Аудит сетевой защиты

Щит и меч

Не имеет значения, обычный ли вы пользователь, выходящий в Интернет с домашнего компьютера, или администратор сети, в зоне ответственности которого десятки машин. От действий злоумышленников могут пострадать все.

Проверить надежность защиты можно только одним способом — попробовать ее взломать. Для этого можно пригласить «варягов» со стороны или попробовать самому. Не подвергая сомнению квалификацию и способности «варягов», лучше выполнять проверку сетевой защиты своими силами, а их помощью воспользоваться уже для окончательной проверки.

Техника сетевых атак

Нельзя построить и поддерживать надежную систему защиты без представления методов и особенностей сетевых нападений. Безопасность через незнание — плохой принцип. Поэтому необходимо обладать некоторыми сведениями и инструментарием взломщика. Рассмотрим общую методику анализа и взлома систем.

В общих чертах сетевая атака содержит следующие фазы:

- перехват и анализ сетевого трафика;
- сканирование портов — определение доступных сервисов;
- идентификация сетевых сервисов;
- исполнение сетевой атаки на основании полученных данных.

А сейчас подробнее о первых трех исследовательских фазах сетевой атаки.

Первая фаза — перехват и анализ сетевого трафика

Для осуществления анализа трафика злоумышленнику прежде всего необходимо получить доступ к машине, расположенной на пути сетевого потока. Используя специальное программное обеспечение, он имеет возможность перехватывать исходящие сетевые пакеты и просматривать их содержимое. Например, перехватив telnet или ftp-соединение, крэкер может считать пользовательские логин, пароль доступа и другую передаваемую информацию, так как эти протоколы не используют шифрование данных.

Возможный вариант защиты — отказ от использования сетевых сервисов, не использующих шифрование передаваемых данных во время соединения, и замена их соответствующими аналогами, поддерживающими криптозащиту. Для удаленного терминала можно использовать ssh, для передачи файлов — sftp, для web-сервисов — ssl или шифрование на уровне протокола IPsec.

В теории использование интеллектуальных свичей должно привести к такому результату, что каждая машина получает только адресованный для нее трафик. Но некоторые модели свичей уязвимы для сетевых атак вида «arp spoofing», которые нарушают таблицу маршрутизации свича, предоставляя крэкеру возможность перехвата трафика.

Вторая фаза — сканирование портов

Применяется для определения TCP/UDP-портов, через которые работают сетевые сервисы. Сканирование определяет тип сетевого протокола, вероятный тип сетевого сервиса и состояние порта — открыт ли он для доступа, или доступ к нему закрыт брандмауэром. На основании полученных во время сканирования данных о реализации стека TCP/IP-протоколов удаленной системы, можно сделать предположение о типе и версии операционной системы.

При сканировании могут использоваться различные методики установления соединений. Традиционное сканирование — последовательный перебор портов с попыткой установить соедине- »

» ние методом «connect()» (аналог вызова «nmap -sT my.host.domain»), в случае установления соединения программа прерывает его. Данный способ сканирования легко определяется по сообщениям сетевых сервисов об установлении и сбросе подключений.

В более интересном методе сканирования программа отсылает удаленной системе на определенный порт TCP/IP SYN-пакет, инициализирующий соединение (аналог вызова «nmap -sS my.host.domain»). Если какой-либо сервис прослушивает этот порт, удаленная система ответит SYN/ACK-пакетом, предложением продолжить установление соединения. В противном случае удаленная система отправит RST-пакет. Получив SYN/ACK-пакет, сканер отвечает RST-пакетом, прерывающим установление соединения. Соединение не устанавливается до конца, и сервис не будет записывать данные об этой попытке, так как произошел сброс. Есть и более интересные методы сканирования, но продолжение этой увлекательной темы выходит за рамки данной статьи.

