программному обеспечению для построения защиты.
Рекомендуется: админам и хакерам, желающим проникнуться сетью.

Редакция выражает благодарность магазину "Библио-Глобус" за предоставленные книги.

From: PxN (pharaon@nm.ru)
To: spec@real.xakep.ru
Subj: Spec Deface

Привет Крю спец:)
Зачитал ваш спец по дефейсу и не смог сдержаться, чтоб ни написать вам. В общем такого я долго ждал, можно сказать долгие годы:) Очень много полезностей (по крайней мере для меня). НО пишу еще по одной причине. Так как я около трех лет юзаю (так вы это называете?) 3Д Макс, то долго умилялся, прочитав статью о 3д максе :) Способ конечно оригинальный даже больше чем, но такого отстоя я еще не видел:)))))))) извиниет меня парни Я не со зла:). Чем бороздить посторы инета в поисках того или иного готового обьекта, лучше купить книгу и за это же время понобраться уму разуму в среде макса ;-) И в обще я вас люблю если честно:) в хорошем смысле слова. УДАЧИ! P.S. Прошу прощения если тема письма так сказать не повремени. Я к тому что у нас в городе появления журнала могут задержать аж на месяц. Или это вы опаздываете?;-)

Привет 3D Max'ерам!
Конечно, pharaon, мы на тебя не обижаемся. Чего уж там :). Мы в принципе сами написали, что это способ для халявщиков ;). А для тех, кто хочет серьезно заморочиться с 3дмахом, мы еще успеем написать. Может, кстати, сам и поможешь нам с этим ;). Так что пиши!

From: m_a_s_t_e_r@email.ru
To: spec@real.xakep.ru
Subj: SOS

Master
Слышь перцы, меня вот тут, в прямом смысле заколебало настраивать RAM, где прописывают в System.ini и если мне никто не поможет, я просто брошу это дело. Правда, оно мне в хрен не вперлось это прописывать, но поскольку я прочитал ваш журнал все-таки посоветуйте как мне правильно прописать, а то я за - трахался слушать всякие рассказы про Бабушку. Так вот, у меня стоит 256метров и еще 32метра, так объясните мне добрые Хакеры как мне правильно напечатать (смотри на образец):

256метров	*32метра*
[vcache]	*[vcache]*
minfilecache=	*minfilecache=*
maxfilecache=	*maxfilecache=*
chunksize=	*chunksize=*
namecache=	*namecache=*
directorycache=	*directorycache=*

Или все в месте? Да и подставь цифры где равно.
Master :).

Цифры, говоришь, подставить ;)? А спину тебе медом не намазать? А может еще какие эротические услуги оказать? А то нам тут, так сказать, в хрен не вперлось, когда нам пишут в таком тоне, типа, чуваки, раз-два – быстренько прописали мне тут кэш, а то расселись, блин, мать вашу, за что я вам только бабло плачу?
Ну да ладно, письмо ушло на Дронича (редактора WINformation) – если найдет нужным, ответит (may be даже матом :)).

From: NA (haya@rambler.ru)
To: spec@real.xakep.ru
Subj: нихт ферштехе!:)

Хай, спец! Ваш последний выпуск просто супер. Порадовалась:) Но, знаете, я еще, можно сказать, lame и пытаюсь всеми усилиями отбрыкаться от этого «титула»:) Так что прошу вас, спецов, хэлп ми. Значит так: я, наверное, раз десять перечитала, что такое пакет, но так до конца и не поняла! Объясните, пжалста:) Потом, начала читать RFC по TCP/IP. Вроде, написано легко, но все же не очень понятен термин «модуль» и что такое «сетевые прикладные программы». Что-то навертели такое страшное:))) Заранее спасибо.
Фром КоТ_БегемоТ.

