Эссе по теме:
«Кража идентифицирующей информации: пароля и логина для доступа к интернету»

Студент 916 группы
Грищев Владимир

Побродив по сети легко можно обнаружить ссылки типа «Взломай Интернет!» или «Хакни провайдера!».

Давайте сначала чётко разберёмся, что понимается под термином "взломать Интернет или провайдера"? На самом деле это означает получить Login и Password, введя которые в окне терминала мы сможем пользоваться интернетом за чужой счёт. Получить их действительно можно. Существует достаточно много способов похитить пароли. Разделим их на две категории:

Похищение с сервера

Похищение у пользователя

Похищение с сервера:

На первый взгляд все выглядит очень просто: в результате удачного "взлома" сервера получаем зашифрованный файл с паролями, а затем расшифровываем его и получаем необходимые нам пароли.

Обычно провайдеры используют UNIX сервера, в которых файл с паролями хранится в папке etc под именем passwd (/etc/passwd).Так как логины не шифруются, то вся задача состоит в расшифровке паролей. Естественно, пароли зашифрованы таким методом, что дешифрация их практически невозможна. Но есть способ узнать пароль. Так как алгоритм шифрования известен, то с помощью метода подбора можно это сделать. Например, с помощью программы John the Ripper , которая берёт некоторое слово, шифрует его и сравнивает с тем, что написано в файле. Если совпадает, то мы получили правильный пароль. Так при мощном компьютере за несколько суток можно получить несколько паролей. Таким образом, главное достать этот файл, а дальше - дело техники.

На любом UNIX'е пароли хранится в файле /etc/passwd но очень часто в этом файле пишут что-то наподобие *, а настоящие пароли хранятся в другом месте. Поискать можно в следующих местах:

/etc/security/passwd
/tcb/auth/files//
/tcb/files/auth/../
/etc/master.passwd
/etc/shadpw
/etc/shadow
/etc/tcb/aa/user/
/.secure/etc/passwd
/etc/passwd[.dir|.pag]
/etc/security/passwd.adjunct
##username
/etc/shadow
/etc/security/* database
/etc/auth[.dir|.pag]
/etc/udb

Результат не гарантирован, но шансы есть. В крайнем случае, можно воспользоваться

программой getpwent (), которая отлавливает файл с паролями на наиболее мудрёных серверах.

Естественно, нужно замести следы. Следы - это файлы /etc/utmp, /usr/adm/wtmp и /usr/adm/lastlog. Редактируйте их с помощью специальной утилиты.

Недостаток этого способа в том, что многие провайдеры ставят у себя защитную систему с названием NIS(Network Information Server)/YP (Yelow Pages). Тогда вместо пароля выводится что-то типа +::0:0::: Если случилось такое, то стоит поискать другого провайдера (или перейти ко второму способу).

Похищение у пользователя:

Можно похитить пароль непосредственно у пользователя (с его компьютера или при вводе самим пользователем). В результате удачного "похищения" получаем один пароль. Тут, естественно не обойтись без специальных программ. Далее привожу несколько сценариев возможных действий.

Саботаж

1. Проникаешь в дом к пользователю и получаешь доступ к его компьютеру.
2. Ищешь в директории Windows по следующей маске: *.pwl. Если что-то нашел, копируешь это на дискету.
3. Смотришь свойства удалённых соединений. Если там задействован сценарий - смотри путь к нему, также копируй этот файл на дискету и быстро сворачивай свою деятельность.
4. Если был скопирован файл с расширением pwl, то необходимо скачать PWLHack (или что-то подобное). Если pwl был зашифрован методом, который практически невозможно расшифровать, то есть только один способ. Используя механизм шифрования пытаться подобрать пароль. Это можно сделать, например, с помощь программы PWLTOOL 6.51.

Итак, у нас есть зашифрованный pwl. Что с ним делать? Сначала проверим его размер, если он составляет ~688 Байт - можно его удалять, он, скорее всего, пуст. Если размер больше - идём дальше. Загружаем программу PWLTOOL 6.51 и выбираем pwl. Сразу запускаем "CheckPassFast" , может, все-таки нет пароля. Если имя pwl'a - RNA (то есть весь файл называется - RNA.PWL), то, ставим login: *Rna и запускаем тот же "CheckPassFast" (поле password оставляем пустым).

Далее можно попробовать проверить на "обычные" пароли (qwerty, 1234, 111, asd, test и т.п.) а также попробовать пароль аналогичный логину.

