Nmap - сканер портов

Опубликовано muff в Сб, 2009-11-28 15:19

Иногда нужно "прослушать", какие порты открыты на том или ином ресурсе. Изобретать велосипед не нужно, есть готовое решение - nmap. Для начала немного общей информации в ознакомительных целях...

Nmap (“Network Mapper”) это утилита с открытым исходным кодом для исследования сети и проверки безопасности. Она была разработана для быстрого сканирования больших сетей, хотя прекрасно справляется и с единичными целями. Nmap использует IP-пакеты оригинальными способами, чтобы определить какие хосты доступны в сети, какие службы (название приложения и версию) они предлагают, какие операционные системы (и версии ОС) они используют, какие типы пакетных фильтров/брандмауэров используются и еще дюжины других характеристик. В тот время как Nmap обычно используется для проверки безопасности, многие сетевые и системные администраторы находят ее полезной для обычных задач, таких как контролирование структуры сети, управление расписаниями запуска служб и учет времени работы хоста или службы.

Выходные данные Nmap это список просканированных целей с дополнительной информацией по каждой в зависимости от заданных опций. Ключевой информацией является “таблица важных портов”. Эта таблица содержит номер порта, протокол, имя службы и состояние. Состояние может иметь значение open (открыт), filtered (фильтруется), closed (закрыт) или unfiltered (не фильтруется). Открыт означает, что приложение на целевой машине готово для установки соединения/принятия пакетов на этот порт. Фильтруется означает, что брандмауэр, сетевой фильт или какая-то другая помеха в сети блокирует порт, и Nmap не может установить открыт этот порт или закрыт. Закрытые порты не связаны ни с каким приложение, так что они могут быть открыты в любой момент. Порты расцениваются как не фильтрованные, когда они отвечают на запросы Nmap, но Nmap не может определить открыты они или закрыты. Nmap выдает комбинации открыт|фильтруется и закрыт|фильтруется, когда не может определить, какое из этих двух состояний описывает порт. Эта таблица также может предоставлять детали о версии программного обеспечения, если это было запрошено. Когда осуществляется сканирование по IP протоколу (-sO), Nmap предоставляет информацию о поддерживаемых IP протоколах, а не об открытых портах.

В дополнение к таблице важных портов Nmap может предоставлять дальнейшую информацию о целях: преобразованные DNS имена, предположение о используемой операционной системе, типы устройств и MAC адреса.

Заинтересовало? Тогда приступим к установке.

Nmap есть в портах. Оттуда и будем устанавливать.

```
# cd /usr/ports/security/nmap && make install clean
```

О возможностях nmap можно узнать ознакомившись с руководством пользователя [1].

Рассмотрим несколько примеров использования nmap.

TCP-Сканирование.

Методом TCP connect () nmap будет сканировать диапазон портов (1-65535) компьютера с IP-адресом 172.16.0.1. Опция -sV служит для получения версий запущенных сервисов.

```
# nmap -sV 172.16.0.15 -p 1-65535
Starting Nmap 5.00 ( http://nmap.org [2] ) at 2009-11-30 03:28 EET
Interesting ports on 172.16.0.15:
Not shown: 65531 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.1p1 (FreeBSD 20080901; protocol 2.0)
53/tcp   open  domain  ISC BIND 4.X
80/tcp   open  http    Apache httpd 2.2.13 ((FreeBSD) mod_ssl/2.2.13 OpenSSL/0.9.8e DAV/2
PHP/5.2.11 with Suhosin-Patch mod_perl/2.0.4 Perl/v5.8.9)
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:14:5E:22:11:2A (IBM)
Service Info: OS: FreeBSD

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ [3] .
Nmap done: 1 IP address (1 host up) scanned in 20983.73 seconds
```

Стоит обратить внимание на то, что в поле SERVICE всегда отображается значение из файла /etc/services, соответствующее номеру порта. Это отнюдь не означает, что по данному порту будет запущен тот сервис, который указан в поле SERVICE. Можно запустить Web-сервер по 22 порту, а сервер SSH - по 80, но nmap все будет писать, что 22 порт - это ssh, а 80 - это HTTP. Теперь просканируем брандмауэр/маршрутизатор на базе Linux. Вначале просканируем маршрутизатор с внутреннего узла сети, а после - с удаленного узла, который находится вне нашей сети (например, в Интернете или другой локальной сети):

```
# nmap 172.16.0.254 -p 1-65535
Starting Nmap 4.00 ( http://www.insecure.org/nmap/ [4] )

Interesting ports on 172.16.0.254:

(The 65529 ports scanned but not shown below are in state: closed)

PORT STATE SERVICE

22/tcp open ssh

8080/tcp open http-proxy

10000/tcp open snet-sensor-mgmt

Nmap finished: 1 IP address (1 host up) scanned in 42.636 seconds
```

```
# nmap -p 1-65535 example.com
Starting Nmap 4.00 ( http://www.insecure.org/nmap/ [4] )

Interesting ports on example.com (172.20.1.100):

(The 65529 ports scanned but not shown below are in state: closed)
```

```
PORT STATE SERVICE

22/tcp filtered ssh

8080/tcp filtered http-proxy

Nmap finished: 1 IP address (1 host up) scanned in 47.537 seconds
```