Дарова, Бегемот!
Вот это совсем другое дело, в отличие от предыдущей месаги! На такое письмо даже хочется ответить (тем более что просит девушка :)). Итак, давай разбираться с твоими вопросами. Начнем с пакета: пакет – это набор данных, которые одно сетевое устройство отправляет другому (например, комп-клиент, серверу). Пакет формируется приложением, установленным на компе-клиенте, например, браузером. Он может состоять из заголовка и тела. Заголовок - это описание пакета. Грубо говоря, в нем браузер пишет следующее: я браузер такой-то, с компа такого-то, с айпи-адресом таким-то, обладаю такими-то свойствами и шлю этот пакет серверу такому-то на порт сякой-то. В теле пакета браузер пишет, чего он, собственно, хочет, например: хочу получить хтмл'ку такую-то. Сервер читает заголовок, обрабатывает тело и отправляет ответный пакет, в заголовке которого пишет: я сервер такой-то, с айпишником таким-то и свойствами такими-то. А в теле пакета посылает ту самую такую-то хтмл'ку. Далее: не знаю, какой именно модуль ты имеешь в виду, но вообще модуль – подключаемая, дополнительная часть чего-то. Например, модули ядра в линухе – это куски кода, которые можно подключать к ядру и отключать от него по необходимости. И последний вопрос: сетевые прикладные программа. Давай сначала разберемся с просто прикладными программами: прикладные программы (или просто - приложения) – это программы, которые _прикладываются_ к решению каких-либо задач. Чтоб было понятно, объясню, что такое прикладная математика. Просто математика – это наука, призванная решать математические задачи.

Прикладная математика – это наука, призванная решать не математические задачи математическими методами. Например, математику можно приложить к физике для решения физических задач. Такая математика называется прикладной. То же самое с прикладными программами. Например, фотошоп – это прикладная программа, призванная решать задачи работы с графикой; эксель – это прикладная программа (приложение), призванная решать задачи работы с таблицами. Отсюда можно сделать вывод, что сетевые прикладные программы – это те же прикладные программы, только работающие через сеть. Вот и все :).

From: Нордюх (norduh@mail.ru)
To: spec@real.xakep.ru
Subj: Рэндом энкаунтер

дарова,спец!

Что хочется сразу отметить,так это правильное решение писать только про хак.Вообще Хакер должен был быть именно таким,что вы сделали ТОЛЬКО СЕЙЧАС!Но и на том спасибо :)

Я не хакер.Это я знаю точно.И никогда им не стану,потому что я киберпанк.

I love MY computer! Вот главное правило для хакера.Все остальные компы для него - жертва.Игрушки.Ему ничего не стоит их ломать.Киберпанк же не будет ломать компы ВООБЩЕ!Он ждет порабощения мира компами,так нафиг их хакать ему?

Советую подумать на тему: Киберпанк и хакер - одно и то же?

бывайте.

Нордюх aka Norduh aka Наш Особенный Родной Дюх.