Если ничего не подошло, требуется собрать как можно больше информации про жертву (ведь есть полный доступ к его компьютеру). Если и это не помогло, попробуй другой логин. Windows не позволяет называть pwl более чем восьмью символами. Например, файл pwl называется "констант", следовательно, логин должен по идее быть таким же, но верным логином может являться "константин". Тоже безрезультатно? Пора открывать словарь. Выбираем вкладку Dictionary и ставим свой словарь. И опять пытаемся подобрать пароль из существующих слов.

Если это не сработало, то пробуем Brute Force с цифрами с 1-7 символов; 1 по 6 символы с латинским алфавитом (всё в том же Pwltool 6.51). Далее, пробуем с русским алфавитом. После этого, как правило, открываются большинство pwl' ов. Если и это не помогло - выбираем SmartForce. Этот режим работы отбрасывает “глупые” пароли типа: aabbcc, aaaab, saaaaa, dddsss и т.п. Устанавливаем длину пароля и уровень "умности". Последнее ставим где-то от 10 до 12. Если и это не помогло тебе, то ещё есть один способ. Копируем файлы user.dat и system.dat (из директории Windows) и нажимаем кнопку "adv" в Repwl и там везде включаем "use foreign registry files" и выбираем скаченные файлы. Также можно скачать у жертвы edialer.ini и во вкладке "More" окна Advanced features достать из него пароли. Там же есть еще масса полезных и мощных режимов работы.

5. Если вышеописанные пункты не удались, то можно попробовать установить на компьютер пользователя программу, регистрирующую появление окна терминала и записывающую нажатия клавиш (можно также записать все нажатия за день, а потом пытаться разобраться в логах)

6. На следующий день надо прийти, удалить программу и скопировать файл лога на дискету.

П.6 можно выполнять не на следующий день, а через некоторое время, убедившись в том, что пользователь соединялся с Интернетом (напр. говоришь: "Проверь почту!")

Болтун - находка для шпиона

Проникаешь в дом к пользователю и получаешь доступ к его компьютеру.
Ставишь программу, срабатывающую где-то через неделю, которая вызывает частые зависания компьютера, причём явно "связанные с интернетом" (напр. компьютер зависает при открытии окна терминала).
Входишь к нему доверие с тем, чтобы он позвал тебя для устранения "зависаний".
Приходишь к нему, расспрашиваешь про проблемы. Проверяешь всё и убеждаешься в "конкретных проблемах". Говоришь: "Чтобы всё исправить необходим логин и пароль интернета".
Удаляешь программу и получаешь "гонорар" (кстати, подобное можно делать только ради этого).

Примечание: Пользователь должен быль полным «чайником».

Камуфляж

Этот сценарий работает в том случае, если невозможно получить доступ к компьютеру жертвы, но известен его e-mail.

Для этого необходимо сначала скачать(Sub7, Net Bus или Back Orifice) или написать самому программу – троян.

Остановимся немного более подробно на том, что такое программа-троян.

Теоретически, "троянским конем" называют программу, которая помимо своей основной документированной функции делает еще что-то нехорошее. Классическим примером троянца можно считать неоднократно описанную в различных (полу)фантастических рассказах ситуацию, когда какая-то корпоративная программа, не обнаружив в платежной ведомости фамилию программиста, ее написавшего, начинала всячески "шалить". В старые времена трояны писались именно как некие дополнительные функции какой-то основной программы. В наше время "чистых" троянов осталось очень мало (в принципе, известную историю о передаче уникальных идентификаторов пользователя на сайт Микрософт при обновлении Windows, можно считать примером классического троянца). Основным различием между вирусом и троянцем можно считать то, что вирус после своего "выхода в свет" не имеет никакой связи с создателем, а троянец предназначен как раз для последующего взаимодействия с запустившим его пользователем. Если в старые времена троянцы ориентировались на одиноко стоящую машину (возможно, многотерминальную), то сейчас они, как правило, ориентированы на сети, в первую очередь Интернет. Не стоит путать удаленную атаку и троянцев (хотя троянцы иногда являются одним из элементов атаки) - если атака похожа на штурм крепости, то троянцы - это свои "диверсанты" в станах этой крепости.

