взлом пентагона

крис касперски ака мыщъх, no-email

настоящие хакеры не знают границ и проникают в закрытые сети различных могущественных организаций. как они это делают? продемонстрируем технику взлома на примере серверов милитаристского Пентагона, который вовсе не так защищен каким кажется

введение

Информационная война – это действительно война, а не игра в салочки. Если хакера поймают его будут долго и нудно иметь во все дырки бритоголовые дяди в далекой американской тюрьме. Не секрет, что наша страна предпочитает не ссорится с Америкой и выдает информационных преступников по первому требованию. А даже если не выдает, сажает сама, так что как ни крути, а все равно геморрой.

Первая задача хакера — есть обеспечение собственной безопасности. В статье "безопасный взлом через GPRS", опубликованной в прошлых номерах Хакера, описываются основные идеи, позволяющие взять верное направление. Тем не менее, угроза раскрытия все равно есть, поэтому до приобретения боевого опыта лучше практиковаться на виртуальных сетях, которые можно протянуть в любом эмуляторе, например, VM Ware.

Так же недопустимо оставлять на взломанном сервере никаких собственных инициалов или другой компрометирующей информации. И уж тем более недопустимо делиться этим фактом с друзьями или оставлять записи в рабочем журнале или дневнике. Даже у стен есть уши. Впрочем, все это лирика. Перейдем к делу.

Рисунок 1 Пентагон — объект нашей атаки

почему стратегические сети уязвимы?

Протянуть защищенную сеть очень легко. Обычная витая пара или коксиал, отрезанный от Интернета и хакеры сосут лапу. Но это в теории. На практике такая схема непрактична и нежизнеспособна. Пентагон не сосредоточен в одном-единственном здании, а представляет собой разветвленную организацию, сотрудники которой работают в различных странах и не могут мотаться за каждым документом к черту на рога. Тоже самое относится к коммерческим фирмам и корпорациям. Например, концерну BMW или FORD.

Развертывание собственной проводной сети было бы идеальным решением с точки зрения безопасности, однако, это не по силам даже такому могущественному государству как

США, поэтому, приходится использовать уже существующие каналы связи. Это в первую очередь X.25 сети, спутниковая связь, и, конечно же, Интернет. X.25 сети — весьма популярные и надежные каналы передачи данных, владельцами которых как правило выступают крупные телефонные компании (например, AT&T), опутавшие своими проводами весь мир. В основном они используются для связи между отдельными сегментами закрытой сети, расположенными в различных городах и странах. В сети можно найти множество факов по устройству и взлому X.25 сетей. Практически все нашумевшие взлома так или иначе связаны с X.25 сетями. Именно так был хакнут City Bank и множество других компаний. При наличии прямого выхода в сеть достаточно иметь обыкновенную терминальную программу, однако, в этом случае хакера смогут легко вычислить, поэтому, приходится искать шлюзы из Интернета в X.25. Чаще всего таким "шлюзом" становится слабо защищенная жертва, подключенная к X.25. Впрочем, при желании можно воспользоваться и более традиционными методами взлома.