Суть этого краткого обзора в том, что для определения попыток сканирования нельзя полагаться только на анализ лог-файлов сервисов, необходимо использовать специальные системы детектирования вторжения (например, snort). Также, настраивая активную защиту (блокировка доступа для IP-адреса или подсети, откуда производится атака или сканирование), необходимо соблюдать осторожность. Нападающий может имитировать сетевую атаку от постороннего IP-адреса (например, маршрутизатора), защита блокирует обмен трафиком с этим хостом — DOS («Denial Of Service» — отказ в обслуживании), и атака удалась — сеть неработоспособна.

Третья фаза — идентификация сетевых сервисов

Классическим методом идентификации сетевых сервисов («fingerprinting») стал сбор так называемых «баннеров». Баннером называется стандартное приглашение сервиса (FTPd, HTTPd, SMTPd, TELNETD, IDENTD). Из информации, заключенной в баннере, нередко можно получить данные о версии сервиса и используемой операционной системе.

Например, для HTTPd (web-сервер):

```
$telnet www.lenta.ru 80
Trying 81.19.69.28...
Connected to www.lenta.ru.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Fri, 03 Jan 2003 10:47:23 GMT
Server: Apache/1.3.26 (Unix) rus/PL30.15
Last-Modified: Fri, 03 Jan 2003 10:45:08 GMT
ETag: «34cc08-13274-3e1569b4-koi8-r»
Accept-Ranges: bytes
Content-Length: 78452
Connection: close
Content-Type: text/html; charset=koi8-r...
```

По информации в строке «Server: ...» можно сделать вывод о типе и версии web-сервера и используемой операционной системе.

По возможности изменяйте баннеры, убирая информацию о типе и версии сервисов. Или, что более интересно, подмените стандартный баннер сервиса на другой. Например, в баннере Microsoft IIS укажите, что это Apache.

Общие замечания

Изучите свою систему. Даже без троянских коней операционные системы часто открыты для доступа. Например, для семейства Windows начальные настройки служб Remote Procedure Call (RPC), NetBIOS и Messenger service дружелюбны для взломщика.

Регулярно проводите мониторинг и ведите лог-запись сетевой активности приложений на своем компьютере. Отключите неиспользуемые сервисы. Установите ограничения на доступ к остальным сервисам.

В стандартные приглашения сервисов внесите предупреждение об уголовном наказании за попытку несанкционированного доступа. Был судебный прецедент, когда компьютерного взломщика оправдали. Доводом защиты послужило то, что баннеры сетевых сервисов взломанных серверов содержали строку «Welcome» («Добро пожаловать» — англ.).

Регулярно проверяйте информацию о наличии ошибок и уязвимостей в используемом программном обеспечении. Информацию надо искать не только на сайте производителя. После обнаружения уязвимости и до ее исправления лучше отключить или ограничить доступ к сервису. После выхода заплатки для уязвимости не следует медлить с ее установкой.

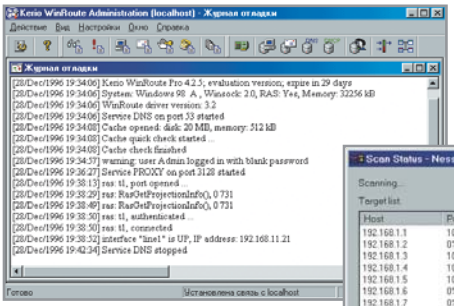
Аудит защиты

Перенесем исследование вопроса надежности сетевой защиты в более практический аспект — рассмотрим программный инструментарий и способы сетевого исследования.

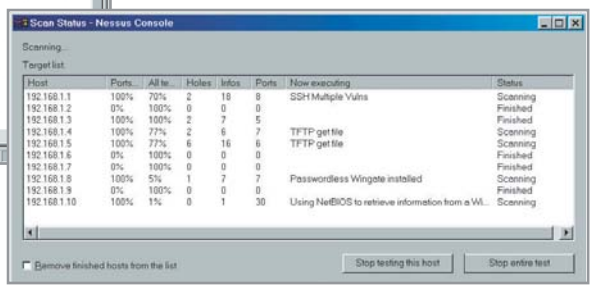
Хотел бы заметить, что применять знания лучше для исследования безопасности своей системы. Хотя сетевое сканирование ресурсов не является преступлением, взлом системы уже уголовно наказуем.

