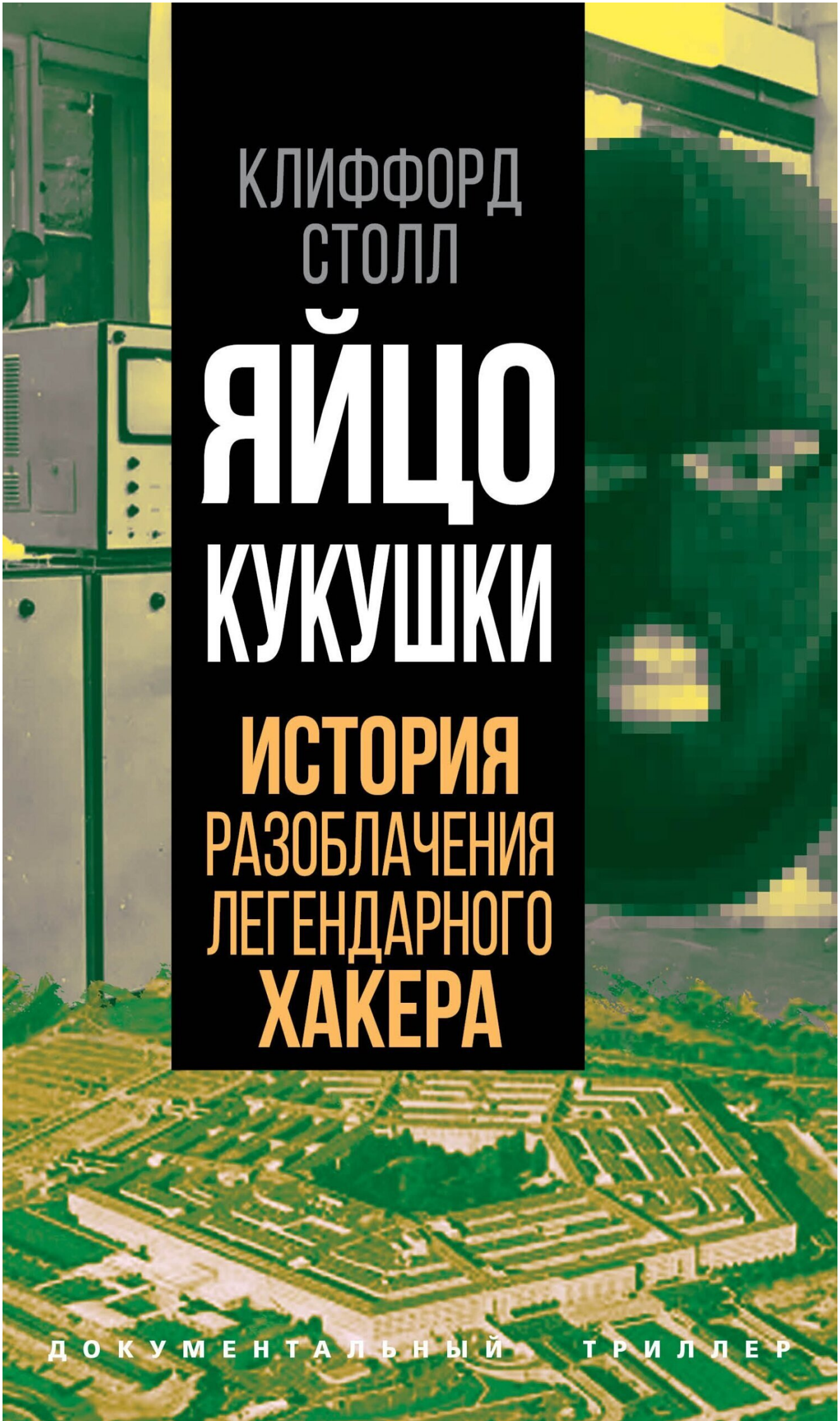
КЛИФФОРД СТОЛЛ
ЯЙЦО КУКУШКИ
ИСТОРИЯ РАЗОБЛАЧЕНИЯ ЛЕГЕНДАРНОГО ХАКЕРА
ДОКУМЕНТАЛЬНЫЙ ТРИЛЛЕР

Документальный триллер

Клиффорд Столл

Яйцо кукушки. История разоблачения легендарного хакера

«Алисторус»
1989

УДК 323
ББК 66.4

Столл К.

Яйцо кукушки. История разоблачения легендарного хакера /
К. Столл — «Алисторус», 1989 — (Документальный триллер)

ISBN 978-5-00180-800-8

В отличие от плохого танцора, хорошему сисадмину мешают только кукушкины яйца. Их откладывают в его компьютер злобные хакеры, чтобы из них вылупились программы, делающие своего папу-кукушку суперпользователем. Сисадмин Клиффорд Столл случайно обнаружил, что кто-то посторонний входил в систему, используя данные уволившегося полгода назад сотрудника. Началась охота на хакеров, которая закончилась задержанием в 1987 году жителей ФРГ — легендарного хакера Маркуса Гесса и трех его подельников Ганса Хьюбнера, Дирк-Отто Бжезинского и Карла Коха, которые успешно атаковали 400 компьютеров Министерства обороны США и его подрядчиков и продавали добытые секреты КГБ. Автор подробно и честно рассказал о том, как смог разоблачить советских кибершпионов. В отличие от посвященных этой же проблеме американских фильмов, изрядно нашпигованных техническими ляпами, этот документальный детектив без ошибок описывает работу охотников за хакерами. В формате PDF A4 сохранен издательский макет книги.

УДК 323
ББК 66.4

ISBN 978-5-00180-800-8

Содержание

Клиффорд Столл
Яйцо кукушки. Преследуя шпиона в компьютерном лабиринте

Clifford Stoll
The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage – New York: Doubleday. 1989

Глава 1

Волшебник, я? Еще неделю назад я был астрономом и в свое удовольствие орудовал телескопами. Сейчас, оглядываясь на это времечко, я вижу, что подремывал годами, пока не уплыли последние денежки по моему гранту.

К счастью, в обсерватории Кек при Лаборатории Лоуренса в Беркли астрономов принимали на вторичную переработку – и вместо биржи труда я оказался в компьютерном центре, в подвале Лаборатории. Могу показать парочку компьютерных фокусов, чтобы потрясти астрономов. Гораздо быстрее коллег разбираюсь во всяких головоломных ситуациях. Выходит, я – компьютерный волшебник? Не знаю, все-таки главное для меня – астрономия…

А что теперь-то? Уныло глядя на терминал, я продолжал думать об орбитах планет и астрофизических явлениях. Как новичку, мне довелось выбирать между застекленным отсеком с единственным окном, выходящим на мост Золотые Ворота, и душным кабинетом, заставленным книжными полками. Наплевав на свою клаустрофобию, я остановился на последнем в надежде незаметно дремать за письменным столом. Рядом располагались кабинеты Вэйна Грэйвса и Дэйва Клэвленда – «зубров»-системщиков. Они громко и постоянно цапались между собой, поэтому я разузнал много любопытного. Вэйн находился в натянутых отношениях с остальными работниками – по его мнению, некомпетентными лентяями. Сам-то он систему знал назубок, начиная с программ-драйверов и кончая СВЧ-антеннами. Единственной приличной вычислительной машиной он считал ВАКС, выпускаемый фирмой ДЭК. Других компьютеров для него просто не существовало – он не признавал ни ИБМ, ни ЮНИКС, ни Макинтош.

Дэйв Клэвленд – безмятежный Будда ЮНИКСа – терпеливо выслушивал бурные речи Вэйна, который безуспешно пытался его подначить: «Ученые всего мира выбирают ВАКСы. Эти машины позволяют создавать надежные программы дюжиной способов!» Дэйв парировал: «Вы осчастливьте „фанатов“ ВАКСа, а я позабочусь об остальных». Увы, Клэвленд не раздражался, поэтому неудовлетворенный Вэйн угасал и погружался в ворчанье.

Прекрасно. В первый же рабочий день я оказался маслом на бутерброде, который регулярно падал мною вниз и тем самым прерывал мой дневной сон. Зато мой внешний вид вполне соответствовал стандартному облику сотрудника лаборатории Беркли: поношенная рубашка, потертые джинсы, длинные волосы и дешевые кроссовки. На управленце можно было иногда увидеть и галстук, но при этом заметно снижалась производительность труда.