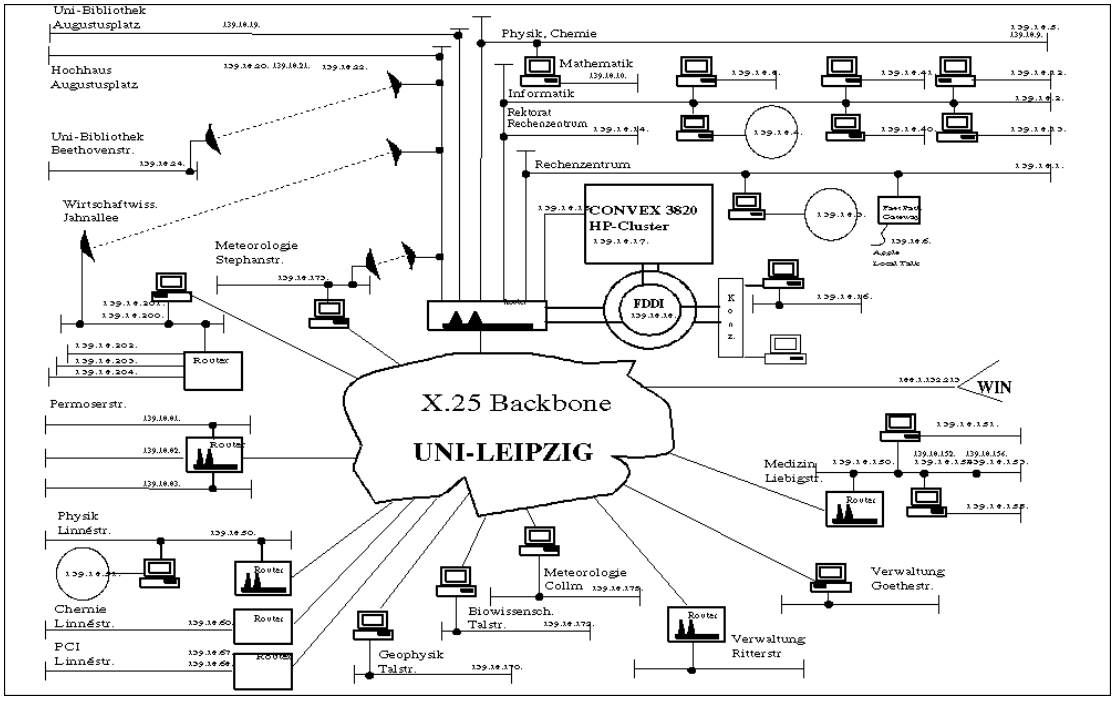

Рисунок 2 пример развертывания X.25 сети

Без представительства в Интернете никакая организация не обходится. Для полноценной работы требуется как минимум web-сайт, электронная почта, реже ftp-сервер и прочие второстепенные сервисы по вкусу. Опять-таки, с точки зрения безопасности, компьютеры, "смотрящие" в Интернет, должны быть физически отключены от "закрытой" сети, а весь обмен данными осуществляться только через съемные носители типа CD-R, причем, перенос информации с Интернет-компьютеров во внутреннюю сеть допустим только после тщательной проверки на наличие вредоносных программ, которые как известно могут внедряться не только в исполняемые файлы, но и в документы. Однако, соображения удобства берут верх над разумом и даже военные организации обычно ограниваются лишь тем, что огораживают закрытую сеть брандмауэрами и парольными системами защиты, но физический доступ к ней из Интернета все-таки есть, а **Интернет** — как известно, представляет собой совокупность узлов, объединенных маршутутизаторами. Маршутизатор — это обыкновенный или специализированный компьютер, который может быть взломан как и все остальное. Во-первых, многие маршутизаторы поддерживают возможность удаленного управления через telnet и имеют вполне предсказуемые пароли словарного типа, во-вторых, в них время от времени обнаруживаются ошибки переполнения буфера, приводящие к возможности захвата управления. Взяв маршутизатор под свой контроль, хакер может легко перехватывать трафик и даже модифицировать его! В частности, недавно в CISCO IOS уже обнаружилось две критические уязвимости (см. статью "завоевание Интернета или кто сказал "мяу" в хакере), а сколько их там есть еще — никто не знает. Контроль над трафиком открывает доступ ко многим секретным сетям даже тем, что не имеют представительств в Интернете, но используют

Интернет-каналы для своих нужд. В частности, трансатлантический оптоволоконный кабель обслуживает уйму закрытых учреждений и потому представляет весьма лакомый кусок.

У некоторых сотрудников (особенно внештатных) могут быть установлены модемы, принимающие входящие звонки, или уязвимое клиентское обеспечение. Не стоит забывать и о беспроводном оборудовании. Голубые Зубья, инфракрасные порты, wi-fi – все это может использоваться для проникновения.

основные способы атаки

Начнем с самого простого. **С сотовых телефонов и ноутбуков.** Подобравшись к зданию атакуемой организации на расстояние прямой видимости (с небоскребов оно будет видно за несколько километров, а то и дальше) и вооружившись снайперской антенной (см. статью "охота за голубым зубом", опубликованную в одном из последних номеров "Хакера"), мы сможем: а) обнаружить уязвимые устройства; б) посмотреть содержимое записной книжки сотового телефона; в) осуществить звонок с сотового телефона жертвы или передать SMS от ее имени на любой номер; г) посмотреть содержимое файлов ноутбука и заслать на него собственный shell-код. Разумеется, не всегда удается осуществить задуманное в полном объеме. Однако, количество успешных взломов этого типа стремительно растет, а окружающие нас устройства становятся все дырявее и опаснее.

Достоверно известно, что американские генералы активно используют ноутбуки от Compaq с Windows XP, в которой беспроводной стек реализован с грубыми ошибками, допускающими засылку shell-кода со всеми отсюда вытекающими последствиями. Так же достоверно известно, что ряд американских крейсеров управляются Windows NT, дыры которой хорошо известны. Таким образом, взлом военных объектов это не миф, а суровая реальность.