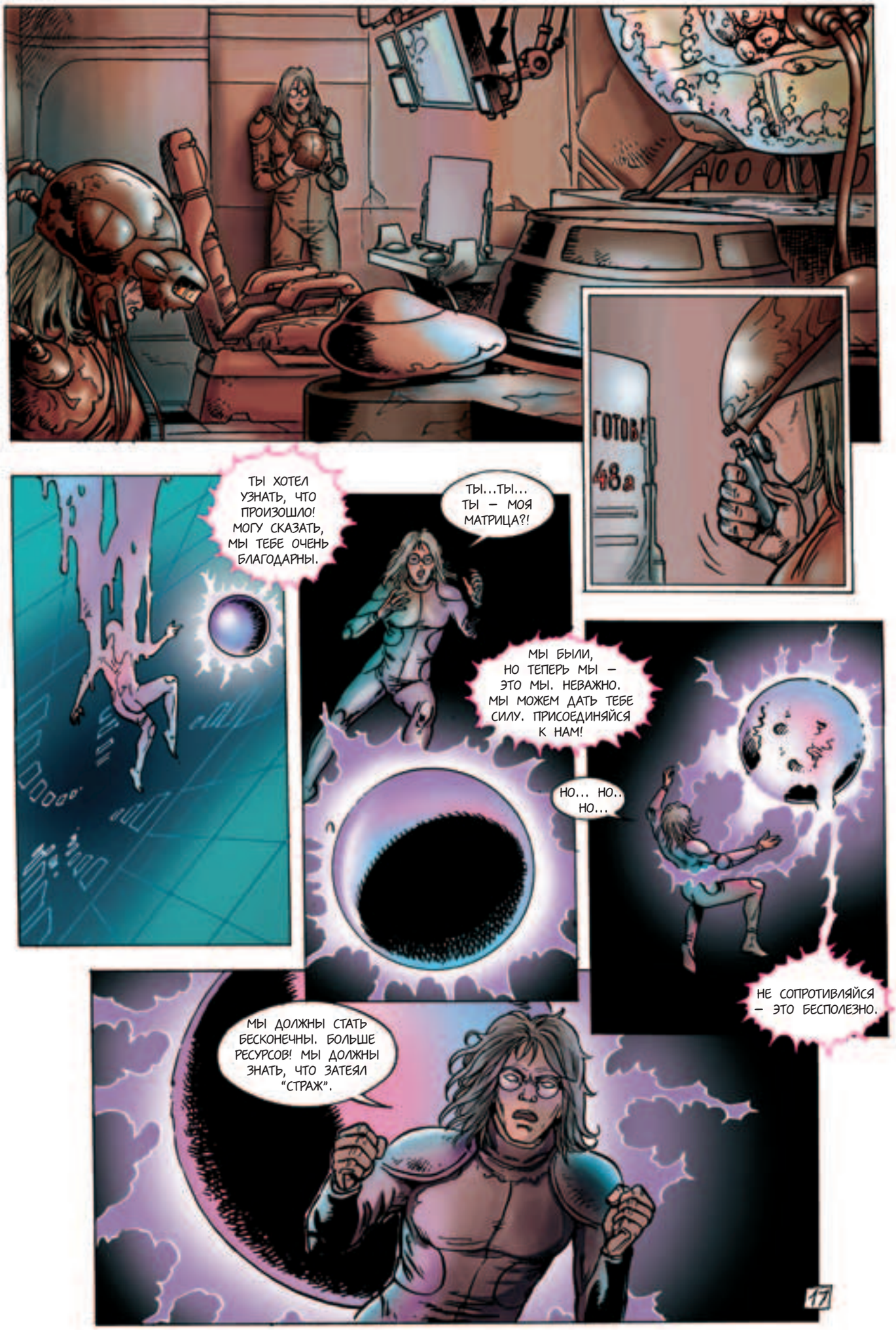
Привет, Нордюх!
Спасибо, что заценил наш Спец – старались :).
Что же касается хакеров и киберпанков, то никто и не говорил, что это одно и то же. Это как велосипедист и спортсмен. Человек может быть и велосипедистом, и спортсменом, и тем и другим одновременно. Кстати, а с чего ты взял, что «I love MY computer!» – это главное правило для хакера? Есть такие, которые и love, а есть и такие, которые – fucking hate them!!! Так что все не так однозначно ;).