Что делают трояны? По большей части, они занимаются тем, что воруют пароли для доступа в Интернет и другую "секретную" информацию (например, номера кредитных карточек) и пересылают ее "хозяину" (а как вы думаете, откуда на "хакерских" сайтах берутся пароли для бесплатного подключения?) Другой распространенный вариант - это установка различных серверов для удаленного управления. Если подобный "зверь"

оказался у вас в системе, то его хозяин сможет работать на вашем компьютере почти как на своем собственном (или же просто пакостить, к примеру, отключая модем). Также, "серверный" троянец может представлять из себя, скажем, FTP-сервер, и позволять злоумышленнику загружать к вам или скачивать от вас любые файлы. Встречается, например, и такая экзотика, которая незаметно для пользователя устанавливает программное обеспечение для распределенного взлома RC5 алгоритма и использует его компьютер в пользу той или иной команды.

На западе встречаются трояны, которые автоматически звонят на 900-е телефонные номера (это номера, за разговор по которым абонент платит дополнительные деньги, скажем, пресловутый "секс по телефону"). В общем, число разнообразных пакостей определяется только фантазией авторов...

Как троянцы попадают на компьютер? К сожалению, однозначно тут сказать ничего нельзя - иначе, можно было бы просто перекрыть эти пути и не беспокоиться. Чаще всего, заражение происходит, когда пользователь запускает какую-то программу, полученную из "сомнительного источника". Стандартным способом распространения троянов является рассылка писем от имени известных серверов, причем в письме указывается, что прицепленный файл - это новая программа/заплатка и т.п. Другой способ - письмо, якобы по ошибке попавшее не туда. Основная задача таких писем - заинтересовать вас и заставить запустить прицепленный файл. Учтите, что даже прицепленная картинка может оказаться троянцем: можно, например, назвать его "1.gif много пробелов .exe" и прицепить соответствующую иконку - и вы в своей почтовой программе увидите только кусок названия: "1.gif". Не менее распространенной является маскировка троянцев под новые версии известных программ (в том числе антивирусов) и под троянцев. Так что, если вы решите поразвлечься и подсунуть трояна своему знакомому, то не исключено, что и сами окажетесь жертвой злоумышленника. Общее правило: всегда с подозрением относитесь к файлам, полученным из незнакомого источника. Да и из знакомого - тоже. Любой файл, полученный вами по почте, если вы заранее не договаривались о его отправке вам, скорее всего, окажется трояном. Большинство, так называемых, "хакерских" программ, предназначенных для взлома сети и т.п. - тоже окажутся троянами. Кстати, довольно часто троянца можно определить и по стилю письма.

Как вычислить трояна? Для того, чтобы троян мог творить свое "черное дело", он должен быть запущен у вас на компьютере. В первый раз вы запускаете его сами, но надеяться на то, что вы будете делать это каждый раз - нельзя. Соответственно, троянец должен позаботиться о том, чтобы не умереть после перезагрузки компьютера. В Windows есть три места, откуда программа может автоматически запуститься при загрузке системы: папка Автозагрузка, win.ini и реестр (разумеется, есть еще различные драйвера, но такие сложные трояны встречаются очень редко). Секции автозапуска в реестре такие:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
Так что, если вы будете периодически проверять эти места, скажем, с помощью PC Security Guard или RunServices, на предмет "неопознанных" программ, то с большой долей уверенности сможете обезвредить троянов. Другое дело, что надо еще разобраться, что это именно троян. Дело в том, что в Windows живет огромное количество файлов, и определить должен ли этот файл здесь "жить" или это "пришелец" довольно сложно. Тем более, что многие трояны имеют достаточно правдоподобные названия, например browser.exe или spoolsrv.exe... Уже запущенного трояна определить сложнее, хотя тоже возможно. Нажав Ctrl-Alt-Del или используя какую-нибудь специальную программу, можно посмотреть список процессов, запущенных на вашем компьютере. С помощью утилиты netstat (или другой аналогичной) можно посмотреть, с кем и на каком порту ваш

компьютер устанавливает связь. Правда, для пользования этими утилитами (точнее, для того, чтобы понять их результаты) требуются определенные знания. Кстати, косвенным признаком наличия трояна может служить Интернет-активность вашего компьютера в то время, когда вы ничего не делаете (хотя с тем же успехом, это может оказаться какая-нибудь безобидная утилита, проверяющая в фоновом режиме ваши закладки или кэширующая страницы). Ну и, наконец, традиционный способ: антивирусы. К сожалению, до последнего времени большинство из них боролось именно с вирусами, отлавливая некоторых троянцев в качестве побочного результата. На мой взгляд, лучшие результаты здесь показывает AntiViral Toolkit Pro - его база троянов достаточно велика и включает наиболее распространенные их них. Существуют также утилиты, защищающие от того или иного трояна, но они довольно неудобны: существуют сотни троянов, а запускать сотню утилит для защиты от них довольно проблематично.