По опыту общения с отечественными военными могу сказать, что им категорически запрещено хранить какую бы то ни было мало-мальски значимую информацию на ноутбуке, но… они ее хранят, потому что так удобно. Что же говорить по американцев и всяких прочих банкиров. Они вообще с карманными компьютерами не расстаются. Знакомые автора не раз и не два вытаскивали через дырявый Голубой Зуб файл секретные файлы, просто направляя антенну в окна офисов или проезжающих мимо автомашин.

Основной недостаток такой атаки — необходимость прямого физического контакта с жертвой. Скажем, атаковать Пентагон из Урюписка уже не получится. А лететь в Америку чревато далеко идущими последствиями. В случае провала операции оттуда можно и не вернутся. Или вернуться уже седым стариком с широко раздолбанной задницей, что очевидно не входит в наши хакерские планы.

Спутниковая связь — другое дело. Вопреки расхожему мнению, спутник вещает не таким уж и узконаправленным пучком, покрывающим огромные территории. Кое-что можно ловить даже на ширпотребовскую тарелку, однако, для серьезной работы потребуется специальное оборудование на несколько тысяч долларов или… куча свободного времени, чтобы сконструировать его самостоятельно. Перехватом чужих передач сегодня увлечены многие. Конечно, в большинстве своем данные зашифрованы, ведь наверху сидят не дураки, однако… военный комплекс чрезвычайно инертен по своей природе и во многих местах использует морально устаревшие алгоритмы шифрования, которые вскрываются на современных процессорах за срок от нескольких дней до года. А ряд оперативных данных передается "открытым тестом" без какой либо шифровки вообще. Не так давно мы с товарищем (имени которого называть не буду, вы его все равно не знаете) надыбали очень интересный канал, передающий… прогноз погоды. Между прочим, очень точный и хороший прогноз, намного более полный, чем можно найти в Интернете.

Рисунок 3 передвижная станция спутниковой связи, используемая военными

Что же касается коммерческих корпораций, то там процент незашифрованной информации очень велик. И ловится он на обычную спутниковую тарелку. Нужно только перевести ее в "неразборчивый" режим. В основном попадаются рекламные ролики и другая медиа-информация, но иногда в хакерском клюве удается унести документы, касающиеся структуры внутренней сети или установленного на ней оборудования. Все это существенно облегчает дальнейший взлом…