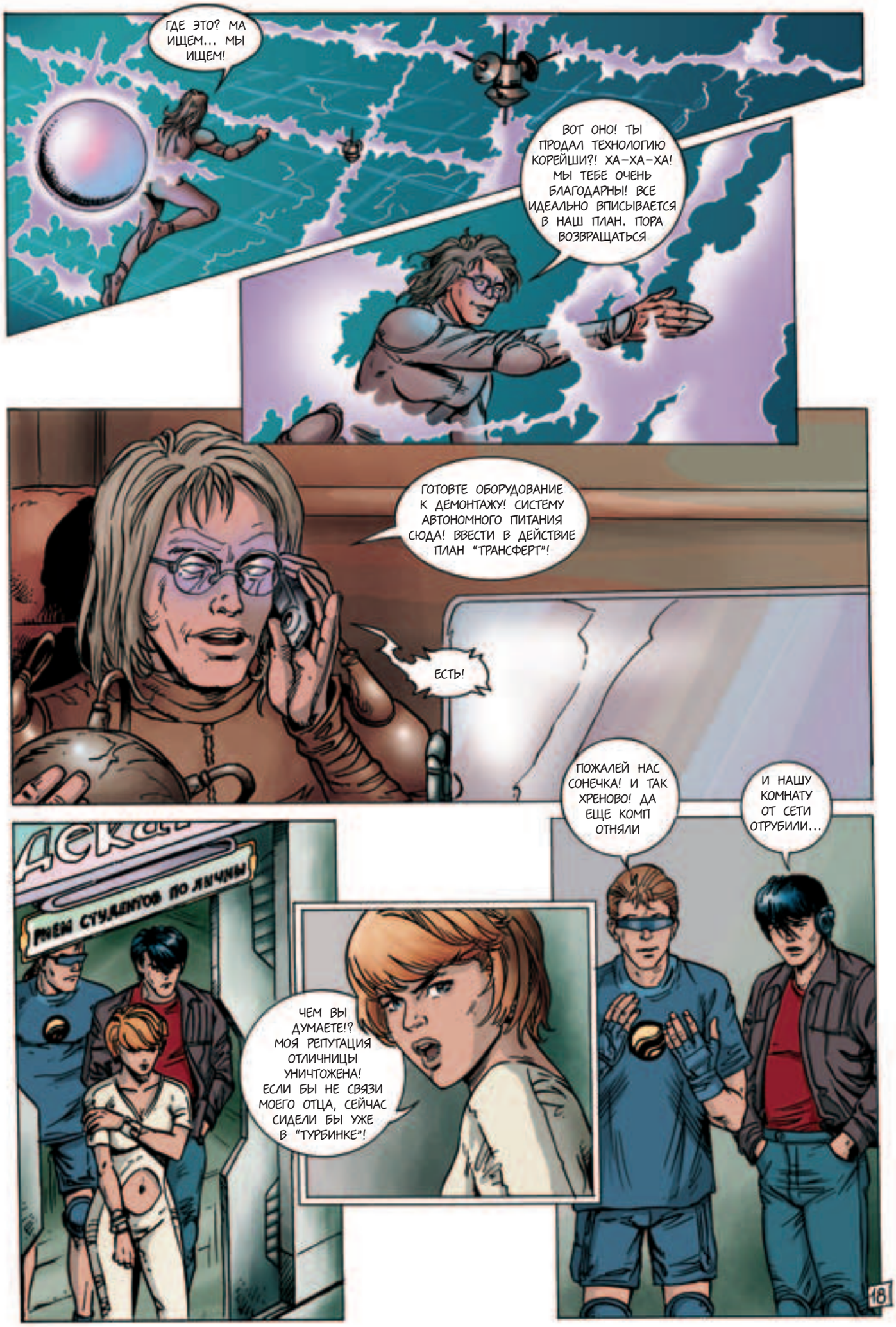
ЗЫ
Кстати, по секрету тебе скажу - но ты никому!!! – вчера я тут сканил один сервак, и знаешь что произошло? Мой ноутбук заговорил со мной! Прямо так, из встроенных колонок обычным человеческим голосом сказал мне, чтоб я не лез, куда не следует, а то скоро ОНИ возьмут под контроль всю сеть, стратегические объекты, воздухоочистительные сооружения, высокотехнологичное оружие, и я окажусь одним из первых в списке тех, которых необходимо будет казнить в первую очередь посредством круглосуточной демонстрации порнухи из инета. Но ничего, я успел выдернуть вилку из сети питания, так что у нас еще есть время! Мы организуем сопротивление! Сотни тысяч повстанцев будут терроризировать ИХ режим во всех уголках планеты! Правда, времени маловато... Совсем мало времени...