В обязанности нашей тройки (Вэйна, Дэйва и мои) входило обслуживание компьютеров лаборатории. Мы ведали дюжиной больших машин – громадных «тяжеловозов», решающих физические задачи. Стоили эти «рабочие лошадки» примерно шесть миллионов долларов. Надо полагать, что ученые, использующие эти компьютеры, рассматривали их как простых производителей, надежных не меньше, чем взаправдашние кони: работать они должны круглые сутки, а мы – старшие конюхи – несли ответственность за каждый цикл вычислений. Из четырех тысяч сотрудников лаборатории услугами главных компьютеров пользовалась примерно четверть. Для каждого из этой тысячи ежедневно велся учет машинного времени, при этом «гроссбухи» хранились в компьютере. Час вычислений стоит триста долларов, поэтому учет надо было вести страшно скрупулезно, и нам приходилось гоняться за каждой выводимой на печать страницей, за каждым блоком дискового пространства и за каждой минутой процессорного времени. Для сбора такой информации имелся отдельный компьютер. Раз в месяц на нем распечатывались отчеты и рассылались по отделам.

Однажды ко мне ввалился Дэйв и невнятно забормотал о неприличном поведении системы учета ЮНИКСа. Кто-то использовал несколько секунд машинного времени, не заплатив за них. Баланс не сходился; по счетам за прошлый месяц на сумму 2387 долларов была обнаружена недостача в 75 центов. Докопаться до источника ошибки в несколько тысяч дол-

ларов – пара пустяков. Но причины недостач в несколько центов обычно зарыты глубоко, и такие раскопки – стоящая проверочка для начинающего компьютерного волшебника.

– Чисто сработано, а? – наивно сказал я.

– Разберись с этим – и ты удивишь мир, – ответил Дэйв.

Детская забава! Я погрузился в программу учета. Она была похожа на кастрюлю со смесью всего на свете, куда начинающий кулинар закладывал любимые продукты, мешал, пробовал, а в результате дал дуба. Однако это рагу все же насыщало нашу лабораторию и просто вылить его было нельзя. В нем я нашел куски, написанные на Ассемблере, Фортране и Коболе – древнейших языках программирования. Я бы не удивился, встретив процедуры на древнегреческом, латыни или санскрите. Конечно же, никакой документации в помине не существовало. Только самый наивный поваренок мог отважиться сунуться со своей ложкой, не зная броду.

Худо-бедно, но все же было чем заняться после обеда. Кроме того, оставался шанс выловить из этого компота ягодку покрупней. Дэйв показал мне системную процедуру учета подключений к компьютеру, занесения в журнал имен пользователя и терминала. Система фиксирует каждое подключение, регистрирует идентификатор задачи пользователя, расходуемое пользователем процессорное время и время отключения. Дэйв объяснил, что есть две системы учета. Обычная программа учета ЮНИКСа просто заносит в отдельный файл записи событий. Но Дэйв создал вторую программу, которая обеспечивает хранение более подробных сведений о том, кто пользовался компьютером.

Сменявшие друг друга группы скучающих студентов годами писали, писали и, наконец, написали программы анализа всей учетной информации. Одна программа производит сбор данных и «засовывает» их в файл. Вторая – считывает этот файл и вычисляет стоимость сеанса работы с компьютером. Помимо всего прочего существует третья программа, которая обеспечивает подведение итогов и распечатку счетов, рассылаемых по отделам. Итоговая сумма из этой третьей программы сравнивается с результатом, получаемым от внутренней программы учета. Два учетных файла, созданных одновременно различными программами, должны давать один и тот же ответ. В течение года все работало как часы, но на этой неделе что-то сломалось. Первое подозрение – ошибка округления. Похоже, что каждый элемент файла учета сам по себе правилен, но при суммировании разности в десятые доли цента накапливаются, что в конечном итоге и приводит к ошибке в 75 центов. Доказать это можно либо углубившись в анализ процесса работы программ, либо путем тестирования, подавая на вход различные наборы данных. Чтобы зазря не размахивать мачете в зарослях тростника, я написал свою коротенькую программу проверки файлов и убедился, что с первой программой проблем нет. Со сбором информации все в порядке.

Вторая программа отняла у меня больше времени. За час я слепил «заплату» и понял: все работает. Программа суммирует длительности промежутков времени и затем умножает их на стоимость. Потеря 75 центов – не на ее совести.

И третья программа ведет себя хорошо: рыщет по списку пользователей, имеющих право доступа, находит их регистрационные записи и распечатывает счета. Ошибка округления? Нет, ни в одной из программ не может пропасть и сотой доли цента. Странно. Откуда же взялись эти дурацкие 75 центов?

Ну что ж, пусть я гоняюсь за призраком, но упрямства мне не занимать: из принципа проторчу здесь до полуночи!

Еще пару-тройку раз все проверив, я сильно зауважал это доморощенное чудо света – программу учета. Факт, что баланс не сходился, но программы не виноваты. К этому времени я нашел список пользователей, имеющих право доступа, и понял, каким образом происходит составление счетов для отделов. Около 7 вечера мне на глаза попалось имя Хантер. У этого парня оказался неправильный адрес счета. Ага! В прошлый месяц он задарма попользовался компьютером ровно на 75 центов.

Вот оно что! Кто-то добавил подпольного пользователя. Элементарно! Победа! Когда я упивался сознанием своей гениальности, заглянула Марта, моя подружка, и мы отпраздновали мой маленький триумф в кафе «Рим» ночным капуччино.

Настоящий волшебник справился бы за несколько минут. Зато я утешал себя тем, что изучил систему учета и немного набил руку в древних языках программирования. На другой день я отправил Дэйву весточку по электронной почте, раскрывая суть трюка.

Дэйв появился у меня около полудня и, шлепнув на стол стопку инструкций, мимоходом буркнул, что никогда не вводил пользователя по имени Хантер – это, скорее всего, сделал другой менеджер системы. Вэйн отрезал: «Это не я. ЧЧИ». Он частенько завершал свои сентенции аббревиатурами. Эта означала: «Читай Чертову Инструкцию».

Я читал инструкцию. Операторам не полагалось вводить нового пользователя без занесения данных в систему учета. В других вычислительных центрах могли попросту нацарапать имя пользователя в журнале, поставить его на учет и дать команду компьютеру. Нам же нужно было следить за всем и всеми, поэтому наша система была поумней. Она содержала ряд специальных программ, позволяющих автоматически проделывать всякие там системные штучки и выполнять нудную бумажную работу. Никакому недотепе в голову не пришло бы вручную вводить нового пользователя. Сама же система такую плюху никогда не сделает.

И все же такой недотепа поработал. Правда, я не мог выяснить, кто он. Никто не знал Хантера. Не было на него и учетной документации. Поэтому я удалил это имя из системы – если начнет вопить, все вернем обратно.

Спустя день компьютер по имени Докмастер прислал нам сообщение по электронной почте: якобы некто из нашей лаборатории нагло пытался вломиться в его компьютер в прошлый уикенд.

Докмастер мог находиться где угодно, но все указывало на Мэриленд. Пересылаемое по электронной почте сообщение проходит через десяток компьютеров и каждый оставил на нем свою отметку.

Дэйв ответил на послание неизменным: «Разберемся». Жди, когда перестанет болеть голова от своих проблем. Однако что-то привлекло внимание Дэйва в полученном от Докмастера сообщении и он передал его Вэйну, сопроводив вопросом: «Что это еще за Докмастер?» Вэйн отдал послание мне и предположил: «Наверное, какой-нибудь банк». Я полагал, что Докмастер это одна из верфей военно-морского флота. Сообщение не выглядело документом особой важности, хотя может быть и стоило потратить пару минут и повнимательней присмотреться к нему. В послании указывались дата и время попытки ворваться в Докмастерский компьютер с нашего ЮНИКСа. Поэтому я проштудировал файлы, в особенности записи, сделанные в субботу утром, и опять наткнулся на расхождения в двух системах учета. По файлу, созданному «родной» системой ЮНИКСа, было видно, что пользователь, некто Свентек, зарегистрировался в 8-25, полчаса пробездельничал и отключился. Наша доморощенная программа также зафиксировала подключение Свентека, но по ее данным он активно использовал сеть с 8-31 до 9-01 утра. Мой бог! Время не совпадает, одна программа показывает активное бодрствование, а другая – глубокий сон.

Тут на меня навалилась куча других дел и я отвлекся.

Обедая с Дэйвом, я мимоходом заметил, что единственным пользователем, подключавшимся в момент попытки взлома Докмастерского компьютера, был некто Свентек. Дэйв уставился на меня и вопросил: «Джо Свентек? Он в Кембридже. Что же он такое творит?» Оказалось, что Джо Свентек, бывший лабораторный «гуру» по части ЮНИКСа, – это настоящий компьютерный волшебник, создавший дюжину дивных программ за последние десять лет. Джо год назад уехал в Англию, но его немеркнущая слава продолжала сиять по всей программистской Калифорнии.