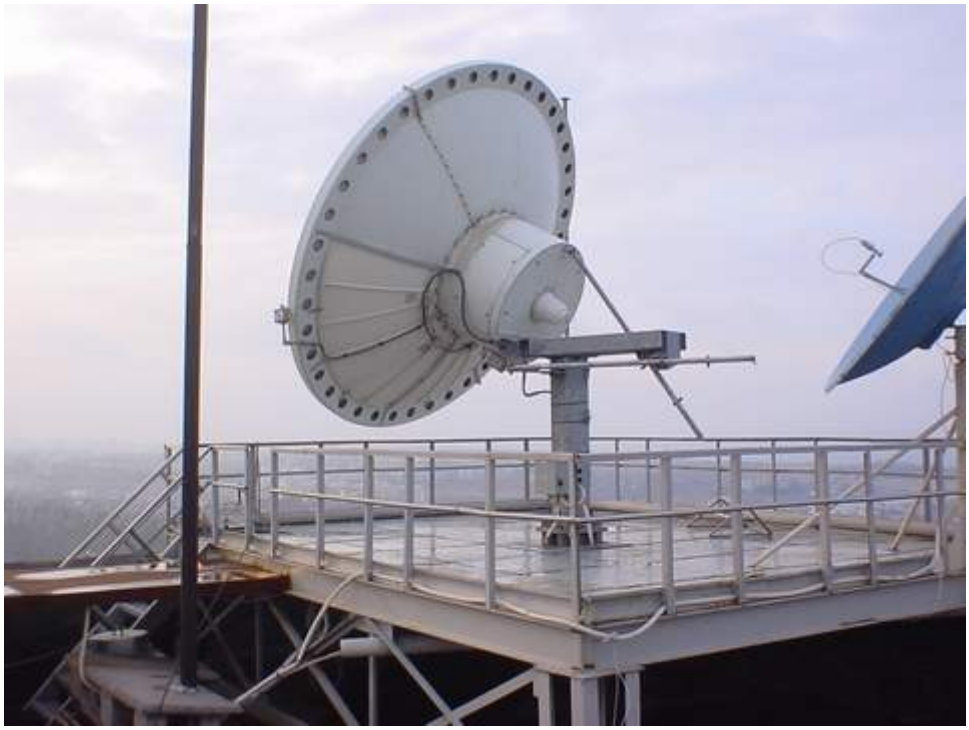

Рисунок 4 а это хакерская параболическая антенна для ее перехвата

Еще стоит упомянуть коротковолновый диапазон, используемый как любителями, так и профессионалами. Простой КВ-трасивер, стоимостью в пару сотен долларов (особенно, если это поддержанный отечественный девайс военного образца), позволит перехватывать многие секретные передачи. Обычно "говорят" морзянкой, но так же используют и человеческий голос, а в последнее время много информации передают в "компьютерном" варианте. Конечно, к локальным сетям радиоперехват никакого отношения не имеет, но от этого его популярность не уменьшается. В эфире можно услышать много такого, что не найдешь ни на одном из серверов Пентагона. Эфир — это настоящий Клондайк. Тем более, что он неподвластен традиционным средствам контроля и в нем можно найти множество друзей, в том числе и хакеров. Например, проинструктировать своих союзников, как взломать уже упомянутые ноутбуки американских генералов.

Рисунок 5 коротковолновый трансивер, используемый для радиоперехвата

Рисунок 6 еще один трансивер — попроще и подешевле

Впрочем, все это слишком экзотичные способы атаки, которые большинство читателей вряд ли воспримет всерьез и уж точно не воспользуется ими на практике по причине отсутствия весьма дорогостоящего оборудования.

проникновение через Интернет

Глотнув холодного пива (колы, квасу) и поплевав на лапки для храбрости, подсмыкнем трусы и наберем в браузере заветную строку www.pentagon.gov (см. рис 7). Конечно, это только публичный сайт, но во-первых, он связан с закрытой сетью, а, во-вторых, даже сам по себе он представляет весьма нехилую мишень для атаки. Можно ли его взломать? А вот мы сейчас попробуем и тогда все узнаем!

Рисунок 7 главная страница сайта Пентагона

Для быстрого анализа обстановки лучше всего воспользоваться одним из многочисленных сканеров безопасности. Лично я предпочитаю отечественный XSpider. Постоянно обновляемый, мощный, удобный в работе и… бесплатный. Ну… практически бесплатный. Демонстрационная версия находит все известные ей уязвимости, но сообщает минимум информации о дыре. К тому же имеется следующие ограничения: отсутствуют потенциально опасные проверки на DoS-уязвимости, проверки содержимого web-серверов на предмет SQL инъекций, инъекций кода, получения файлов и не содержат детали, отсутствует целый ряд проверок, использующих оригинальные эвристические механизмы, отсутствуют проверки, связанные с использованием различных словарей и т. д. и т. п.

Тем не менее, для большинства задач этого вполне достаточно. Главное — определить направление, в котором следует рыть, выявив все явно уязвимые сервисы, а все остальное можно сделать и самостоятельно. Свежую версию можно скачать с сайта http://www.ptsecurity.ru/. В zip-архиве она займет чуть больше, чем 4 мегабайта (http://www.ptsecurity.ru/download/xs7demo.zip). Полноценную версию можно либо заказать на сайте, либо найти в любом парнокопытном.