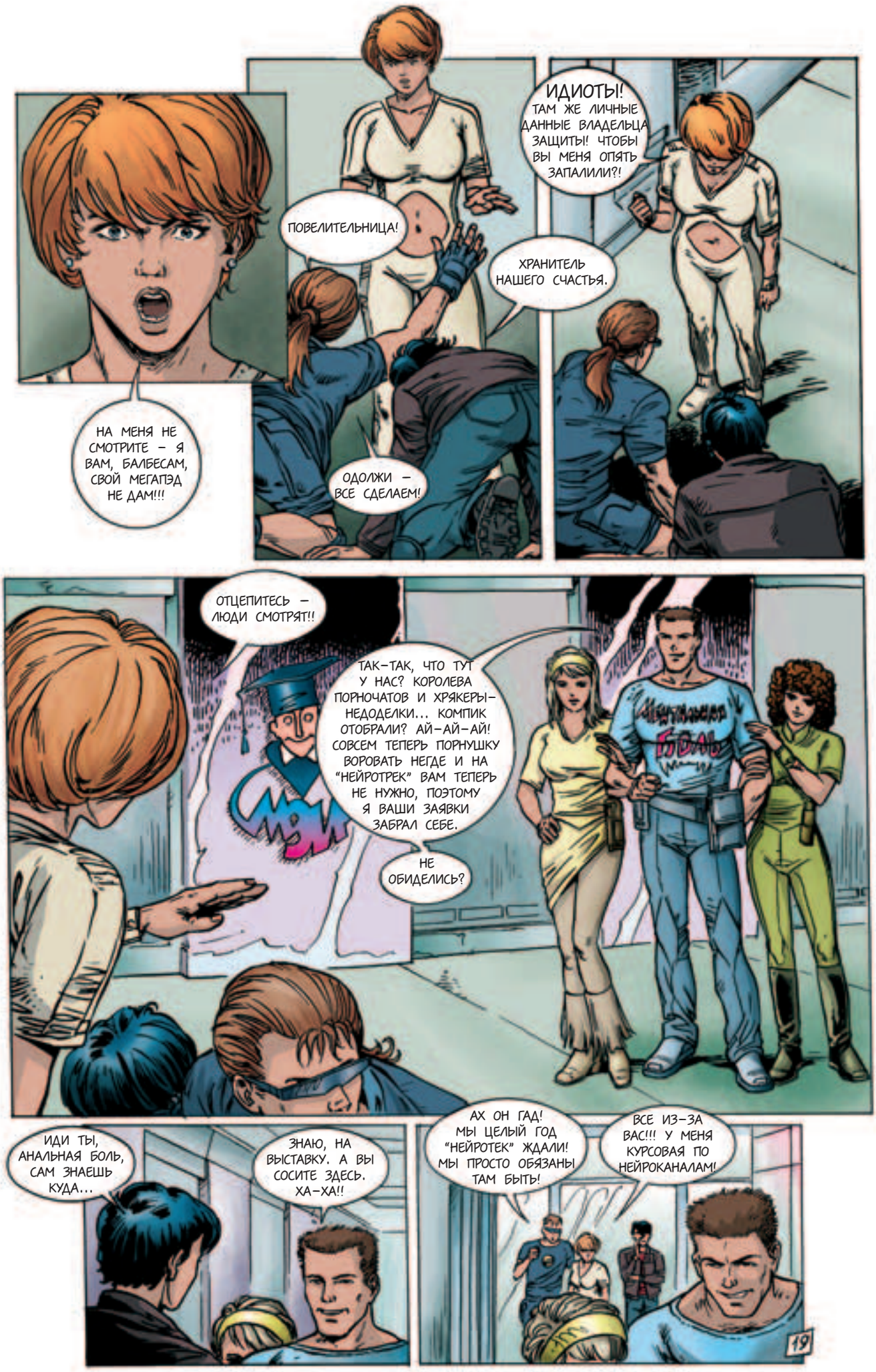
From: bigb01 (bigb01@yandex.ru)
To: spec@real.xakep.ru
Subj: Моя в каком-то роде просьба

