Лекция 9

Пассивные сетевые атаки

Типичный сценарий атаки

Стадия 1: Внешняя разведка

На этой стадии нарушители собирают как можно больше информации об атакуемой системе, ничем себя не выдавая. Они могут делать это, собирая общедоступную информацию, маскируясь под действия обычного пользователя.

На этой стадии нарушителя невозможно обнаружить. Нарушитель будет высматривать "кто есть кто", чтобы собрать как можно больше информации о целевой системе.

Нарушитель, возможно, использует для этого DNS-таблицы (используя утилиты 'nslookup', 'dig' или другие средства, используемые для работы с DNS), чтобы найти имена машин, принадлежащие исследуемой сети. Нарушитель будет разыскивать другую открытую информацию, такую как публичные Web- и FTP–сервера с анонимным входом, принадлежащие компании. Нарушитель может просматривать новые статьи или пресс-релизы о деятельности компании и т.п.

Типичный сценарий атаки

Стадия 2: Внутренняя разведка

Нарушитель использует более сильные методы для получения информации, но по-прежнему не делает ничего предосудительного. Он может исследовать Web-страницы серверов компании, попытаться определить используемые ими скрипты, выделив из них уязвимые, которые очень часто подвергаются хакерским атакам. Нарушитель может запустить утилиту 'ping' для того, чтобы посмотреть какие компьютеры активны в сети. Он может провести сканирование UDP/TCP-портов на намеченных для атаки компьютерах для того, чтобы определить доступные сервисы. Для определения доступных служб злоумышленник может использовать такие утилиты как 'rpcinfo', 'showmount', 'snmpwalk'. В данный момент нарушитель ведет "нормальную" деятельность в сети и в ней нет ничего, что могло быть классифицировано как нарушение. В этот момент сетевые системы обнаружения вторжений могут сообщить, что "кто-то дергает за ручки дверей".

Типичный сценарий атаки

Стадия 3: Атака

Нарушитель пересекает границу и начинает использовать возможные уязвимости на выделенных компьютерах. Для этого нарушитель может попытаться скомпрометировать ранее выявленные уязвимые скрипты. Кроме того нарушитель может попытаться использовать известные уязвимости типа "переполнения буфера". Еще одной широко распространенной формой проведения атаки является проверка учетных записей с легко подбираемыми (или пустыми) паролями. Следует отметить, что злоумышленник может пройти через несколько стадий атаки. Например, если он смог получить доступ к учетной записи обычного пользователя, то затем он будет пытаться совершать дальнейшие действия для того, чтобы получить доступ к учетной записи суперпользователя.

Типичный сценарий атаки

Стадия 4: Скрытие следов

На этой стадии злоумышленник успешно проник в сеть. Теперь его цель заключается в том, чтобы скрыть свидетельства проведения атаки путем исправления журналов регистрации. Он может инсталлировать специальные утилиты, дающие ему удаленный доступ, выполнить замену существующих сервисов своими собственными "троянскими конями", или создать свои собственные учетные записи и т.д. Системы контроля целостности могут обнаружить нарушителя именно на этом этапе, отслеживая изменения в системных файлах. Далее нарушитель будет использовать систему в качестве опорной площадки для проникновения в другие системы, поскольку большинство сетей имеет незначительное число средств для защиты от проведения внутренних атак.

Типичный сценарий атаки

Стадия 5: Получение прибыли

Нарушитель использует преимущества своего статуса для кражи конфиденциальных данных, злоупотребления полученными системными ресурсами (т.е. организует атаки в другие сайты с захваченного сервера) или осуществляет другие разрушительные воздействия.

Сценарий может начинаться и по-другому. Вместо проведения атаки на конкретный сервер, нарушитель может просто просканировать случайный адрес в сети Internet, пытаясь найти системы, обладающие определенными брешами в защите. При сканировании злоумышленник определяет используемую версию ОС, а также запущенные сетевые службы. Как правило, злоумышленники сохраняют информацию о проведенных результатах сканирования, для того, чтобы в дальнейшем воспользоваться полученной ранее информацией при появлении новой уязвимости.