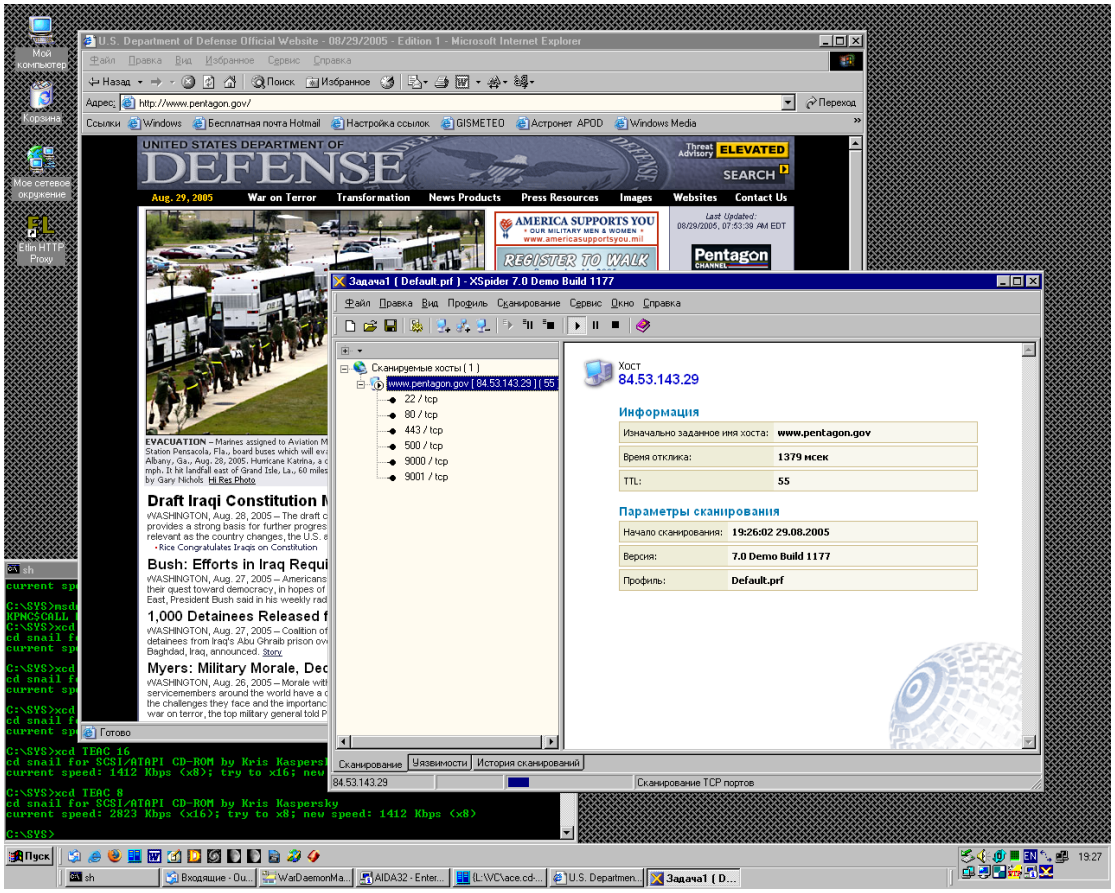

Рисунок 8 внешний вид сканера XSpider

К слову говоря, в военных организациях работают далеко не самые лучше специалисты, поскольку по условиям труда это скорее похоже на тюремное заключение, чем на убежище души. Так что вероятность успешного взлома весьма высока. Короче говоря, запускаем сканер, в меню "правка" выбираем "добавить хост" (или просто наживаем <Ins>), вводим имя атакуемого сервера (в данном случае www.pentagon.gov) или его IP-адрес (в данном случае 84.53.143.29) и ждем что XSider нам скажет.

Ждать придется довольно долго. Даже на шустрых DSL-каналах полный цикл сканирования занимает больше, чем три часа, в течении которых нам придется пить кофе и откровенно скучать, тупо созерцая строку статуса, комментирующую происходящее…