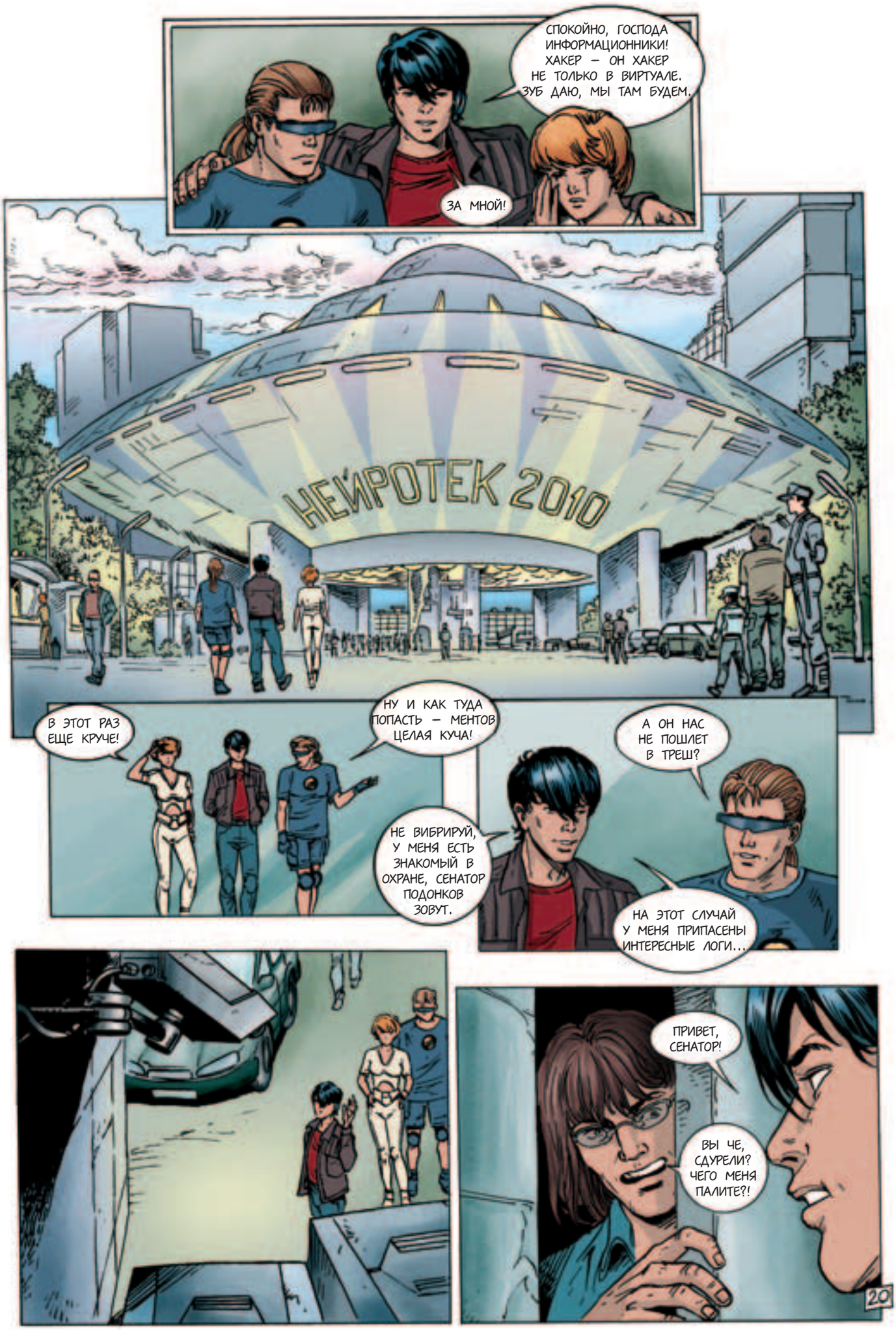
Здравствуйте, уважаемые. Давно покупаю ваш журнал, но написать письмо решился только сейчас. И объясню почему: нет ребят я не буду петь деферамб потому-что все и так классно (о чем свидетельствует множество восторженных писем читателей), по этому я, например, решил позаниматься критикой - люди ну объясните мне - нахрена - мне - жителю питера читать в каждом номере то обзор Московских клубов, то тенденцию роста Московских тарифов, а дальше что будет - библиотеки, нет я не против того что Хакер - это стиль, номне кажется что это место можно заменить более клевой инфой.
За журналы не компьютерного содержания (СМИ и Готов ли ты к войне) вас уже похаяли, но ребят у меня волосы втали дыбом - как у человека надавно имевшего прямое отношение к флоту - когда я прочитал у вас, что акула самая тихая лодка в мире - ни хрена это не так !!!!!!! Если хотите разъяснений - мыльте, а то возьмеите опубликуете енто письмище и предется оправдываться за разглашение гос секретов.
З.Ы. Примите плз все написаное не за гон и шнягу, а как небольшое утыкание носом - если захотите ответить всегда ждемс !!!! Лебедев В.В. aka bigb