Анализ трафика

Для исследования сетевой активности будем использовать снифер (от англ. «sniffer» — нюхач. Программа, предназначенная для анализа сетевого трафика.) tcpdump. Разработанный для Unix-систем, tcpdump перенесен на Win- »



▲ Проверка настроек сетевого брандмауэра Kerio WinRoute Pro



▼ Просмотр отчета, полученного в ходе исследования сканером Nessus выбранной подсети, об обнаруженных уязвимостях

» dows-платформу (windump). Для своей работы сниферу необходим драйвер обработки сетевых пакетов pcap (Packet Capture library).

Дистрибутивы и документация размещены по следующим адресам:

- для Unix-систем: www.tcpdump.org
- для Windows-систем: http://windump.polito.it

В условии фильтрации можно указать: адрес получателя/отправителя (host), сеть (net или net/mask), порт (port), направление (src или dst), протокол (ether/fddi/ip/arp/rarp/decnet/lat/sca/moprc/mopdl/tcp/udp), размер пакета (less или greater). Для составления сложного фильтра из нескольких простых можно использовать логические условия: или (or), и (and), отрицание (not). Например, условие — показать все пакеты, отправленные хостом 192.168.1.10, где порт получателя 110, будет выглядеть так:

- src host 192.168.1.10 and dst port 110

Подробная информация о параметрах фильтрации доступна в виде man-документации, поставляемой с системой или в виде html-документов, доступных на сайте www.tcpdump.org.

Наиболее распространенные бреши в защите — это передача важных данных в открытом виде (например, telnet, ftp и pop-протоколы) и некорректная маршрутизация. Первая проблема обычно связана с обыкновенной человеческой ленью и недостатком знаний. Совсем несложно использовать ssl для web-сервисов, ssh вместо telnet, sftp вместо ftp и т. д. Вторая проблема может быть вызвана не только ошибкой сетевого администратора, но и некорректной работой программного обеспечения. Лучший совет: не доверять авторитету и заявлениям разработчиков, а проверять корректность работы самому.

Сканирование портов

Web-ресурсы

Провести сканирование портов своей системы можно, используя web-сервисы, например, на серверах www.cotse.com или www.void.ru. Некоторые компании — разработчики программных брандмауэров предоставляют на своих сайтах всем желающим web-сервисы для аудита надежности своих разработок (Norton PF, Sygate PF).

Необходимо заметить, что если между вашим компьютером и сканирующей системой находится сетевой шлюз, то сканироваться будет именно шлюз, а не ваша система. К тому же необходимо учитывать, что если вы подсоединены к Интернету по каналу с небольшой пропускной способностью, например с помощью модемного соединения, то сканирование может привести к нарушению работы канала и прерыванию в обслуживании.

Разнообразных сетевых сканеров существует довольно много: Internet Security Scanner, Network Superscanner, Satan, Strobe, Portscanner, XSpider и многие другие. Они отличаются методами сканирования, точностью, наборами функций, пользовательским интерфейсом, условиями распространения и многим другим. Примеры поиска уязвимостей и сканирования портов в данной статье будут приведены на основе сканеров Nessus и nmap. Причины тому — надежность, открытый код и условие свободного распространения.

Поиск уязвимых сервисов — сканер вторжения

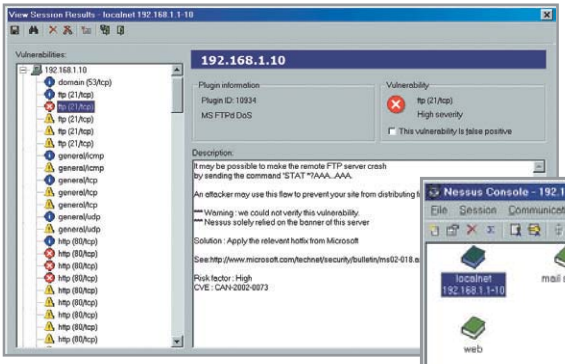
Сканер вторжения Nessus предназначен для поиска уязвимых и слабозащищенных сервисов. Nessus состоит из двух частей — сервер (unix-система) и клиент (unix или windows-система). Сканер имеет модульную архитектуру. Каждая возможная уязвимость описывается в виде отдельного модуля на специально разработанном языке NASL (Nessus Attack Scripting Language). База данных по известным уязвимостям постоянно обновляется. Управление сканером осуществляется как графическим интерфейсом, так и с помощью командной строки. Результат проверки системы может быть представлен в виде текстового отчета или, если необходимо, в документах формата LaTeX, NSR, HTML, XML. Сканер распространяется бесплатно в виде исходных кодов. Автор сканера Рено Дерезон (Renaud Deraison). Сайт разработчика www.nessus.org.