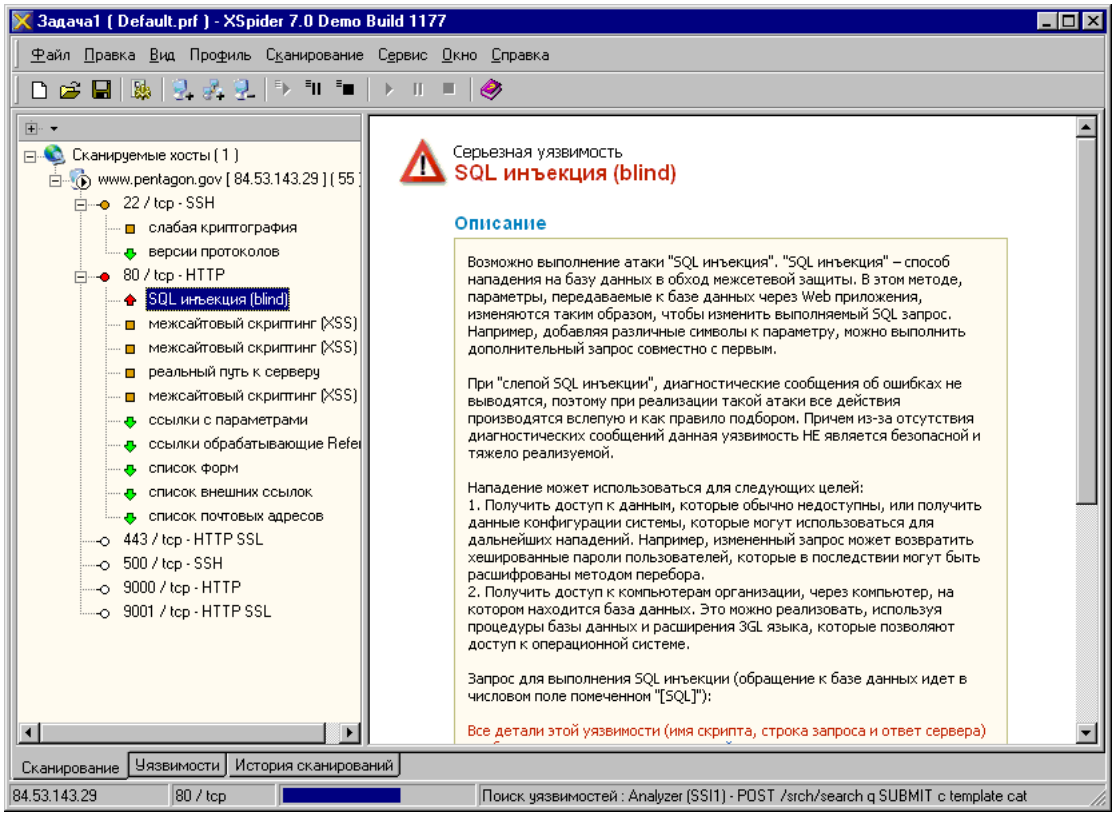

Рисунок 9 XSpider нашел критическую уязвимость в WEB-сервере Пентагона

Первым делом, XSpider определяет открытые порты. Их целых шесть — 22/TCP (SSH), 80/TPC (HTTP), 443/TCP (SSL), 500/TCP (SSH), 9000/TCP (HTTP) и 9001/TCP (HTTP SSL). Ради эксперимента можно подключиться к серверу по 9001 порту, набрав в строке браузера https://www.pentagon.gov:9001. И это сработает! Правда мы попадем на ту же самую страницу сайта, что и вначале, так что пользы от такого взлома немного. Но лиха беда начало!

XSpider определил тип SSL-сервера, в качестве которого используется SSH-1.99-Server-VI, основанный на OpenSSH Server, исходные тексты которого свободно лежат в сети. Если нам повезет, то основательно изучив их, мы найдем одну или несколько ошибок переполнения буфера, впрочем, быстрый успех маловероятен. Можно угробить кучу времени и все впустую. Лучше подождать, пока их не найдут другие, а затем быстро атаковать сервер, пока его не успели залатать. Но ведь мы не хотим провести всю оставшуюся жизнь в ожидании? ОК, тогда идем дальше!

SSL-сервер поддерживает устаревшие версии протоколов 1.33 и 1.5, которые недостаточно безопасны и могут быть взломаны за разумное время. Однако, для этого нам во-первых, необходимо тем или иным образом перехватить трафик, а, во-вторых, дождаться пока на сервер не постучится клиент, использующие протокол устаревших версий. Довольно малоперспективное занятие… Ладно, оставим SSL в стороне и возьмемся на WEB, который, как всегда выглядит довольно многообещающим скопищем багов.

Сайт Пентагона вращается под: Sun-ONE-Web-Server/6.1, а SunOS по сути является клоном UNIX'a. В ней намного меньше дыр, чем в LINUX'e, но намного больше, чем, например, в BSD. К слову сказать, использование рабочих станций от компании Sun вполне типичное явление для любой крупной организации и получить к ним доступ вполне реально, достаточно напоить пивом любого банковского администратора.

Сканирование WEB-сервера занимает львиную долю времени, зато обнаруживает уйму любопытных подробностей. XSpider обнаруживает шесть ошибок SQL-инъекций. Что такое SQL-инъекция? Это весьма коварная дыра, позволяющая формировать свои собственные запросы к базе и просматривать секретные данные. К сожалению, в демонстрационной версии отсутствует подробная техническая информация и нам остается лишь гадать как должен выглядеть хакерский запрос. Для удобства XSpider дает ссылку на коммерческую версию, а ниже несколько ссылок со статьями по теме SQL-инжектига. Очень удобно! Щелкаешь и читаешь! Кстати говоря, если поднять прошлогоднего Хакера, то в одном из номером можно найти нехилый материал "база данных под прицелом", где все расписано.