Далее необходимо написать программу-приманку. На неё будем ловить пользователя.
"Склеиваем" специальной программой сервер трояна с приманкой.
С помощью электронной почты, например, отсылаем письмо с вложенным в него трояном, а в письме расхваливаем программу-приманку так, чтобы пользователь обязательно запустил exe'шник.
Сервер трояна присылает тебе IP жертвы. Сидим и караулим жертву в интернете. Как только обнаружим его, закачиваем ему программу, следящую за нажатиями клавиш и запускаем её.
На следующий/через день опять караулим пользователя. Скачиваем лог, в котором ищем Логин и Пароль.

Программа-приманка пишется для того, чтобы пользователь запустил программу-троян. Её расхваливают как могут, например:
Патч для Quake 8.
Обновление Quake до восьмой версии.
Обновление ICQ до 21 версии.
Ускорение Интернета в 10 раз.
Ищет и уничтожает CIH (вирус).
Свой вариант.
Приманка делает что-нибудь из следующего списка:
Проверяет на вирус (какой-то, который не может обнаружить не один коммерческий антивирус.)
Пишет красивым шрифтом (с эффектами) какой-то текст (напр. поздравляет с Новым Годом).
Свой вариант.

Итак, если всё сделано правильно, то у нас есть в наличии Логин и Пароль для входа в Интернет за чужой счет.

Примеры кражи идентифицирующей информации с помощью «троянов».

6.02.2001
В федеральном суде Красногвардейского района Санкт-Петербурга прошло рассмотрение дела 22-летнего Александра Мараховского, который был признан виновным в причинении имущественного ущерба клиентам провайдерских компаний "Адмирал Телеком" и “Ситилайн”.
Он рассылал по электронной почте «троянов» клиентам этих компании, с помощью которых крал логины и пароли для доступа в интернет.

27.10.2000
Как сообщило агентство Associated Press, хакеры взломали компьютерную сеть корпорации Microsoft и, по имеющимся данным, получили доступ к исходникам новой версии операционной системы Windows и программного обеспечения Office.
Сотрудник Microsoft, пожелавший остаться неизвестным, сообщил журналистам, что хакеры послали в компьютерную сеть корпорации почтовый «троян» QAZ и затем воспользовались одним из зараженных компьютеров, чтобы получить пароль доступа к информации.

21.05.2001
Российская антивирусная компания "Лаборатория Касперского" опубликовала сообщение, предостерегающее пользователей от использования программы "CC-Bank". Эта программа позволяет бесплатно получать номера кредитных карт и прочую информацию о них в обмен на просмотр баннеров, которые, по утверждению авторов, помогают проекту существовать. Для получения одного номера нужно просмотреть 15 баннеров.
Под генератор номеров кредитных карт систем Visa и MasterCard маскируется троянская программа "Eurosol", которая крадет информацию о личных счетах пользователя в финансовой электронной системе WebMoney.
После запуска программы CC-Bank на экран выводится диалоговое окно, в котором и должны появляться баннеры. После просмотра 15 баннеров появляется номер и все выходные данные очередной кредитной карты. Тем временем троянская программа "Eurosol" копирует себя в каталог WinDir под именем Netbios32.exe и регистрируется в файле System.ini, что обеспечивает ей скрытый запуск при каждом старте Windows. Кроме того, программа сканирует систему на наличие защитного программного обеспечения ATGuard, и при его обнаружении изменяет настройки. После изменения настроек ATGuard не препятствует попыткам файла Netbios32.exe установить TCP/IP-соединение с внешними серверами.
Затем "Eurosol" сканирует содержимое жестких дисков в поиске ключевых файлов клиентской программы системы WebMoney с целью получения сведений о личном счете жертвы. "Eurosol" находит файлы Keys.kwm (секретный ключ) и Purses.kwm (виртуальный "кошелек"). В случае успешного поиска файлы шифруются и отсылаются на удаленный FTP-сервер, с которого потом преступник может получить все необходимые сведения о чужом кошельке.

При написании эссе использовалась информация с сайтов:

http://www.zudteam.org
http://money.gol.ge
http://soft.wp-club.net
http://hackonline.250x.com/trojans.html
http://hackonline.250x.com/pwl.html
http://www.xpage.clx.ru
http://promoter.150m.com/troyan.htm
http://hackzone5.stsland.ru/vir1.html
http://hackonline.stsland.ru
http://hacker.dax.ru/articles
http://mail.rc5.aha.ru
http://www.netoscope.ru