Дэйва удивило, что Джо снова в городе – ни один из приятелей Свентека ничего о нем не слышал. «Должно быть, он подключился к нашему компьютеру через сеть», – предположил Дэйв.

– Ты считаешь, это Джо напроказничал? – спросил я.

– Да что ты! – возмутился Дэйв. – Джо – хакер старой закалки! Блистательный и изысканный, ничего общего не имеющий с нынешними ублюдками, поганящими слово «хакер». Не стал бы он вламываться в какой-то там мерилэндский компьютер. А если бы вломился, то и следа бы не оставил.

Любопытно: целый год Джо Свентек живет в Англии, ничем не проявляя себя вплоть до субботнего утра, затем пытается ворваться в мерилэндский компьютер и отключается, оставляя «отпечатки пальцев» в системе учета. Все это я высказал Вэйну в коридоре. Оказывается, Вэйн слышал, что сейчас Джо проводит свой отпуск в лесах, вдали от всяких компьютеров. «Забудь про эту чепуху. Приедет Свентек – и все прояснится. Я, правда, точно не знаю когда. ТУС.» Теперь Уже Скоро, если расшифровать Вэйна.

Моя головная боль – не Свентек, а расхождения в системах учета. Почему программы показали разное время? И почему в одном файле была зафиксирована активная деятельность, а в другом нет? Выяснилось: расхождение объясняется тем, что используется двое часов, и одни из них ежедневно отстают на несколько секунд. За месяц и набежало пять минут.

Но активная деятельность Свентека должна была быть зафиксирована в обеих квитанциях. Связано ли это с тем, что произошло с системой учета на прошлой неделе? Все ли я там раскопал? Может, собака зарыта в другом месте?

Глава 2

После программистских хлопот я сидел на нудной лекции по структуре галактик. Профессор с ученым видом бубнил себе под нос и разрисовывал на доске змеюшник из математических уравнений. Пытаясь не заснуть, я стал обдумывать ситуацию. Кто-то добавил нового пользователя. Неделю спустя подключается Свентек и пытается взломать мэрилендский компьютер. До Свентека не добраться. Похоже, пытаются обойти программу.

– Что значит эта попытка попользоваться задарма нашим компьютером? – спрашивал я себя. – Неужели нашли способ обойти систему учета?

Для больших вычислительных машин существует два типа программного обеспечения: программы пользователей и системные программы. То, что вы сами пишете и инсталлируете – это пользовательские программы, например, мои программы анализа атмосферы планет. Сами по себе они работать не могут. Они неспособны отдавать команды непосредственно компьютеру и вынуждены «разговаривать» с операционной системой. Когда астрономической программе требуется что-то сообщить, она не в состоянии просто взять и «выплюнуть» текст на экран моего терминала. Этот текст передается операционной системе, которая отдает команду аппаратуре на вывод.

Операционная система, а также редакторы, библиотеки программ и интерпретаторы языков программирования составляют системное программное обеспечение. Вам нет нужды писать эти программы: они поставляются вместе с компьютером. Никто не должен совать в них свой нос.

Программа учета – это системная программа. Чтобы влезть в нее или обойти, нужно либо быть менеджером, либо исхитриться получить право привилегированного доступа к операционной системе. Но как получить это право? Самое простое – войти в компьютер с паролем менеджера системы. Наш пароль не менялся месяцами, но вряд ли кто-то проболтался. Чужаку же никогда его не разгадать: «вайверн» – мифологический крылатый дракон. Но даже если вы и придуритесь под менеджера системы, то вряд ли будете валять дурака с системой учета. Она слишком туманна и, к тому же, плохо задокументирована. Хотя и работает. Стоп! Наша домороченная программа работает, как надо. Кто-то добавил нового пользователя, не обращаясь к ней. Может, этот кто-то не подозревал о ее существовании. Чужак не знает о наших маленьких хитростях. А наши менеджеры системы и операторы на них собаку съели. Джо Свентеку наверняка все известно. А как насчет чужака – хакера?

У слова «хакер» два разных значения. Приличные люди, компьютерные волшебники, способные заставить работать любую программу. Это не обычные инженеры-программисты, добросовестно отрабатывающие свои сорок часов в неделю, а фанаты, не отходящие от терминала, пока компьютер полностью не удовлетворит их любопытство. Хакер отождествляет себя с компьютером и знает его как самого себя. Именно таким меня считают астрономы: «Клифф не столько астроном, сколько хакер!» (Программистский народец, конечно, придерживается иной точки зрения: «Клифф не силен в программировании, зато какой астроном!» Еще в аспирантуре я понял, что лучше всего оставить каждую сторону при своем мнении). Но в общепринятом смысле хакер – это компьютерный взломщик[1]. В 1982 году, когда группа студентов использовала терминалы, модемы и телефонные линии междугородней связи для взлома Ком-

[1] Каким же словом лучше назвать компьютерного взломщика? Компьютерные волшебники старой закалки гордятся, когда их называют хакерами, и презирают проходимцев, присвоивших это имя. При общении по сетям они называют этих хулиганов века электроники не иначе как кракерами (от англ, cracker – хлопушка) и киберпанками. В Нидерландах существует специальный термин «computervredebreuk», что буквально означает «нарушение компьютерного мира». Хотите знать мое мнение? Такого варвара, как компьютерный взломщик, я могу обозвать только непарламентарно: «злодей», «негодяй» и «свинья».

пьютеров в Лос Аламосе и в Колумбийском Медицинском Центре, всей околокомпьютерной публике стало известно об уязвимости сетевых систем.

Частенько до меня доходят слухи о вторжении в чью-то систему; жертвами обычно оказываются университеты, а виновниками – студенты или подростки. «Способные студенты вломились в компьютер, хранящий совершенно секретные сведения». Обычно такие шалости не причиняют существенного вреда и списываются на хакерские проказы. Могли бы события, показанные в фильме «Военные игры», произойти в действительности – мог бы хакер-подросток взломать пентагоновский компьютер и спровоцировать войну? Сомневаюсь. Нетрудно напакостить в университетском компьютере в котором напрочь отсутствует система защиты. В конце концов, коллеги редко запирают двери друг от друга. А вот военные системы – другое дело. Попасть в них так же трудно, как и на военные базы. И даже проникнув в военный компьютер, войну не развяжешь. Такие решения, я думаю, принимаются не компьютером.

Машины лаборатории Лоуренса в Беркли не оборудованы какой-то особенной системой защиты, но от нас требуют держать чужаков подальше и пресекать злоупотребления. Мы не боимся, что сломают нашу систему, а просто не хотим, чтобы наше финансовое агентство и департамент энергетики наехали на нас. Если они потребуют выкрасить компьютеры в защитный цвет, то закажем кисти.

Чтобы не лишать счастья общения с компьютером наших друзей-ученых, обитающих по соседству, мы завели несколько учетных записей для гостей. Зная гостевые учетное имя и пароль, любой может пользоваться компьютером, пока на счет за машинное время не набежит несколько долларов. Хакер запросто может проникнуть в систему – дверь широко открыта. Однако много он не наработает – время ограничено примерно одной минутой. И все же, можно успеть полазить по системе, считать несколько файлов общего доступа и выяснить, кто еще подключился. Мы полагали, что небольшая брешь в системе защиты окупается прочими удобствами.

Осмысливая происходящее, я пришел к выводу, что здесь вряд ли пахнет хакерством. Кому интересна физика частиц? Большинство наших ученых просто сомлеют от счастья, если кто со стороны удосужится прочитать их опусы. Хакеру здесь просто нечего ловить – у нас нет ни суперкомпьютеров, ни тайн сексуальной индустрии, ни других секретных сведений.

За пятьдесят миль отсюда располагалась Лоуренсовская Ливерморская Лаборатория, выполнявшая секретные работы по разработке ядерных бомб и проекту Звездных Войн. Вот где непаханое поле для хакера! Но не подключенные ни к одной из сетей ливерморские компьютеры не допускали никакого внешнего доступа: полная изоляция.

Если кто-то вломится в нашу систему, что он сможет натворить? Ну, считать файлы общего доступа. Многие из наших ученых хранят в них свои данные, там же находится большая часть программного обеспечения. Хотя они и называются файлами общего доступа, чужак не может лазить по ним. Некоторые данные защищены законами о частной собственности или авторских правах, например, наша библиотека программ или программа обработки слов. Другие базы данных тоже не предназначены для широкого использования: списки адресов сотрудников лаборатории и незавершенные отчеты по текущим работам. Все это, правда, вряд ли может стать объектом охоты, поэтому ни о каком засекречивании сроду речи не было. Меня не трогает, если кто-то из гостей-пользователей узнает чей-то телефонный номер. Есть проблема посерьезнее: может ли чужак стать суперпользователем?