Еще Пентагоновский сервер подвержен межсайтовому скриптингу или, как его называют профессионалы — XSS (Cross site scripting). Упрощенно говоря, это возможность вставки HTML кода в уязвимую страницу. Добраться до секретных данных с его помощью навряд ли получиться, но зато можно перехватывать пользовательские сессии или навязывать всем посетителям сайта подложные данные, то есть делать дефейс. Учитывая, что сайт Пентагона — это информационно-политическое лицо Америки, к которому обращаются новостные агентства всего мира, целостность его содержимого очень важна. Хорошо продуманная деза может иметь далеко идущие последствия. Как всегда, XSpider приводит ссылки на статьи по теме кросс-скриптинга, которые будут полезны для анализа, но вот для определения формы уязвимого запроса потребуется приобрести коммерческую версию. Но мы же ведь не террористы и не вандалы, правда? Вот и не будем пакостить! Тем более, откуда у нищих студентов деньги?

Остальные дыры не так интересны. Из них можно упомянуть разве что успешно определенную версию и тип SSH сервера, в качестве которого используется AkamaiGHost. Дополнительную информацию и исходные тексты можно найти в Интернете, только навряд ли поиск переполняющихся буферов увенчается быстрым успехом.

Судя по всему сеть Пентагона не защищена брандмауэром. Пинг и трассировка проходят легко. Следующий листинг приводится к качестве подтверждения.

```
Трассировка маршрута к 84.53.143.29 с максимальным числом прыжков 30

  1  1650 ms     22 ms     22 ms  83.239.33.45
  2    27 ms     31 ms     79 ms  192.168.15.220
  3    34 ms     57 ms     27 ms  83.239.0.17
  4    28 ms     27 ms     27 ms  195.161.158.25
  5   149 ms    104 ms    144 ms  lnd-bgw0-ge0-3-0-0.rt-comm.ru [217.106.6.45]
  6   111 ms    202 ms    111 ms  195.66.224.202
  7   108 ms    107 ms    108 ms  84.53.143.254
  8   159 ms    128 ms    155 ms  84.53.143.29

Трассировка завершена.
```

Листинг 1 трассировка маршрута к серверу Пентагона

По современным меркам, корпоративная сеть без брандмауэра (или с демократически настроенным брандмауэром) это вопиющие исключение из правил. Впрочем, брандмауэр еще не помеха. Достаточно открыть "Хакер" со статьей "преодоление firewall'ов снаружи и изнутри" и раздолбать защитную стену в пух и прах.

Тоже самое относится и к сканировании IP-адресов. Пентагон от этого никак незащищен. Можно просканировать все подсеть целиком. Впрочем, она довольно обнообразна и ничего интересного в ней нет. В частности, узлы 84.53.143.27 и 84.53.143.28 держат открытыми следующие порты: 22/TCP (SSH), 80/TCP (HTTP), 123/UDP (NTP), 500/TCP (SSH) и 1935/TCP (TINCAN). Правда, при попытке подключиться к 80-порту нас ждет глубокий облом. Вот и ломись после этого туда, куда не просят. Как говориться, незваный гость хуже татарина.

заключение

Кончено, было бы наивно ждать от этой статьи демонстрации законченного взлома военных серверов или закрытых сетей. Во-первых, к моменту публикации информация неизбежно бы устарела (админы ведь не только кофе пьют), а, во-вторых, кто же захочет подписывать себе приговор, расписавшись в совершении преступления. Фактически, мы ничего не сделали, только запустили готовую программу, явно не относящуюся к числу вредоносных. Никакого злого умысла у нас тоже не было. Просто хотелось посмотреть…

И что же обнаружилось в итоге? Мы можем взломать сам Пентагон, если только захотим! Конечно, никто не говорит, что это будет легко, но это возможно!

>>> врезка хищение пароля

Как похитить пароль из закрытой сети? Это самое простое! Достаточно иметь e-mail человека, окопавшегося по ту сторону баррикады. Очень многие из нас имеют дурную привычку назначать одинаковые пароли на все ресурсы, хотя в "приличных домах" по соображениям секретности этого делать ни в коем случае не рекомендуется! Но… запоминать множество различных паролей тоже нереально. Один знакомый товарищ стянул из закрытой сети интересный архив с жизненно важной инфой. Естественно, запароленный, причем

запароленный не абы чем, а RAR'ом последней версии. Парольные переборщики отдыхают. Словарный поиск тоже не дал ничего интересного. После долго траха решили обратиться за помощью к самой жертве. Засовывать паяльник ей никуда не стали, но вот пару интересных ресурсов подсунули. Весь фокус в том, что эти ресурсы требовали аутентификации, то есть попросту говоря ввода пароля. Очень часто, жертва вводит свой любимый универсальный пароль. В крайнем случае становятся известны привычки жертвы – выбирает ли она в качестве паролей словарные слова, и если выбирает, то по какому принципу. В данном случае паролями оказались женские имена с четырьмя цифрами на конце, представляющими судя по всему знакомых девушке с датами рождения. Был составлен специальный переборщик и меньше чем за день секретный архив удалось открыть.