В одном случае порт ssh открыт (open), другом - отфильтрован (filtered). Значение Filtered значит, что порт отклоняет (reject) или отбрасывает (drop) трафик. Это не говорит о том, запущен ли на этом порту сервис или нет.

UDP-сканирование.

UDP-порты надо обязательно сканировать. При поиске уязвимостей UDP-сервисы обычно упускают из виду. Мол, там ничего нет интересного. Так делать нельзя. Многие UDP-сервисы (echo, chargen, DNS - работает как по TCP, так и по UDP, а также RPC (Remote Procedure Call)) работают по протоколу UDP. Некоторые из них известны своим огромным списком эксплоитов, позволяющим получить права root'а. UDP-сканирование делается с помощью опции -sU сканера nmap:

```
# nmap -sU 172.16.0.1 -p 1-65535
Starting Nmap 4.00 ( http://www.insecure.org/nmap/ [4] )

All 65535 ports on 172.16.0.1 are: closed

Nmap run completed - 1 IP address (1 host up) scanned in 85599:56 seconds
```

Время сканирования очень большое примерно 1 секунда на порт. Отчего так долго? Система ограничила отправку ICMP-ответов: не более 1 в секунду. При UDP-сканировании нужно использовать опцию -T. Она позволяет указать агрессивность сканирования. Есть 6 скоростей сканирования: Paranoid, Sneaky, Polite, Normal, Aggressive и Insane (-T Polite). Первая скорость самая медленная, последняя - самая быстрая.

PING-сканирование.

Последующий режим nmap - это Ping-сканирование, которое обыкновенно используется для того, чтобы определить, «жив» ли узел или нет. Если узел включен и подключен к сети (не 220!), значит, он «жив».

Многие узлы игнорируют ICMP-запросы echo, поэтому nmap отправляет ACK-пакеты на порт 80 (по умолчанию). Если в ответ получен RST-пакет, то жертва "жива". С помощью tcpdump можно увидеть, как nmap комбинирует методы - первым идет обычный "пинг", а после этого он отправляет пакеты на порт 80 (http).

Данный метод не совершенен. ICMP-запросы echo игнорируются многими узлами. Еще и 80-й порт нередко закрывают брандмауэром, поскольку посылается ACK-пакет без предварительной установки соединения. Чтобы "обойти" stateful-брандмауэр, нужно использовать для пинга SYN-пакеты:

```
# nmap -sP -PS 172.16.0.1
```

Также можно изменить порт (указать другой порт, не 80):

```
# nmap -sP -PS22 172.16.0.1
```

Эта команда указывает nmap использовать порт 22/tcp(ssh) вместо 80. Если не знаете, какие порты открыты, а какие - нет, то нужно использовать стандартные порты 21, 22, 25 и 53.

Ping-сканирование хорошо подходит, когда есть список машин сети и нужно узнать, в какое время к сети подключаются некоторые машины, а когда - отключаются от нее. Его можно использовать для обнаружения новых машин в сети. Для ping-сканирования диапазона IP-адресов обязательно используйте при указании IP-адреса звездочку (*). Когда нужно просканировать диапазон 172.16.0.0-172.16.0.255, надо использовать следующую команду:

```
# nmap -sP 172.16.0.*
Starting Nmap 4.00 ( http://www.insecure.org/nmap/ [4] )

Host 172.16.0.1 appears to be up.

Host 172.16.0.3 appears to be up.

Host 172.16.0.255 seems to be a subnet broadcast address (returned 1 extra pings).

Nmap finished: 256 IP addresses (2 hosts up) scanned in 2.767 seconds
```

Обзор основных возможностей на этом закончу. Думаю интересно будет, также, ознакомиться со следующими материалами:

Система определения версий служб в сетевом сканере Nmap [5]

Обход Брандмауэров/IDS [6]

Источник (получено *2025-03-14 00:24*): http://muff.kiev.ua/content/nmap-skaner-portov

Ссылки:
[1] http://muff.kiev.ua/node/69
[2] http://nmap.org/
[3] http://nmap.org/submit/
[4] http://www.insecure.org/nmap/
[5] http://www.cherepovets-city.ru/insecure/runmap/runmap-versionscan.htm
[6] http://nmap.org/man/ru/man-bypass-firewalls-ids.html