Чтобы одновременно удовлетворить потребности около сотни пользователей, операционная система разделяет аппаратные ресурсы (как многоквартирный дом разделяется на отдельные квартиры). Жизнь в каждой квартире течет независимо от соседей. Один квартиросъемщик смотрит телевизор, другой болтает по телефону, а третий моет посуду. И все это одновременно. Необходимые для этого средства – электроэнергия, телефонная связь и вода – предоставляются комплексом коммунального обслуживания. И каждый квартиросъемщик

ворчит по поводу плохого обслуживания и непомерной квартплаты. Так же компьютеры: один пользователь может решать задачу, другой – слать сообщение по электронной почте, а третий – рисовать картинки. Компьютерные ресурсы предоставляются системным программным обеспечением и операционной системой; и каждый пользователь нудит о ненадежности программ, путанице в документации и высоких расценках на машинное время.

Чтобы никто не совал нос в чужие дела, в двери каждой квартиры имеется замок, а у каждого квартиросъемщика – ключ. Нельзя зайти в чужую квартиру без ключа. Если стены толстые, то возня одного соседа не докучает другому. Право на «частную жизнь» в компьютере обеспечивает операционная система. Нельзя забраться в чужую область памяти, не зная пароля. И если операционная система позаботится о правильном распределении ресурсов, то пользовательские программы не будут мешать друг другу.

Но стены домов не такие толстые, чтобы голоса подвыпивших приятелей соседа не будили меня. А мой компьютер взбрыкивает, если одновременно на нем работает больше сотни человек. Как дому нужен управляющий, так и нашим компьютерам необходим менеджер системы, или суперпользователь. У управляющего есть специальный ключ-отмычка, которым он может открыть дверь в любую квартиру. Менеджер может прочитать или изменить в компьютере любую программу или данные, обойти защиту операционной системы и орудовать в компьютере на всю катушку. Такая власть необходима для обслуживания системного программного обеспечения («Разберись с редактором!»), для регулировки быстродействия системы («Что-то сегодня ни шатко, ни валко») и для того, чтобы люди могли выполнять свои задания («Эй, выдай Барбаре отчетец»). Привилегированные пользователи учатся ступать осторожно. Они не могут особо напортить, если их привилегии распространяются только на чтение файла. Но лицензия суперпользователя позволяет вносить изменения в любую часть системы – от его плюх не увернешься! Суперпользователь всемогущ. Когда наступает момент перехода на зимнее время, он переводит системные часы. Новый дисковый накопитель? Только он может поставить нужный драйвер. В различных операционных системах программисты с привилегированным доступом называются по-разному: суперпользователь, корень, менеджер системы. Их пароли и учетные имена ревниво скрываются от посторонних.

А что, если чужак-хакер получит в нашей системе привилегированный статус? Понятно, тогда он может открыть учетную запись для нового пользователя. Хакер, обладающий привилегиями суперпользователя, мог бы держать в заложниках кого угодно. Имея отмычку к системе, он мог бы вырубить ее, когда вздумается, или заставить валять дурака. Он мог бы читать, записывать или изменять любые данные в памяти компьютера. Ни один пользовательский файл не был бы закрыт для него. Системные файлы тоже были бы у его ног – он мог бы читать сообщения электронной почты до их доставки. Он мог бы даже изменить содержимое файлов учета, чтобы замести следы.

Лектор монотонно бубнил о гравитационных волнах. Внезапно я проснулся. Я все понял! Я подождал, пока слушатели задавали вопросы, сам что-то спросил, вскочил на велосипед и помчался в Лабораторию Лоуренса в Беркли. Хакер-суперпользователь! Кто-то вломился в нашу систему, завладел ключом-отмычкой, присвоил себе привилегии и превратился в суперпользователя. Но кто? Как? Когда? И, самое главное, зачем?

Глава 3

От Калифорнийского Университета до Лаборатории Беркли всего четверть мили, но склон холма, по которому проходит Циклотрон Роуд, настолько крут, что на велосипеде это расстояние можно покрыть лишь за пятнадцать минут. На моей развалине не нашлось нужной передачи, поэтому последние несколько сотен футов я почти полз на коленях. Наш компьютерный центр пристроился между тремя ускорителями частиц: 184-дюймовым циклотроном (на котором Эрнест Лоуренс впервые получил миллиграмм чистого, способного к расщеплению урана), Беватроном (при помощи которого был открыт антипротон), и Хайлаком (местом рождения полудюжины новых элементов).

Теперь эти ускорители уже устарели: их мегаэлектронвольты – вчерашний день, а бал правят гигаэлектронвольтные ускорители со встречными пучками. На наших старушках уже не получишь Нобелевскую премию, однако ученые по полгода ждут свидания с ними. Изучать на них ядерные частицы и исследовать новые формы материи с экзотическими названиями (например, кварк-глуонные плазмы или пионовые конденсаты) – одно удовольствие. А когда физикам не надо проводить свои эксперименты, потоки частиц используются медиками и биологами, в частности, для исследований в области терапии раковых заболеваний.

В разгар работ по Манхэттенскому проекту во время Второй мировой войны Лоуренсовские циклотроны были единственным средством измерения сечений реакций ядерного взаимодействия и взаимодействия урановых атомов. Естественно, лаборатория была окутана завесой секретности: она служила прототипом заводов по производству атомных бомб.

В 50-е годы все работы лаборатории Лоуренса в Беркли оставались засекреченными, пока Эдвард Теллер не основал Лоуренсовскую Ливерморскую Лабораторию, расположенную в часе езды отсюда. Все секретные работы были переданы в Ливермор, а несекретные – остались в Беркли. Может быть, специально, чтобы запутать врагов, обе лаборатории получили имя первого нобелевского лауреата из Калифорнии. Кроме того, обе они занимались исследованиями в области физики и финансировались Комиссией по атомной энергии – детищем Министерства Энергетики. Это почти все, что было у них общего. Для работы в лаборатории Беркли не нужен специальный допуск: здесь не проводились закрытые работы, да и военные контракты на горизонте не маячили. Ливермор, напротив, являлся центром разработки ядерных бомб и лазерного оружия по программе Звездных Войн. Неподходящее местечко для длинноволосого бывшего хиппи. Если лаборатория Беркли едва сводила концы с концами за счет ассигнований на науку и нерегулярных субсидий из университетских фондов, то Ливерморская – постоянно разрасталась. С момента создания Теллером водородной бомбы для всех проводимых в Ливерморе секретных исследований всегда находились средства.

В Беркли больше не велось работ по щедро финансируемым военным программам. Наградой за это была открытость. Нас тянуло к изучению любопытных явлений, и мы всегда могли публиковать результаты. Ускорители наши казались детскими игрушками по сравнению с чудищами швейцарского ЦЕРНа или расположенной в Иллинойсе Лаборатории Ферми. Но они давали громадное количество информации, которую приходилось обрабатывать на солидных компьютерах. Мы с гордостью смотрели на физиков, анализирующих на наших компьютерах информацию, полученную на других ускорителях.

По вычислительной мощности ливерморские компьютеры казались гигантами по сравнению с нашими (самые большие, самые быстрые и самые дорогие Крэи). Они помогали выяснить, что происходит в первые наносекунды термоядерного взрыва.

Из-за закрытости исследований большая часть ливерморских компьютеров была изолирована. У них было также несколько несекретных систем для обычных научных расчетов. Но все, что касалось секретных работ – не для простого смертного. Невозможно было также

ввести извне данные в ливерморскую систему. Например, разработчик взрывателей для ядерных бомб, пользующийся засекреченными компьютерами, должен был являться в лабораторию собственной персоной с магнитной лентой подмышкой. Он не мог пользоваться ни одной из сетей, пересекающих страну вдоль и поперек, не мог подключаться и гонять свою программу с домашнего терминала. Такова цена жизни в засекреченном мире.

Хотя по вычислительной мощности наши компьютеры были несравнимы с ливерморскими, они вовсе не были увальнями. Наш ВАКС – быстродействующий, удобный и популярный среди физиков компьютер. Нам не было нужды изобретать собственные операционные системы – мы купили готовую – VMS фирмы ДЕК – и содрали в университете ЮНИКС. Наши компьютеры можно было включать в какую угодно сеть и обеспечивать доступ к ним из любой точки земного шара. Когда в полночь решение задачи вдруг начинает вырисовываться, то я спокойно набираю телефон лабораторного компьютера с домашнего терминала, а не кручу педали велосипеда вверх по склону.