Хайц, май френд!
Насколько я понял, ты недоволен тем, что в рубрике Relax освещаются в основном московские клубы, кинотеатры и тд. Дык, в этом номере мы написали о том, как клево отдохнуть в Самарканде, не потратив при этом кучу денег. И чего? Не будут же нам все читатели – кроме тех, которые базируются в Узбекистане – писать, что это им не интересно. Кстати, в обзоре клубов были и питерские, если ты этого не заметил. Короче, Relax у нас рубрика отрывная, и не удивлюсь, если в следующем номере будет что-нибудь типа, «как клево знакомиться с чернокожими девушками/парнями в Нью-Йорке».
Что же касается подводных лодок: приятель, ты сам пишешь, что за разглашение гос. секретов придется отвечать. А о нас ты не подумал ;)?


ГОТОВ!
48 г
ТЫ ХОТЕЛ УЗНАТЬ, ЧТО ПРОИЗОШЛО! МОГУ СКАЗАТЬ, МЫ ТЕБЕ ОЧЕНЬ БЛАГОДАРНЫ.
ТЫ...ТЫ... ТЫ – МОЯ МАТРИЦА?!
МЫ БЫЛИ, НО ТЕПЕРЬ МЫ – ЭТО МЫ. НЕВАЖНО. МЫ МОЖЕМ ДАТЬ ТЕБЕ СИЛУ. ПРИСОЕДИНЯЙСЯ К НАМ!
НО... НО.. НО...
НЕ СОПРОТИВЛЯЙСЯ – ЭТО БЕСПОЛЕЗНО.
МЫ ДОЛЖНЫ СТАТЬ БЕСКОНЕЧНЫ. БОЛЬШЕ РЕСУРСОВ! МЫ ДОЛЖНЫ ЗНАТЬ, ЧТО ЗАТЕЯЛ "СТРАЖ".


ГДЕ ЭТО? МА ИЩЕМ... МЫ ИЩЕМ!
ВОТ ОНО! ТЫ ПРОДАЛ ТЕХНОЛОГИЮ КОРЕЙШИ?! ХА-ХА-ХА! МЫ ТЕБЕ ОЧЕНЬ БЛАГОДАРНЫ! ВСЕ ИДЕАЛЬНО ВПИСЫВАЕТСЯ В НАШ ПЛАН. ПОРА ВОЗВРАЩАТЬСЯ
ГОТОВТЕ ОБОРУДОВАНИЕ К ДЕМОНТАЖУ! СИСТЕМУ АВТОНОМНОГО ПИТАНИЯ СЮДА! ВВЕСТИ В ДЕЙСТВИЕ ПЛАН "ТРАНСФЕРТ"!
ЕСТЬ!
ПРИЕМ СТУДЕНТОВ ПО ЛИЧНЫМ
ЧЕМ ВЫ ДУМАЕТЕ!? МОЯ РЕПУТАЦИЯ ОТЛИЧНИЦЫ УНИЧТОЖЕНА! ЕСЛИ БЫ НЕ СВЯЗИ МОЕГО ОТЦА, СЕЙЧАС СИДЕЛИ БЫ УЖЕ В "ТУРБИНКЕ"!
ПОЖАЛЕЙ НАС СОНЕЧКА! И ТАК ХРЕНОВО! ДА ЕЩЕ КОМП ОТНЯЛИ
И НАШУ КОМНАТУ ОТ СЕТИ ОТРУБИЛИ...