Для работы со сканером необходимо на сервере создать пользователя и определить его полномочия командой nessus-adduser. Зарегистрированный пользователь »

Случай из жизни

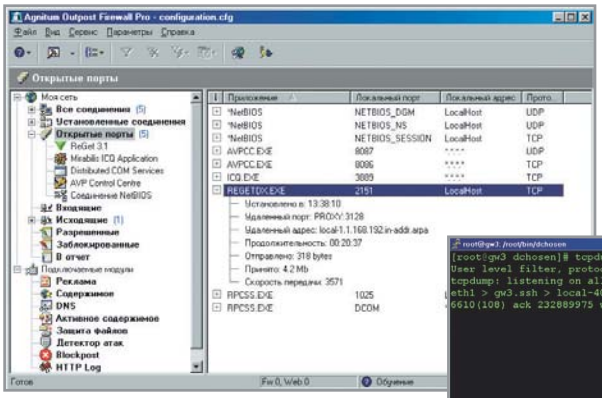
Всего один открытый порт

Два приятеля работали админами, один в Киеве, другой в Москве. Киевлянин как-то похвастался закупленной системой межсетевой защиты. Москвич ради интереса просканировал подсеть киевлянина и, в числе прочего, нашел открытый порт сетевого принтера. Решив подшутить над приятелем, он скинул на открытый порт текстовый документ. Через пару дней они связались. Москвич спросил: «Ну как, получил мое письмо?» Киевлянин закричал: «Как, это был ты?» Оказалось, что принтер принял переданный файл за последовательность управляющих кодов и данных. Напечатав несколько символов на странице, принтер выбрасывал лист и начинал печатать на следующем. Так было отстреляно около трех тысяч листов бумаги.

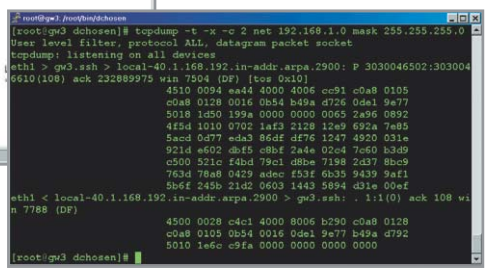


▼ Главное окно клиентской части сканера вторжения Nessus (NessusWX)

▲ Отображение в клиентской части сканера вторжения Nessus результатов сканирования выбранной подсети



▲ Просмотр статистики установленного сетевого соединения. Брандмауэр Outpost Firewall Pro



▼ Содержимое сетевых пакетов, переданных во время ssh-сессии, в шестнадцатеричных кодах. Пакеты перехвачены снифером tcpdump

» может подключаться к серверу nessusd, используя unix или win-клиенты Nessus. Более подробная документация поставляется вместе с системой и представлена на сайте разработчика.

Полезные утилиты

Напоследок рассмотрим несколько программ, которые могут пригодиться в защите вашего компьютера.

Snort

Система анализа сетевого трафика. Распознаются попытки осуществления сетевых атак «buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts». Реализована возможность оповещения администратора при обнаружении атаки. На базе snort можно построить свою собственную систему IDS («Intrusion Detection System» — система обнаружения вторжения). Для анализа логов snort можно использовать snort2html и RazorBack.