Пассивные атаки

Анализ сетевого трафика

Перехват трафика может осуществляться:

- обычным «прослушиванием» сетевого интерфейса. Метод эффективен при использовании в сегменте концентраторов вместо коммутаторов, в противном случае данный метод малоэффективен, поскольку на снифер попадают лишь отдельные кадры;
- подключением снифера в разрыв канала;
- ответвлением (программным или аппаратным) трафика и направлением его копии на снифер;
- через атаку на канальном или сетевом уровне, приводящую к перенаправлению трафика жертвы или всего трафика сегмента на снифер с последующим возвращением трафика в надлежащий адрес.

Пассивные атаки

Анализ сетевого трафика

Сетевой анализ упомянутых ранее протоколов FTP и TELNET показывает, что TELNET разбивает пароль на символы и пересылает их по одному, помещая каждый символ пароля в соответствующий пакет, а FTP, напротив, пересылает пароль целиком в одном пакете.

Такая ситуация существует из-за того, что базовые прикладные протоколы семейства TCP/IP разрабатывались очень давно, в период с конца 60-х до начала 80-х годов, и с тех пор абсолютно не изменились.

На сегодняшний день подавляющее большинство пользователей продолжают работать со стандартными протоколами семейства TCP/IP, разработанными более 20 лет назад. В результате, как показывают сообщения американских центров по компьютерной безопасности (CERT, CIAC), в последние годы анализ сетевого трафика в сети Internet успешно применялся злоумышленниками, и, согласно материалам специального комитета при конгрессе США, с его помощью было перехвачено около миллиона паролей для доступа в различные информационные системы.

Пассивные атаки

Анализ сетевого трафика

Ограничить область прослушивания в сети Ethernet можно разбиением сети на сегменты с помощью коммутаторов. В этом случае злоумышленник, не прибегая к активным действиям, может перехватить только кадры, получаемые или отправляемые узлами сегмента, к которому он подключен.

Простое прослушивание также не позволяет злоумышленнику модифицировать передаваемые между двумя другими узлами данные. Для решения этих задач злоумышленник должен перейти к активным действиям, чтобы внедрить себя в тракт передачи данных в качестве промежуточного узла.

Единственным надежным способом борьбы с прослушиванием сегмента Ethernet является шифрование данных.

Пассивные атаки - AntiSniff

Методы выявления пакетных сниферов основанные на особенностях обработки операционными системами кадров Ethernet, содержащих IP-датаграммы, направленные в адрес тестируемого узла.

Некоторые ОС, находясь в режиме прослушивания, передают датаграмму уровню IP, независимо от адреса назначения кадра Ethernet (в то время как в обычном режиме кадры, не направленные на MAC-адрес узла, системой вообще не рассматриваются).

Другие системы имеют особенность при обработке кадров с широковещательным адресом: в режиме прослушивания MAC-адрес ff:00:00:00:00:00 воспринимается драйвером интерфейса как широковещательный. Таким образом, послав сообщение ICMP Echo внутри «неверного» кадра, который при нормальных обстоятельствах должен быть проигнорирован, и получив на него ответ, AntiSniff заключает, что интерфейс тестируемого узла находится в режиме прослушивания.

Вместо ICMP может использоваться любой протокол, который гарантированно генерирует ответ, кроме того для этих целей может быть использован любой протокол, который может генерировать ошибку.

Пассивные атаки - AntiSniff

Методы выявления пакетных сниферов основанные на предположении, что программа прослушивания на хосте злоумышленника выполняет обратные DNS-преобразования для IP-адресов подслушанных датаграмм.