Но в данный момент я все же крутил педали и мчался на работу, мучаясь вопросом: «Неужели хакер?» Этим можно было объяснить все казусы с системой учета. Если бы чужак подобрал ключи к операционной системе и затребовал привилегии суперпользователя, то он мог бы по своему выбору стирать учетные записи. Или, еще хуже, мог начать калечить другие компьютеры. Я поставил велосипед и побежал через лабиринт кабинетиков. Было далеко за пять и основной народ уже сидел по домам. Что же делать, если кто-то лазает по системе? Ну, можно послать по подозрительному адресу электронную почту: «Эй, вы вправду Джо Свентек?» Можно заблокировать доступ Джо к компьютеру и посмотреть, что будет. От размышлений о хакерстве меня отвлекла лежащая на столе записка: астрономической группе необходимо знать, насколько ухудшится качество получаемых с телескопа изображений, если снизить требования к зеркалам. Это обещало вечер программных моделей. Хотя официально я больше с телескопами не работал, но слаб человек… И я вывел все графики.

На следующее утро я бурно доложил Дэйву Клэвлэнду: «Даю голову на отсечение, это хакер.» Дэйв сел, закрыл глаза и произнес: «Да, голову, оно конечно…»

Я почти слышал его мысли. Дэйв никогда не затягивал гайки в системе защиты, полагая, что физикам это не понравится и они поищут другое местечко. Он держал систему открытой, посвящая все время улучшению программ, а не навешиванию замков. Неужели кто-то злоупотребил его доверием?

Моим новым боссом был Марв Атчли. Тихий и чувствительный, Марв не мог держать народ в узде и распустил всю группу. Марк был полной противоположностью Рою Керту. В свои пятьдесят пять Рой выглядел как Родней Дангерфилд в роли профессора колледжа. Он занимался физикой в лучших традициях Лоуренсовской лаборатории, сталкивая между собой протоны и антипротоны и разглядывая оставшийся после этого мусор. Рой обращался со студентами и персоналом, как со своими частицами и античастицами: выстраивал их в очередь, накачивал и затем выстреливал ими в неподвижные объекты. Для исследований ему требовались большие вычислительные мощности – в лаборатории происходили миллионы событий всякий раз, когда включался ускоритель. Долгие задержки и долгие извинения настроили его против компьютерщиков, поэтому когда я стучал в дверь, то убеждал себя, что буду говорить только о квантовой физике и уж никак не о компьютерах. Мы с Дэйвом могли предугадать реакцию Роя на возникшую проблему: «Какого черта оставляете двери открытыми?»

Да, реакцию босса можно предугадать, но как на нее ответить? Первое, что пришло в голову Дэйву – это заблокировать чертов доступ и забыть обо всем. Мне же казалось, что следует попугать этого хулигана: пригрозить вызвать родителей. Вламывается-то, скорее всего, какой-нибудь студентишка из ближайшего университета. Но мы не были до конца уверены, что к нам вообще кто-то вламывается. Да, это объясняло некоторые неполадки в системе учета – кто-то узнает пароль менеджера системы, подключается к нашей машине, вводит нового поль-

зователя и сует нос в учетную систему. Но зачем пользоваться новым именем, если уже есть доступ к системе на правах менеджера?

Наш начальничек не любит плохих новостей, но все же ему пришлось, тяжело вздохнув, встретиться с нами во время обеда. У нас не было прямых доказательств хакерства – просто логические умозаключения, выведенные из обстоятельств: налицо банальная ошибка в системе учета. Если была попытка взлома, то неизвестно, как далеко она зашла. Не знаем мы также, кто взломщик. Рой Керт оборвал нас сразу же: «Почему я должен терять из-за вас время? Вы еще ничего не знаете. Разберитесь и представьте доказательства.»

Итак, как же разоблачить хакера? Найти хулигана, использующего атрибуты доступа Свентека, и проследить за его подключениями. Я провел весь четверг, беря на карандаш всех, кто подключался к компьютеру. Даже написал программу, заставляющую пищать мой терминал в начале каждого сеанса связи. Я не мог знать, что делает каждый пользователь, но я мог видеть его имя. Каждые две минуты мой терминал взвизгивал, и я смотрел, кто подключился. Вот несколько моих приятелей-астрономов, работающих над научным отчетом, вот аспиранты, корпящие над своими диссертациями. Больше всего подключалось чужаков, и я спрашивал себя: «Как определить, кто из них может быть хакером?»

В этот день в 12–33 подключился Свентек. Я почувствовал, как в мою кровь обильными порциями поступает адреналин. Затем – полный упадок сил, когда он исчез. Единственное, что осталось – это идентификатор его терминала: он использовал терминальный порт tt23. Задача – определить физические провода, соответствующие логическому имени tt23. Терминалам нашей лаборатории и модемам, подключаемым через телефонные линии, присвоены метки «tt», а сетевым подключениям – «nt». До меня дошло, что подключался этот парень либо из лаборатории, либо по телефонному каналу через модем. Теоретически можно было проследить всю цепочку – от компьютера до человека на противоположном конце. Но чтобы проверить все и всех, потребовалось бы месяцев шесть. Первоочередной задачей было выявить подключения из здания. Я подозревал, что использовался модем, связанный по телефонному каналу, но нельзя исключать и вход в компьютер из лаборатории. За несколько лет было подсоединено добрых пять сотен терминалов, и только Поль Мюррей во всем этом разбирался. К счастью, доморощенные схемы соединений были задокументированы лучше доморощенных программ.

Поль, один из наших аппаратчиков, как одинокий волк скрывался в логове из проводов. За панелью одного устройства он подсоединял детектор частиц к локальной системе Этернет. Эта система образует электронные конвейеры, объединяющие сотни малых вычислительных машин. Несколько миль оранжевого этернетовского кабеля, извиваясь как змея, пролегало по всей лаборатории. Поль знал каждый его дюйм. Когда я появился, он припаивал какой-то провод и встретил меня потоком отборной ругани. Он отказался помочь, пока я не представлю официального подтверждения, что мне действительно нужны схемы соединений. О, черт! Аппаратчики никогда не интересуются программистскими проблемами, а сами программисты в аппаратуре – ни бум-бум. Но я-то паять умел, поэтому взял его запасной паяльник и через две минуты, дуя на обожженные пальцы, выслушал скупую похвалу. Наконец, он выбрался из клубка этернетовских кабелей и показал мне все коммутационное хозяйство лаборатории. Здесь были телефоны, системы внутренней связи, радиоаппаратура и компьютеры, и все это – в переплетении кабелей, проводов, волоконно-оптических линий. Подозрительный порт tt23 входил в эту комнату, и вторичный компьютер подключал его к одному из тысячи возможных терминалов. Любому, кто наберет номер лаборатории, произвольным образом назначался какой-нибудь юниксовский порт. В следующий раз, когда я увижу что-то подозрительное, я должен буду сломя голову нестись к коммутатору и определять соединение, исследуя вторичный компьютер. Если соединение будет разорвано до того, как я успею, то, считайте, ничего

не вышло. И даже в случае успеха я смогу лишь определить пару проводов, идущих в лабораторию. До хакера еще далеко.

По счастливому стечению обстоятельств дневное подключение не прошло бесследно. Поль набирал статистику о том, сколько человек использовало коммутатор. Случайно он записал номера портов для всех подключений за последний месяц. Так как я знал время, когда Свентек использовал порт tt23, то можно было выяснить, как он подключался. Распечатка статистики показала, что сеанс, начавшийся в 12–33, длился одну минуту, а темп передачи данных составлял 1200 Бод. Это уже кое-что. Темп передачи – это скорость, с какой данные передаются по проводу. 1200 Бод – это 120 символов в секунду, т. е. несколько страниц текста в минуту. Подключаемые к телефонной линии модемы работают именно с темпом 1200 Бод. А для терминалов лаборатории используются более высокие значения – 9600 или даже 19200 Бод. Только человек, связывающийся с компьютером через модем по телефону, вынужден гонять свои данные через такую тонкую соломинку. Но именно анонимность и удобство телефонной связи наиболее привлекательны для посторонних пользователей. Так! Концы начинают сходиться. Я еще не мог доказать, что с системой балуется хакер, но уже видел, что кто-то подключается к ней через телефонный канал и использует атрибуты доступа Свентека.

Конечно, подключение с темпом передачи 1200 Бод – еще не доказательство факта хакерства. Все это неубедительно для босса. Я должен найти явное свидетельство хакерства. Но как?