>>> врезка атака на администратора

Один из популярных способов проникновения в хорошо защищенную сеть выглядит приблизительно так: звоним администратору и сообщаем, что из абсолютно достоверных источников нас стало известно о готовящейся атаке, после чего сообщаем несколько туманных "деталей" в обтекаемых словах и вешаем трубку. Существует вполне определенная вероятность того, что администратор, пытаясь повысить безопасность своей системы, только добавит дыр (и эта вероятность тем больше, чем сильнее волнуется администратор).

Для отвлечения внимания можно прибегнуть к имитации атаки, выполняя различные бессмысленные, но целенаправленные действия. Известно случай, когда в ответ на мусор, направленный в 80й порт, администратор одного Интернет-магазина просто отключил WEB-сервисы, чтобы "спокойно" проанализировать ситуацию, поскольку, считал: лучше на время остаться без WEB'а, чем позволить хакерам проникнуть в локальную сеть и похитить конфиденциальную информацию. Естественно, простой WEB-серверов обернулся внушительными убытками, хотя никакой опасности на самом деле и не было.

>>> врезка шантаж

Если попытки проникнуть в сеть, несмотря на все усилия так и не возымели успеха, хакер может отважиться на прямой шантаж сотрудников фирмы. Статистика показывает, что угроза физической расправы встречается довольно редко, а, если и встречается, то в подавляющем большинстве случаев лишь угрозой и остается.

На первом месте лидируют обещания рассказать ревнивому мужу (жене) о супружеской измене, – не важно имела ли она место в действительности или нет. Для этого вовсе не обязательно устанавливать скрытые камеры или заниматься фотомонтажом, – достаточно быть хорошим рассказчиком, умеющим убедить собеседника. Опасаясь за распад семьи, многие из нас идут на мелкие (с нашей точки зрения) должностные преступления, оборачивающиеся, тем не менее, значительными убытками для фирмы.

Второе место занимают угрозы убедить сына (дочь) в том, что вы не настоящие родители. Поскольку, в подростковом возрасте между детьми и родителями часто случаются серьезные конфликты, вероятность того, что ребенок поверит постороннему дяде, чем и нанесет себе тяжелую душевную травму, отнюдь не нулевая!

>>> врезка: ошибка переполнения в WIDCOMM

Создатели Голубого Зуба предлагают готовое программное обеспечение для его поддержки, распространяемое под торговой маркой WIDCOMM (Wireless Internet and Data/Voice Communications — Беспроводной Интернет и Коммуникации для передачи Голоса и Данных), что избавляет производителей оборудования от необходимости реализовывать весь стек протоколов самостоятельно. Программисты старой школы (к которым принадлежит и Юрий Харон) хорошо знают истинную цену решений из "пробирки". Обжегшись на чужих ошибках пару раз, они не доверяют никакому коду, кроме своего собственного. И ведь не зря!

В августе 2004 года в WIDCOMM'е было обнаружено тривиальное переполнение буфера, позволяющее захватывать управление устройством простой посылкой специально подготовленного пакета. Никакой PIN для этого подбирать не нужно!.

Уязвимость затрагивает BTStackServer версии 1.3.2.7, 1.4.1.03 и 1.4.2.10, используемые в Windows 98, Windows XP, Windows CE и других системах. Кроме этого, WIDCOMM используется многими компаниями: Logitech, Samsung, Sony, Texas Instruments, Compaq, Dell… полный перечень включает в себя более трех десятков наименований. Все BlueTooth устройства, производимые этими компаниями, находятся под угрозой и в любой момент могут быть

атакованы. Для популярного наладонника HP IPAQ 5450 даже написан специальный эксплоит! В некоторых случаях, проблема решается установкой всех заплаток или сменой прошивки, некоторые же устройства остаются открытыми до сих пор.

Подробности можно найти здесь: http://www.pentest.co.uk/documents/ptl-2004-03.html