Такая операция выполняется многими сниферами по умолчанию для упрощения анализа перехваченного трафика. AntiSniff фабрикует датаграммы с фиктивными IP-адресами, то есть не предназначенные ни одному из узлов тестируемой сети. После чего прослушивает сеть на предмет DNS-запросов о доменных именах для выданных ранее фиктивных адресов. Узлы, отправившие такие запросы, находятся в режиме прослушивания.

Пассивные атаки - AntiSniff

Метод исходящего маршрута.

Этот метод основывается на передаче информации о желательном маршруте внутри заголовка IP. Этот метод может быть использовано для детектирования снифферов в соседних сегментах.

Суть метода состоит в следующем. Создается пакет ICMP-echo на проверяемую машину, в маршруте которого указано, что он должен быть отправлен через другую машину в том же сегменте. У промежуточной машины должна быть отключена маршрутизация, следовательно, она не будет передавать пакет на целевой компьютер. Если получен ответ, то, скорее всего, целевой компьютер прослушал пакет из линии. В ответе, необходимо проверь значение поля TTL для того чтобы определить точную причину, по которой пакет вернулся (был ли он прослушан, или же просто был маршрутизирован).

Пассивные атаки - AntiSniff

Методы выявления пакетных сниферов основанные на том, что интерфейс, находящийся в обычном режиме, отфильтровывает кадры, направленные не на его адрес, с помощью программно-аппаратного обеспечения сетевой карты, и не задействует при этом ресурсы операционной системы.

В режиме прослушивания обработка всех кадров ложится на программное обеспечение злоумышленника, то есть, в конечном счете, на операционную систему. AntiSniff производит пробное тестирование узлов сети на предмет времени отклика на сообщения ICMP Echo, после чего порождает в сегменте шквал кадров, направленных на несуществующие MAC-адреса, при этом продолжая измерение времени отклика. У систем, находящихся в обычном режиме, это время растет, но незначительно, в то время как узлы, переведенные в режим прослушивания, демонстрируют многократный (до 4 раз) рост задержки отклика.

Пассивные атаки

Метод хоста (определение снифера на локальном компьютере)

Часто злоумышленники оставляют на взломанной системе специальные программы, выполняющие требуемые им функции – например прослушивание трафика. Для того, чтобы проверить, что сетевой интерфейс находится в режиме прослушивания в Unix-системах необходимо выполнить команду:

```
# ifconfig -a
lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232
        inet 127.0.0.1 netmask ff000000
hme0: flags=863<UP, BROADCAST, NOTRAILERS, RUNNING, PROMISC, MULTICAST> mtu 1500
        inet 192.0.2.99 netmask ffffff00 broadcast 192.0.2.255
        ether 8:0:20:9c:a2:98
```

Наличие флага PROMISC говорит о том, что интерфейс находится в режиме прослушивания.

Пассивные атаки

В связи с вышеизложенным отметим, что представление о прослушивании как о безопасной деятельности, которую нельзя обнаружить, не соответствует действительности.

Пассивные атаки

Сканирование сети

Сканирование сети имеет своей целью выявление активных компьютеров сети. Эта задача выполняется посылкой ICMP-сообщений Echo с помощью программы ping с последовательным перебором адресов узлов в сети. Стоит попробовать отправить Echo-сообщение по широковещательному адресу — на него ответят все компьютеры, поддерживающие обработку таких сообщений. Стоит отметить, что далеко не все сетевые ОС ведут себя подобным образом.

Для исследования топологии сети и обнаружения маршрутизаторов нарушитель может воспользоваться утилитами подобными traceroute.

Также злоумышленник может применить «обратное сканирование»: в этом случае на тестируемые адреса посылаются не сообщения ICMP Echo, а другие сообщения, например RST-сегменты TCP, ответы на несуществующие DNS-запросы и т. п. Если тестируемый узел не существует (выключен), злоумышленник получит в ответ ICMP-сообщение Destination Unreachable: Host Unreachable. Следовательно, если сообщение не было получено, то соответствующий узел подключен к сети и работает.