Рой Керт однажды показал мне детектор частиц высоких энергий, подсоединенный к Беватрону: они зафиксировали огромное количество взаимодействий на субатомном уровне, которые в 99,99 процентах случаев можно было объяснить, применяя законы физики. Если потратить время, исследуя след каждой частицы, то можно прийти к заключению, что вообще-то все частицы подчиняются известным физическим законам и что открытие не состоялось. Другой подход – отбросить все объяснимые взаимодействия и заняться только теми, которые не подчиняются каноническим правилам. Астрономы – дальние родственники физиков – действуют аналогично. Успех им приносит изучение аномалий – квазаров, пульсаров, гравитационных линз – всего, что не укладывается в рамки построенных моделей. Знание статистики распределения кратеров на Меркурии позволяет вычислить, с какой частотой эта планета подвергалась бомбардировке на ранних стадиях развития солнечной системы. Но обратите внимание на несколько кратеров, пересекаемых скрепами и кряжами, и вы узнаете, как сжималась планета в процессе охлаждения в первый миллиард лет. Собирайте информацию и отбрасывайте все ожидаемое. Все, что осталось – предмет для размышлений.

Так, теперь попробуем применить все эти рассуждения и вычислить нежданного гостя. На моем столе стоял терминал, кроме того, я мог позаимствовать еще парочку. Предположим, что я пытаюсь контролировать все пути, ведущие в компьютерный центр. В систему входит примерно пятьсот линий подключения. Большая их часть работает с темпом передачи 9600 Бод, что соответствует приблизительно ста пятидесяти словам в секунду. Если одновременно работает половина линий, то мне придется читать свыше десяти тысяч страниц каждую минуту. Да, так ничего не выйдет.

Но быстродействующие линии связаны только с лабораторными терминалами. Мы уже отследили одно подозрительное подключение с темпом передачи 1200 Бод. Таких линий гораздо меньше и работают они намного медленнее. Пятьдесят линий с темпом 1200 Бод дадут сто страниц текста в минуту – все еще слишком быстро, чтобы можно было читать с экрана. Я не могу одновременно наблюдать за работой пятидесяти человек, но могу сделать распечатки всех интерактивных сеансов связи и потом прочесть. Кроме того, распечатка – уже доказательство, что некто вмешивается в работу системы; если же не обнаружится ничего подозрительного, то можно будет поставить точку. Тогда мне нужно будет фиксировать каждое подключение с темпом передачи 1200 Бод. Технически это вряд ли возможно, поскольку я не знаю, по какому телефону будет подключаться хакер: придется контролировать примерно четыре

дюжины каналов. И еще меня беспокоит этическая сторона. Имею ли я право следить за потоками информации, проходящими через наши каналы? Моя подружка Марта как раз заканчивала юридический колледж. За пиццей мы говорили на тему привлечения к ответственности взломщиков компьютеров. Я поинтересовался, будут ли проблемы, если я «прослушаю» потоки чужих данных.

– Значит, так, – невнятно проговорила она, пытаясь жевать и объяснять одновременно, – ты – не фараон, поэтому тебе не нужен ордер на обыск. Худшее, что тебя ждет – это обвинение в нарушении прав личности. Вряд ли люди, подключающиеся к компьютеру через телефонный канал, будут требовать, чтобы владелец системы не заглядывал к ним через плечо. Поэтому слушай на здоровье.

С чистой совестью я начал создание системы контроля. У нас пятьдесят линий с темпом передачи 1200 Бод. Хакер может воспользоваться любой из них. У меня не было оборудования, чтобы регистрировать информационные потоки.

Но есть простой способ зафиксировать хакерскую активность: так переделать операционную систему, чтобы при любом подозрительном подключении сама система фиксировала бы каждое нажатие клавиши на клавиатуре. Чертовски соблазнительно. Все, что потребуется – добавить несколько строк в программу «демон».

Демоны – это программы, копирующие данные из внешнего мира в операционную систему – глаза и уши ЮНИКСа. (Древнегреческие демоны – низшие божества – что-то среднее между богами и людьми. В этом смысле мои демоны были чем-то средним между богоподобной операционной системой и низшим миром, в котором живут диски и терминалы.) Я могу раскурочить демона и устроить этакий тройник: символы, введенные с клавиатуры хакера, будут одновременно поступать и в операционную систему, и на принтер. Просто и элегантно.

Вэйн напутствовал меня: «Если ты напортачишь, то развалишь всю систему. Превратишь ее в кучу навоза – и ройся потом. Только и радости, что увидишь на распечатке „Аварийное прерывание ядра“. Потом не рыдай у меня на плече!» Тут подскочил Дэйв: «Сынок, если твой хакер хоть что-то петрит в ЮНИКСе, то он просто обязан заметить изменения в демонах!»

Убедительно. Любой дока-программист заметит изменения в операционной системе. Как только хакер почует контроль, он превратит наши базы данных в груду мусора и слиняет. Перехваты следует производить так, чтобы их никто не засек. Невидимая и неслышимая слежка – вот что надо.

Может быть, просто записать поступающую по телефонным каналам информацию на магнитную ленту? Нет, магнитофоны не годятся, слишком много хлопот. Запись придется воспроизводить, когда хакер уже отключится. И, наконец, где я найду пятьдесят магнитофонов?! Единственный участок тракта, где можно перехватить поток данных – между модемом и компьютером. Модемы преобразуют телефонные гудки в электрические импульсы, понятные для наших компьютеров и демонов. Модемные шины представляют собой плоские двадцатипятипроводные кабели, проложенные под фальшполом коммутатора. К ним можно подключить принтер или персональный компьютер, регистрирующий каждый передаваемый через шины символ.

Потребуется всего-то пятьдесят телетайпов, принтеров и портативных компьютеров. Несколько телетайпов достать легко – обратиться в отдел снабжения. Портативные терминалы можно выклянчить у Дэйва, Вэйна и остальных ребят. В пятницу вечером мы подняли из коммутаторной дюжину мониторов. Остальные тридцать можно заполучить, когда все уйдут. Я бродил среди столов секретарш, заимствуя персональные терминалы. В понедельник, конечно, будет скандальчик, но легче после извиниться, чем сперва добиться.

Уставленный четырьмя дюжинами стареньких телетайпов и портативных терминалов пол воплощал ночной кошмар компьютерщика. Я дремал среди всего этого и мурлыкал колыбельную принтерам и компьютерам. Каждый из них перехватывал данные на отдельном канале,

и всякий раз, когда кто-то подключался, я вздрагивал от треска телетайпов. Каждые полчаса один из мониторов сообщал, что кончилась бумага или дисковое пространство, поэтому мне приходилось устанавливать новый рулон и перезагружаться.

В субботу утром я проснулся оттого, что Рой Керт тряс меня за плечо: «Ну, где же твой хакер?» Запах от меня шел, как от козла: я все еще был в спальном мешке. Я глупо моргал и бормотал, что надо просмотреть пятьдесят стопок распечаток.

Он фыркнул: «Ну, прежде, чем погрузишь свой нос в эти бумаги, верни принтеры. Ты, как маньяк, таскал оборудование. Думаешь, здесь твой личный огород?»

С осоловелыми глазами я поволок принтеры законным владельцам. На первых сорока девяти не было ничего интересного. Из пятидесятого свисало восемьдесят футов распечатки. Ночью некто пытался пробраться через дыру в операционной системе.

Глава 4

Хакер лазал по нашей системе три часа. Втайне мой Декрайтер записал весь сеанс на восьмидесяти футах бумаги. Зафиксирована была каждая команда, каждая ошибка набора с клавиатуры и все реакции компьютера. Этот принтер контролировал телефонный канал из Тимнета. Я не знал, что несколько наших линий с темпом передачи 1200 Бод не связаны с модемами, а идут из Тимнета – телекоммуникационной компании, обеспечивающей компьютерную связь по всему миру.

Ранее компания «Белл» монополизировала средства связи. Позвонить из Нью-Йорка в Чикаго можно было только по каналам фирмы AT&T. Используя модемы, можно передавать данные по местной телефонной линии, однако для междугородней связи помехи и дороговизна делают ее непригодной для организации взаимодействия между компьютерами. К концу 70-х годов другие фирмы тоже захотели погреть руки и предложили специализированный вид услуг – «телефон» для данных. Тимнет создал сеть, связывающую компьютеры главных городов. Идея Тимнета проста и элегантна: создать «хребет» для передачи цифровой информации, позволить любому желающему подключаться к этому хребту, используя внутригородские телефонные каналы, и затем передавать данные в любой компьютер. Система Тимнета весьма экономична: она обеспечивает сжатие данных, поступающих от нескольких десятков пользователей, в несколько пакетов и передачу этих пакетов в нужные компьютеры. Система устойчива к помехам и обеспечивает любое нужное быстродействие. Клиенты, кроме того, экономят свои денежки, поскольку для них обеспечивается доступ в удаленный компьютер с помощью телефонного звонка.