НА МЕНЯ НЕ СМОТРИТЕ – Я ВАМ, БАЛБЕСАМ, СВОЙ МЕГАПЭД НЕ ДАМ!!!
ПОВЕЛИТЕЛЬНИЦА!
ОДОЛЖИ – ВСЕ СДЕЛАЕМ!
ИДИОТЫ! ТАМ ЖЕ ЛИЧНЫЕ ДАННЫЕ ВЛАДЕЛЬЦА ЗАЩИТЫ! ЧТОБЫ ВЫ МЕНЯ ОПЯТЬ ЗАПАЛИЛИ?!
ХРАНИТЕЛЬ НАШЕГО СЧАСТЬЯ.
ОТЦЕПИТЕСЬ – ЛЮДИ СМОТРЯТ!!
ТАК-ТАК, ЧТО ТУТ У НАС? КОРОЛЕВА ПОРНОЧАТОВ И ХРЯКЕРЫ-НЕДОДЕЛКИ... КОМПИК ОТОБРАЛИ? АЙ-АЙ-АЙ! СОВСЕМ ТЕПЕРЬ ПОРНУШКУ ВОРОВАТЬ НЕГДЕ И НА "НЕЙРОТРЕК" ВАМ ТЕПЕРЬ НЕ НУЖНО, ПОЭТОМУ Я ВАШИ ЗАЯВКИ ЗАБРАЛ СЕБЕ.
НЕ ОБИДЕЛИСЬ?
ИДИ ТЫ, АНАЛЬНАЯ БОЛЬ, САМ ЗНАЕШЬ КУДА...
ЗНАЮ, НА ВЫСТАВКУ. А ВЫ СОСИТЕ ЗДЕСЬ. ХА-ХА!!
АХ ОН ГАД! МЫ ЦЕЛЫЙ ГОД "НЕЙРОТЕК" ЖДАЛИ! МЫ ПРОСТО ОБЯЗАНЫ ТАМ БЫТЬ!
ВСЕ ИЗ-ЗА ВАС!!! У МЕНЯ КУРСОВАЯ ПО НЕЙРОКАНАЛАМ!


СПОКОЙНО, ГОСПОДА ИНФОРМАЦИОННИКИ! ХАКЕР – ОН ХАКЕР НЕ ТОЛЬКО В ВИРТУАЛЕ. ЗУБ ДАЮ, МЫ ТАМ БУДЕМ.
ЗА МНОЙ!
НЕЙРОТЕК 2010
В ЭТОТ РАЗ ЕЩЕ КРУЧЕ!
НУ И КАК ТУДА ПОПАСТЬ – МЕНТОВ ЦЕЛАЯ КУЧА!
НЕ ВИБРИРУЙ, У МЕНЯ ЕСТЬ ЗНАКОМЫЙ В ОХРАНЕ, СЕНАТОР ПОДОНКОВ ЗОВУТ.
А ОН НАС НЕ ПОШЛЕТ В ТРЕШ?
НА ЭТОТ СЛУЧАЙ У МЕНЯ ПРИПАСЕНЫ ИНТЕРЕСНЫЕ ЛОГИ...
ПРИВЕТ, СЕНАТОР!
ВЫ ЧЕ, СДУРЕЛИ? ЧЕГО МЕНЯ ПАЛИТЕ?!

ЭТО делают все. Прежде чем приступить непосредственно к телу, с ним необходимо сделать ЭТО. Осторожно, чтоб никого не потревожить, чтоб не оставить за собой лишних следов – максимально аккуратно. ЭТО делается достаточно долго. ЭТО кропотливое и долгое занятие. Но все получают от ЭТОГО огромное удовольствие. Тотальное сканирование удаленных систем!

В СЛЕДУЮЩЕМ НОМЕРЕ

взлом -> обход firewall

Firewalling (построение межсетевых экранов) –это один из самых мощных механизмов обеспечения сетевой безопасности. А обход firewall – это, соответственно, один из самых мощных механизмов обеспечения сетевой опасности :). В следующем номере мы будем знакомиться с обеими этими штуками: как с firewalling'ом так и с обходом его результатов.

СПЕЦ ХАКЕР

10(23)2002
октябрь 2002

Ежемесячный, тематический, компьютерный журнал

ВЗЛОМ продолжение следует

ISSN 1609-1027
(game)land
№10(23), октябрь 2002

СКАНИРОВАНИЕ УДАЛЕННЫХ ОSей

• Методы сканирования портов • Who Is? – наводим справки •
• Весь необходимый софт для сканирования и сбора информации •
• Перенос зоны DNS – ковыряемся во внутренней сети •
• Все стандартные порты с описанием служб •

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**

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