Пассивные атаки

Методы сканирования портов

Сканированием портов называется метод удаленного анализа, осуществляемый путем передачи тестовых запросов на создание соединения и позволяющий определить список активных служб предоставления удаленного сервиса на каком-либо хосте.

Сканирование портов (или разведка) применяется на подготовительной стадии перед атакой, так как позволяет получить необходимые начальные сведения о потенциальном объекте воздействия: список открытых портов, а следовательно, и перечень потенциально атакуемых серверных приложений, запущенных на компьютере.

Поскольку номера портов всех основных сервисов Internet стандартизованы, то, определив, например, что порт 25/TCP открыт, можно сделать вывод о том, что данный хост является сервером электронной почты, и т. п. Полученную информацию злоумышленник может использовать для дальнейшего проведения атаки на уровне приложения.

Пассивные атаки

Методы сканирования портов

На первом этапе клиенту необходимо создать обычное TCP-соединение с указанным TCP-портом сервера. Для этого клиент передает на сервер TCP SYN-запрос на необходимый порт.

Если клиент получает ответ на этот запрос (TCP | SYN | ACK), то порт открыт и TCP-соединение будет создано. Если же ответ за определенный промежуток времени так и не пришел, то это означает, что либо порт закрыт и соответствующий сервер не запущен, либо имеют место физические проблемы со связью с данным IP-адресом.

Необходимо обратить внимание на то, что первый этап (создание TCP-соединения с указанным портом) является стандартным и абсолютно инвариантным относительно вида серверного приложения, к которому осуществляется подключение. На этой особенности и основаны все методы сетевого сканирования TCP-портов.

Пассивные атаки

Методы сканирования портов

Все известные на сегодняшний день основные методы сканирования портов в зависимости от возможности определения непосредственного инициатора сканирования (хоста, откуда осуществлялся удаленный анализ) можно разделить на две группы:

1. Методы открытого сканирования: непосредственный инициатор однозначно определяется объектом сканирования по IP-адресу приходящих запросов.
2. Методы "невидимого" анонимного сканирования. Непосредственный инициатор не определяется объектом сканирования (однозначно определяется только "промежуточный" источник сканирующих запросов), таким образом, гарантируется анонимность инициатора сканирования.

Методы открытого сканирования

Сканирование TCP Connect

Наиболее простой способ сканирования состоит в установлении TCP-соединения с тестируемым портом с помощью функции connect. Если соединение удалось установить, то значит, что порт открыт и соответствующее серверное приложение доступно.

Достоинством этого методы является возможность выполнения сканирования любым пользователем, даже без применения специального программного обеспечения: стандартная программа telnet позволяет указать произвольный номер порта для установления соединения.

Существенный недостаток — возможность отслеживания и регистрации такого сканирования: при анализе системного журнала сканируемого хоста будут обнаружены многочисленные открытые и сразу же прерванные соединения, в результате чего могут быть приняты меры по повышению уровня безопасности.

Методы открытого сканирования

Сканирование TCP FIN

В этом методе на сканируемый порт посылается сегмент с установленным битом FIN. Хост должен ответить RST-сегментом, если FIN-сегмент адресован закрытому порту. FIN-сегменты, направленные на порт, находящийся в состоянии LISTEN, многими реализациями TCP/IP игнорируются. Стандарт требует в состоянии LISTEN посылать RST-сегменты в ответ на сегменты, имеющие неприемлемый ACK SN, про сегменты, имеющие только флаг FIN, ничего не говорится. Таким образом, отсутствие отклика говорит о том, что порт открыт.

Варианты этого метода сканирования состоит в посылке сегментов с установленными флагами FIN, PSH, URG («Xmas scan») или вообще без всяких флагов («Null scan»). Подчеркнем, что сетевые ОС фирмы Microsoft таким методом просканировать не удастся, так как в их реализации передача пакета TCP RST в ответ на подобный запрос не предусмотрена.