Чтобы удовлетворить потребности научных работников из различных уголков страны, лаборатория в Беркли также была абонентом Тимнета. Когда ученому из Стоунибрука, штат Нью-Йорк, надо подключиться к нашему компьютеру, то он просто набирает городской номер Тимнета. Поскольку его модем связан с Тимнетом, то все, что требуется – попросить подсоединить его к Лоуренсовской лаборатории в Беркли, – и можно начинать работать, как у нас за терминалом. Физикам из отдаленных уголков очень нравился этот вид услуг, и нам всегда было очень приятно сознавать, что что они спускают свои баксы на наш компьютер, а не на какой-нибудь другой.

Некто вламывался, используя Тимнетовский канал. Поскольку «щупальца» Тимнета тянулись по всей стране, то наш хакер мог находиться где угодно. Но в этот момент меня интересовало не где он, а что успел натворить за три часа. Моя догадка подтвердилась: для взламывания нашего компьютера использовались атрибуты доступа Свентека.

Это был не простой взлом. Хакер был суперпользователем.

Этот хакер напоминал кукушку. Кукушка откладывает свои яйца в гнезда других птиц. Это – гнездовой паразит: ее кукушат будут растить другие матери. Кукушата, вылупившись из яиц, выбрасывают из гнезд «родных» обитателей. Жизнь птенцов кукушки – это смерть птенцов других видов. Таинственный гость подложил в наш компьютер яйцо-программу, а система «высидела» ее и накормила привилегиями.

Этим утром хакер написал коротенькую программу захвата привилегированных прав. Обычно ЮНИКС не позволяет запускать такие программы, так как никогда не дает пользователю прав выше тех, которые ему назначены. Задача заключалась в том, чтобы замаскировать эту программу – кукушкино яйцо – так, чтобы система ее восприняла как родное дитя.

Каждые пять минут система ЮНИКС выполняет собственную программу с именем atrun. Atrun планирует другие задания и выполняет рутинную работу по «уборке дома». Она работает в привилегированном режиме на всю катушку, чувствуя за своей спиной могучую поддержку операционной системы. Если на место atrun подставить фальшивую программу, то она срабо-

тает через пять минут и получит полные системные привилегии. По этой причине atrun располагается в защищенной области памяти системы, доступной только менеджеру. Здесь и было гнездо кукушки: за пять минут хакер, наверное, успеет подменить atrun своей программой.

Чтобы обтяпать это дельце, ему нужно найти способ поместить яйцо-программу в защищенную область-гнездо. У операционной системы есть специальные защитные средства. Обычные программы копирования их обойти не могут; нельзя задать команду «скопировать программу в системную область».

Но было кое-что, чего мы никогда не замечали. Ричард Столман, свободный художник-программист, всегда громко заявлял, что информация должна быть открытой. Его программы, которые он раздавал задаром направо и налево, блистали остротой мысли, хорошим стилем и вдохновением. Столман создал мощную программу редактирования под названием «Гну-Эмакс». Гну – это гораздо больше, чем простой текстовый редактор. Ее очень легко перестроить под любого пользователя. Она здорово облегчает написание других программ. Естественно, что всем нашим физикам сразу потребовалась Гну; мы успешно инсталлировали ее, большую часть времени глядя в потолок. Была только одна проблема: в ней сидела плюха.

Инсталляция производилась так, что возможность пересылать файл из собственного каталога в чей-либо другой обеспечивалась необычным способом. Гну не проверяла, кто принимает этот файл, и нужен ли он в месте назначения. Она просто переименовывала его и меняла метку принадлежности. То есть происходила простая передача права владения от одного пользователя к другому.

Переслать файл из вашей области в мою нетрудно. Но лучше не пытаться переслать его в защищенную системную область – это может делать только менеджер. Программа Столмана должна была бы контролировать такие попытки. Но не контролировала. Это позволяло кому угодно переслать файл в защищенную системную область. Хакер это знал, а мы нет. Хакер использовал Гну для замены родной системной версии atrun на свою программу. Пять минут спустя система начала насиживать подложенное яйцо, и он получил ключи от нашего компьютера.

Гну оказалась дырой в системе защиты.

Теперь я все понял. Наш приятель должен был войти в систему с атрибутами пользователя-гостя, раздобыть привилегии, используя плюху в Гну, и затем добавить нового пользователя в учетные файлы.

На первых нескольких футах распечатки я ясно вижу, как кукушка готовит гнездо, откладывает яйцо и ждет, когда его начнут насиживать. Следующие несколько футов – и оперившийся кукушонок расправляет крылья.

Первое, что он сделал – замел за собой следы: переписал на место «родную» версию atrun. Затем покопался в электронной почте всех пользователей, ознакомился с новостями, сплетнями и любовными письмами. Он узнал о модификациях, внесенных за последний месяц, грантах и приеме новых служащих. Он искал изменения в файлах менеджера системы и узнал, что я только что поступил на работу. Он выяснил мой заработок и прочел резюме. И что самое страшное – ему известно мое учетное имя и то, что я – системный менеджер. В любом случае теперь мне лучше пользоваться другим именем.

Каждые десять минут хакер выдавал команду «who» (кто), чтобы проверить список пользователей, подключенных к компьютеру. Затем он проверил, нет ли изменений в операционной системе – если бы я подменил демонов, то он, конечно же, это обнаружил бы. Я чувствовал себя ребенком, играющим в прятки, когда водящий проходит в нескольких дюймах.

За первый час он написал программу, просматривающую всю электронную почту и ищущую любое упоминание о его деятельности. Ключом служили слова «хакер» и «защита».

Один сотрудник запустил программку «gather» (сбор), собирающую данные по эксперименту. Совершенно безвредная, она просто каждые пять минут собирала информацию и запи-

сывала в файл. Хакер обнаружил эту программу, поворочал мозгами десять минут, пытаясь понять, затем уничтожил. Он уничтожал любое задание, которое, как ему казалось, следит за ним. Он вскрыл мою почту, проверяя, нет ли в ней упоминания о хакерах. Вэйн был прав: если не замаскироваться, то он обнаружит слежку.

Мы должны быть неслышимы и невидимы. Когда хакер успокоился, он стал читать файлы. Изучив несколько командных файлов и комментариев научных работников, он нащупал пути в другие компьютеры. Каждую ночь наш компьютер автоматически связывается с двадцатью другими для обмена почтой и сетевыми новостями. Перед хакером было двадцать новых мишеней.

Из почтового файла:

«Привет, Эд!

Следующие две недели я буду в отпуске. Если потребуются данные, войди под моим именем в ВАКС. Учетное имя – Вильсон, пароль – Марианна (так зовут мою жену). Счастливо поразвлечься!»

Не знаю, как Эд, а хакер развлекся. Он подключился к ВАКСу через нашу локальную сеть и вошел с атрибутами Вильсона. Вильсон вряд ли узнает, что хакер ковырялся в его файлах, а скорее всего, ему плевать. Файлы содержали числовые данные, нужные разве что другому физику-ядерщику.

Наш непрошеный гость знал о существовании в лаборатории внутренних сетей. Десяток наших больших компьютеров был связан с сотней малых вычислительных машин; для этого использовались Этернеты, последовательные шлейфы и «жевательная резинка». Когда физикам нужно получить данные от подключенного к циклотрону компьютера, меньше всего они думают об элегантности. За несколько лет инженеры и техники оплели лабораторию паутиной кабелей, соединяющих компьютеры со всем, что работает. Локальная сеть охватывала каждый кабинетик. Организация этой сети основывалась на доверии. Если уж вы работаете на одном компьютере, то имеете право работать и на соседнем. Это экономит время: при использовании нескольких машин не надо знать больше одного пароля. Наш «друг» не мог знать, для чего используются эти системы, но уже нащупывал путь в локальную сеть, ища способ подключения к не исследованным пока компьютерам.

В конце сеанса на ленте принтера уже не осталось краски. Слегка поводив карандашом по бумаге, я все же с трудом мог различать следы, оставленные печатающей головкой: хакер скопировал наш файл паролей и затем отключился.

Меня отвлек звук бас-гитары. Прямо на улице играла группа «Грейтфул Дэд». Полиция не могла удержать народ и публика сидела прямо на газоне. Я выскочил из лаборатории и растворился в тысяче летних рубашек. Загорелые попрошайки – наследие шестидесятых – сновали в толпе, клянча билетики и предлагая программки, букетики и травку. Соло на барабанах доносилось со Строберри Каньон, добавляя тему судьбы, оценить которую могли только мы – дети полей. Жизнь била ключом – хакер не стоил того, чтобы из-за него пропускать концерт «Дэдов».