Perl

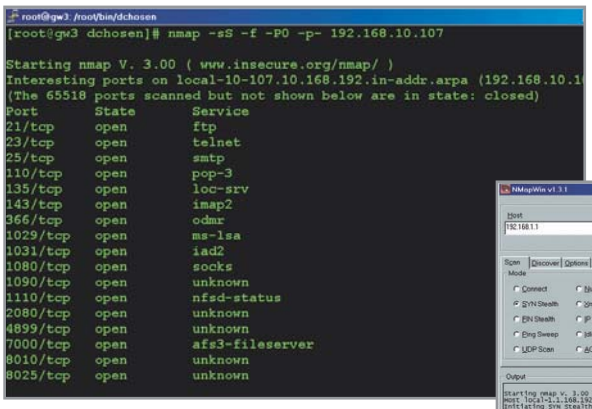
Вероятно, самый известный сценарный язык, пользующийся заслуженной популярностью. Название Perl происходит от сокращения Practical Extraction and Report Language («практический язык извлечения данных и формирования отчетов»), что точно отражает одно из его назначений. Мощное достоинство языка — развитый аппарат регулярных выражений. Perl-сценарии удобны для анализа лог-файлов сервисов.

Agnitum Outpost Personal Firewall

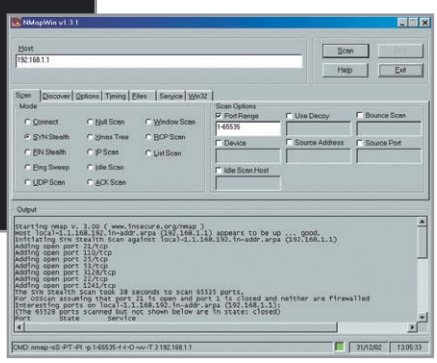
Программные персональные брандмауэры для Windows-систем. Осуществляется контроль сетевого трафика и сетевой активности программных приложений. Модульная архитектура предоставляет возможность для функционального расширения. Удобная и подробная система статистики предоставит полную информацию о сетевой активности системы. Продуманная система создания сетевых правил существенно облегчит настройку брандмауэра. Система управления активными web-элементами, возможности по удалению web-рекламы и кэшированию dns-записей — увеличат безопасность и ускорят загрузку web-документов.

Kerio WinRoute Pro

Брандмауэр ориентирован на применение в сетях среднего размера. Включает в себя маршрутизатор, почтовый сервер SMTP/POP3, а также DNS, DHCP и прокси-серверы. Предоставляет обширные возможности контроля сети. Kerio WinRoute Pro работает на всех Windows-системах и может обслуживать любой компьютер-клиент из корпоративной сети по протоколу TCP/IP независимо от используемой клиентом операционной системы — Linux, Mac OS, Unix, AS400 или какой-либо еще.



▲ В результате исследования выбранной системы сканером Nmap были получены данные о доступных сетевых сервисах



▼ Просмотр результатов сканирования системы, полученные сканером Nmap для Windows (NMapWin)

Заключение

Вопрос не в том, будут пытаться взломать вашу систему или нет. Вопрос в том, когда ее попытаются взломать. Ответ — быстро. Почти сразу, как только вы подсоединитесь к Интернету. Будут ли взломщики новичками или профессионалами — это вопрос другой. Следы первых обычно легко заметны, а профи вы, скорее всего, сразу не увидите. Вашей задачей является заставить первых искать более легкую добычу, а вторым серьезно осложнить задачу.

Для разработки плана защиты необходимо иметь представление о сетевой активности вашей системы. Используемые сетевые протоколы, передаваемые данные, системные сервисы и пользовательские приложения — обо всем необходимо иметь представление и обладать возможностью контроля. Детальное представление схемы сетевой активности существенно облегчит построение сетевой защиты.

Не следует забывать, что разработка и поддержка сетевой защиты — это интеллектуальное соревнование между нападающим и защитником. Постоянное развитие методик нападения и защиты требует пристального внимания. Ценой совершенной ошибки будет потерянная информация — самое ценное в этом тысячелетии, как уверяют все социологи. ■ ■ ■ **Александр Красоткин**