Методы открытого сканирования

Сканирование с использованием IP-фрагментации

Сканирование с использованием IP-фрагментации не является само по себе новым видом сканирования. Вместо этого данный метод предназначен для усложнения задачи обнаружения факта сканирования. Данный метод может применяться совместно с упомянутыми ранее методами. Суть его состоит в разбиении TCP SYN- или TCP FIN-запроса на несколько маленьких IP-фрагментов (минимальный размер поля данных в IP-фрагменте 8 байт, следовательно, TCP SYN-запрос, имеющий минимальный размер 20 байт, можно разбить на три фрагмента). Первый фрагмент не содержит флагов, на основании, которых данные пакеты могут быть заблокированы. Тем не менее, если межсетевой экран выполняет дефрагментацию пакетов, то данный метод является неэффективным.

Методы открытого сканирования

UDP сканирование

Сканирование UDP-сервисов представляет собой достаточно сложную процедуру. Это связано с тем, что протокол UDP является протоколом без установления соединения, а, следовательно, отсутствуют предварительные шаги по созданию виртуального канала.

Для выполнения сканирования UDP-портов можно воспользоваться тем фактом, что большинство хостов в ответ на получение пакет, направленного на закрытый UDP-порт отвечают ICMP пакетом ICMP_PORT_UNREACH. Таким образом, можно обнаружить закрытые порты. Исключив закрытые порты можно получить список открытых портов. Данный вид сканирования является медленным, так как в соответствии с RFC 1812 хост может значительно ограничить количество ответов содержащих ICMP-сообщения об ошибках.

Методы "невидимого" удаленного сканирования

Скрытая атака по FTP

Первым методом анонимного сканирования является метод, получивший название FTP Bounce Attack (скрытая атака по FTP). Протокол FTP (RFC 959) имеет ряд чрезвычайно интересных функций, одна из которых - возможность создания так называемых "proxy" FTP-соединений с FTP-сервера. Если реализация FTP-сервера поддерживает режим proxy, то любой пользователь (и анонимный в том числе) может, подключившись к серверу, создать процесс DTP-server (Data Transfer Process - процесс передачи данных) для передачи файла с этого FTP-сервера на любой другой сервер в Internet.

Эта особенность протокола FTP позволяет предложить метод TCP-сканирования с использованием proxy ftp-сервера, состоящий в следующем: ftp-серверу после подключения выдается команда PORT с параметрами IP-адреса и TCP-порта объекта сканирования. Далее следует выполнить команду LIST, по которой FTP-сервер попытается прочитать текущий каталог на объекте, посылая на указанный в команде PORT порт назначения TCP SYN-запрос. Если порт на объекте открыт, то на сервер приходит ответ TCP | SYN | ACK и FTP-клиент получает ответы "150" и "226", если же порт закрыт, то ответ будет таким:

425. Can't Build Data Connection: Connection Refused

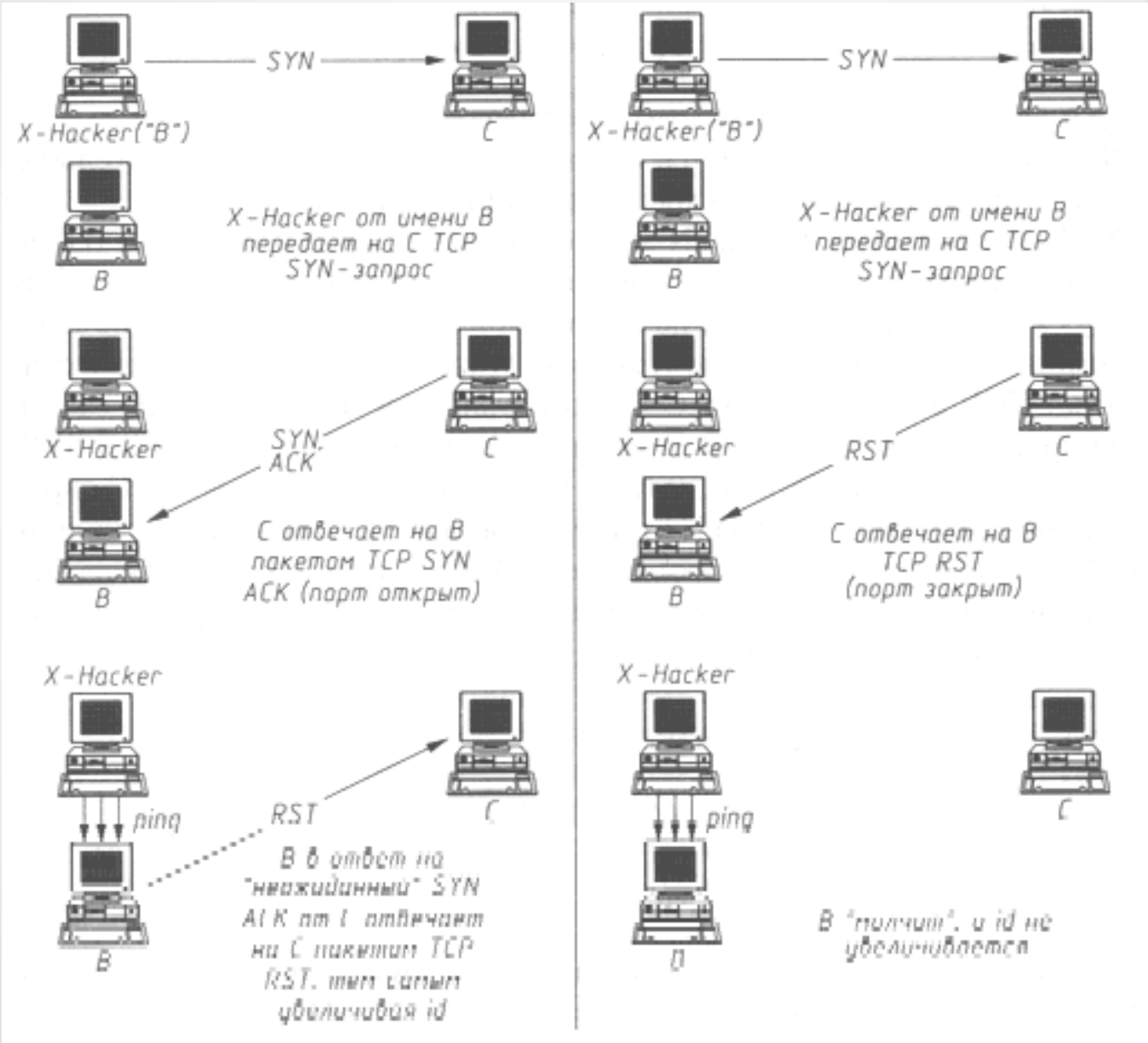
Методы "невидимого" удаленного сканирования

Сканирование с использованием "немого" хоста

Сальвадор Сапфилинпо (Salvatore Sanfilippo) из Intesis Security Lab впервые заявил об этом методе 18 декабря 1998 года в конференции BUGTRAQ. Оригинальное название метода Dumb host scan переводится как "сканирование с использованием "немого" хоста". Основные положения, лежащие в основе метода, состоят в следующем:

- с каждым переданным пакетом значение ID в заголовке IP-пакета обычно увеличивается на 1;
- хост отвечает на TCP SYN запрос TCP | SYN | ACK, если порт открыт; и TCP RST, если порт закрыт;
- существует возможность узнать количество пакетов, переданных хостом, но параметру ID в заголовке IP;
- хост отвечает TCP RST на TCP SYN | ACK и ничего не отвечает на TCP RST.