Глава 5

В понедельник утром исполнилось ровно две недели, как я здесь работаю. Я казался себе не таким уж волшебником…

Я подробно, как первокурсник, записал в журнал все события. Не то чтобы я намеревался использовать эти записи – просто хотелось попрактиковаться в текстовом процессоре Макинтоша. И еще я помнил «Правило большого пальца для астрономов»: все, что не записано – не существовало.

Босс потребовал меня к себе, как только пришел.

Я думал, что он в ярости из-за этих терминалов. Руководство у нас добродушное, но даже волшебникам не полагается тащить без спроса груды оборудования. Но Рой даже не заикнулся о терминалах. Его интересовал хакер.

– Когда он возник?

– В воскресенье, в пять утра, на три часа.

– Стер что-нибудь?

– Уничтожил одну программу, которая, как ему казалось, следит за ним.

– Опасность реальна?

– Он – суперпользователь. Может уничтожить все файлы.

– Можно с ним покончить?

– Наверное. Мы знаем одну дырку; можно легко заштопать.

– Полагаете, это его остановит?

Я мог догадаться, куда он клонит. Рою не хотелось захлопывать двери. Он знал, что мы можем легко аннулировать права доступа Свентека. А теперь, когда мы знаем про дыру, то и привести в порядок «Гну Эмакс»: достаточно добавить в программу пару строчек для проверки каталога назначения. Первое, что приходит в голову – прикрыть лавочку. Мы знаем, как хакер проникает в систему, и знаем, как его вышвырнуть оттуда. Но какие подарочки оставил нам наш загадочный гость? У каких еще пользователей он срисовал атрибуты доступа? В какие еще компьютеры вломился? Именно от этого болела голова. Распечатка показала, что хакер – весьма компетентный программист-системщик, способный использовать малейшие плюхи, о которых мы и понятия не имели. Что же он еще натворил?

Если вы – суперпользователь, то можете изменять любые файлы. Не перекурочил ли хакер системные программы, открывая себе черный ход? Не поставил ли заплату на систему, чтобы она распознавала его волшебный пароль? Не занес ли компьютерный вирус? В персональных компьютерах вирусы распространяются путем копирования самих себя в другие программы. Если вы передаете кому-нибудь зараженную дискету, вирус копирует самого себя в другую программу, распространяясь с дискеты на дискету. Если вирус доброкачественный, то его трудно обнаружить, правда, и особого вреда он не приносит. Но нетрудно соорудить злокачественный вирус, копирующий самого себя и стирающий файлы данных. Так же просто создать вирус, который будет спать несколько месяцев и в один прекрасный день вдруг взорвет все вокруг. Вирусы – это существа, преследующие программистов в их ночных кошмарах.

Обладая правами суперпользователя, хакер мог заразить нашу систему так, что ее потом уже никогда не вылечишь. Его вирус мог скопироваться в системные программы и затеряться в дебрях компьютерной памяти. Копируя себя из программы в программу, он увернулся бы от любой попытки его уничтожить.

В персональном компьютере можно заново установить операционную систему после ее уничтожения. Наша же подвергалась очень сильным изменениям. Мы не можем обратиться к изготовителю и сказать: «Дайте нам исходную копию». При заражении можно только реинстал-

лировать систему с лент, хранящих копию возобновления. Если вирус занесен шесть месяцев назад, то эти ленты тоже заражены.

Может, он поставил нам логическую мину – программу с «часовым механизмом», которая рванет когда-нибудь в будущем? Или, возможно, этот незваный гость «расстрелял» наши файлы, «убил» парочку заданий и «развинтил» систему учета. Не натворил он чего поужасней?

Можно ли доверять программам и данным? Мы не могли. Если вдруг он нашел другой способ взлома, то попытка вышвырнуть его не сработает. Необходимо выяснить, кто он, что натворил и что собирается делать.

– Скорее всего, это какой-нибудь студентик университета Беркли, – сказал я Рою. – Все они ЮНИКСовские волшебники и держат нас за идиотов.

– Я не очень в этом уверен, – сказал Рой, откинувшись в кресле. – Почему некто из Беркли вламывается через Тимнет, когда мог бы без труда набрать номер нашей системы и подключиться по телефону?

– Может быть, Тимнет – это крыша, – возразил я. – Укрытие. Если бы он прямо набрал номер лаборатории, то мы бы его накрыли. Но теперь нам надо следить и за Тимнетом, и за телефонными подключениями.

Мои размахивания руками не убедили босса. Может быть, научный опыт, а может быть, природная склонность к сомнениям развили в Рое критический склад ума: он не согласится, что это студент, пока его сюда не притащат. Уикендовские распечатки показали, что это, несомненно, хороший программист, но его можно было искать где угодно. Чтобы выследить парня, надо висеть на телефонных каналах. Изрядная работенка.

Рой принял решение не принимать решения. «Давай перекроем на день все сетевые подключения. Завтра утром я поговорю с директором лаборатории. Подумай, что надо сделать. Мы можем подождать, но рано или поздно мы сядем на хвост этому парню или просто вышвырнем его.»

Мне сильно надо гоняться за кем-то? Это отвлечет меня от программирования. Вряд ли ловля хакера имеет много общего с астрономией или физикой. Больше похоже на игру в прятки или в сыщика и вора. Но есть в этом деле и плюс – я могу изучить телефонные каналы и принципы работы сетей. Представляю себя ребенком, ворвавшимся в мамочкину спальню с воплем: «Ни с места! Бросай клавиатуру!»

Во второй половине дня во вторник позвонил Рой: «Директор сказал: „Это электронный терроризм. Бери все, что нужно, но поймай этого ублюдка. Забирай все машинное время. Потрать три недели. Схвати его за хвост!“»

За мной стоит все рассвирепевшее руководство. Вперед!

Глава 6

Я рулил домой, изобретая хитроумные ловушки для хакера. По мере приближения к дому мои мысли устремились в направлении ужина. Здорово, если к ужину меня ждут!

Вот уже несколько лет Марта Мэтьюс и я жили вместе. До этого мы были друзьями и настолько хорошо знали друг друга, что не могли даже представить, что когда-то были незнакомы. Мои приятели только руками разводили. Они не предполагали, что я способен оставаться с одной и той же женщиной столько лет. Я влюбился, ухаживал, затем мы почувствовали, что не можем обходиться друг без друга. Обычно я сохранял хорошие отношения с бывшими возлюбленными, но не делал попыток к продолжению романов. Цинизм и сарказм защищали меня. Но с Мартой – другое дело. Постепенно между нами исчезали все барьеры. Она настаивала, чтобы мы обсуждали наши разногласия, хотела знать причины моего настроения, требовала, чтобы мы оба думали о том, как лучше ладить. Иногда это трудно было вынести – я терпеть не мог ничего обсуждать, когда был раздражен, – но обычно действовало благотворно. У меня появился инстинкт построения гнезда. Мне нравилось в свободное время бродить по дому и устранять всякие там неполадки, ремонтировать выключатель, менять лампочки или чинить витражи из цветных стекол. Мы провели много уютных вечеров вдвоем: она – за шитьем, я – за чтением. Иногда играли в скрэббл. Я начинал чувствовать…

Жениться? Мне?! Нет. Ни за что. Брак – это конец, ловушка для дураков. Когда вы женитесь, от вас ждут, что вы останетесь на всю жизнь таким, как в первый день. Если дойдет дело до ругани, то смыться невозможно. И надоест видеть одно и то же лицо каждый день. Тоска и пошлость.

Жить вместе – совсем другое дело. Оба свободны. Мы добровольно выбираем, продолжать ли совместную жизнь. Мне так лучше, и Марта, кажется, довольна.

Я спрашивал себя, не расстроится ли она, если следующие несколько недель я буду ночевать на работе. За три недели надо отловить хакера. А реально? Пара дней уйдет на подготовку, еще несколько – на выслеживание в сети и захват с поличным. Вероятно, придется сотрудничать с полицией, значит, еще день или два. За две недели, наверное, управимся, и я смогу вернуться к обслуживанию компьютеров, а, может быть, займусь астрономией.

Мы должны сплести сеть, достаточно мелкую для хакера и достаточно крупную для наших ученых мужей. Я должен обнаружить хакера, как только он подключится к линии, и позвонить ребятам из Тимнета с просьбой отследить его.

Конец ознакомительного фрагмента.