Сканирование с использованием "немого" хоста



Методы "невидимого" удаленного сканирования

Сканирование с использованием "немого" хоста

Хост X-Hacker при помощи, например, утилиты hping определяет число исходящих от хоста B пакетов по ID из заголовка IP, имеющего вид:

#hping B -r

HPING B (eth0 194.94.94.94): no flags are set, 40 data bytes

60 bytes from 194.94.94.94: flags=RA seq=0 ttl=64 id=41660 win=0 time=1.2 ms

60 bytes from 194.94.94.94: flags=RA seq=1 ttl=64 id=+1 win=0 time=75 ms

60 bytes from 194.94.94.94: flags=RA seq=2 ttl=64 id=+1 win=0 time=91 ms

60 bytes from 194.94.94.94: flags=RA seq=3 ttl=64 id=+1 win=0 time=90 ms

60 bytes from 194.94.94.94: flags=RA seq=4 ttl=64 id=+1 win=0 time=91 ms

60 bytes from 194.94.94.94: flags=RA seq=5 ttl=64 id=+1 win=0 time=87 ms

Методы "невидимого" удаленного сканирования

Сканирование через proxy-сервер

Первый состоит в использовании анонимных Free Telnet Account сервров (серверов со свободным Telnet-доступом), которых в Internet довольно много. При помощи telnet можно, подключившись к данному хосту, от его имени вести сканирование любого хоста в Internet. Для этого создается небольшой скрипт, который, последовательно изменяя порт назначения, будет выдавать следующую команду: telnet Scan_Host_Name Target_TCP_Port.

Если порт закрыт, telnet вернет сообщение Connection Refused (В соединении отказано) или не вернет ничего. Если же порт открыт, появится приглашение соответствующей службы.

Второй способ заключается в использовании proxy-серверов. В Internet можно найти немало proxy-серверов, администраторы которых разрешают анонимное подключение к ним с любых IP-адресов. Это приводит к тому, что нарушитель получает промежуточный хост, от имени которого, используя различные прикладные службы (telnet, ftp и т. д.), он может вести работу с любыми объектами в Internet, сохраняя при этом полную анонимность.

Методы удаленного определения версии ОС

1. Классические методы

(telnet, ftp,…)

2. Особенности ОС по обработке ошибок.

Как показывает практика, различные ОС при работе в сети по-разному реагируют на один и тот же запрос. Более того многие реализации ОС отходят от спецификаций из стандартов, что может привести к парадоксу. Некоторые ОС могут быть выявлены благодаря тому, что они более полно и точно реализуют требования RFC. Исследовав особенности реакций на запрос ОС, версии которых заранее известны, можно набрать определенную статистику, сопоставив реакции на запрос с типом ОС.

(Методы опроса стека TCP/IP удаленного хоста)

Методы удаленного определения версии ОС

Определение закона изменения ISN сервера

Хост посылает на сервер SYN-пакет с запросом на соединение, записав в пакет свое (известное) значение ISN. Сервер, получив запрос на соединение, прибавляет к полученному ISN единицу и записывает полученное значение в поле ACK ответа (т.е. SYN ACK-пакета), а в поле ISS ответа - свой собственный ISN, и передает пакет устанавливающему соединение хосту. На приемной стороне (т.е. на стороне хоста) пакет анализируется. Операция повторяется до тех пор, пока не будет выявлен закон изменения ISN сервера:

- закон "постоянного приращения" (традиционный закон "+64" - старые версии UNIX): значение ISN сервера, записываемого в поле ISS ответа на запрос "установление соединения", увеличивается на постоянную величину (либо на 64) с каждым обрабатываемым запросом;
- закон "случайных приращений" (новые версии Solaris, IRIX, FreeBSD, DigitalUNIX, Cray) --- приращение ISN носит случайный характер;
- истинно случайные значения (Linux 2.0.x, OpenVMS, новые AIX): значение ISN является случайной величиной;
- закон "время-зависимых приращений" (Windows): значение ISN периодически во времени увеличивается на некоторую небольшую величину;
- постоянный (концентраторы 3Com [ISN=0x803], принтеры Apple LaserWriter [0xC7001]): значение ISN остается постоянным.