NMAP

Open source приложение для сканирования сети.

Общие флаги

nmap -e eth2 scanme.nmap.org	Конкретный интерфейс
nmap -A <target>	Агрессивный режим (объединение режимов определения версии ОС, версий сервисов, скрипт сканирования, трассировки)
-n	отключить обратное разрешение IP в DNS
--data-length <length>	Добавка случайных байтов информации к каждому пакету

nmap -iL targets.txt	Запуск с источниками из файла.
	Могут разделяться пробелом, табуляцией или переводом строки. Поддерживает диапазоны
	192.168.1.20-30
	192.168.*
	192.168.0/24
	scanme.nmap.org/24
	комментарии
	`cat targets.txt`
	`# FTP servers`
	`192.168.10.3`

nmap 192.168.1.1-255 --exclude 192.168.1.1	Исключение из диапазона
nmap --exclude-file dontscan.txt 192.168.1.1/24	Исключение адресов из файла
--randomize-hosts	перемешивание последовательности узлов
nmap -iR 100	100 случайных адресов -iR 0 это все адреса.
http-max-cache-size=0	Отключение кэша (по умолчанию включен)
-sL	имя сетевого узла

Таймауты

--max-rtt-timeout	Максимальное время ожидания ответа. По умолчанию несколько секунд. `sudo nmap -sU --max-rtt-timeout 100ms host.ru`
--host-timeout	Ограничение времени сканирования всего хоста. `sudo nmap -sU --host-timeout 5m host.ru`
--max-retries	Максимальное количество повторных попыток. `sudo nmap -sU --max-rtt-timeout 100ms --max-retries 0 host.ru`
-T4	Время задержки (ожидания) между запросами, 0 - очень много, 3 - по умолчанию, 5 - очень быстро

Поиск хостов

NMAP использует несколько техник пинга с использованием разных протоколов.

-PS/PA/PU/PY [portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO [protocol list]: IP protocol ping

Номера протоколов поверх IP

1	ICMP
2	IGMP
4	IP-in-IP
6	TCP
17	UDP
132	SCTP

Для остальных протоколов только будут установлены IP заголовки.

Все техники по умолчанию отправляют пустые запросы.

Ключ	Описание

-sn <target>	Ping-сканирование сети.
	`nmap -sn 192.168.1.0/24`
	`Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 09:02 +08`
	`Nmap scan report for 192.168.1.1`
	`Host is up (0.00044s latency).`
	`MAC Address: 00:18:E7:F3:65:EE (Cameo Communications)`
	
	Отправляются разные пакеты в зависимости от привилегий пользователя.
	С опцией traceroute должен показывать дополнительные маршруты, но это не то же самое что traceroute. У меня до всех тестовых адресов получился один шаг
	`nmap -sn --traceroute microsoft.com`
	
	`Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 11:03 +08`
	`Nmap scan report for microsoft.com (13.107.246.77)`
	`Host is up (0.00055s latency).`
	`Other addresses for microsoft.com (not scanned):`
	`2603:1020:201:10::10f 2603:1010:3:3::5b 2603:1030:b:3::152 2603:1030:20e:3::23c 2603:1030:c02:8::14`
	
	`TRACEROUTE (using port 80/tcp)`
	`HOP RTT     ADDRESS`
	`1   0.53 ms 13.107.246.77`
	
	`Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds`

nmap -sn -PS <target>	TCP SYN сканирование.
	`nmap -sn -PS 192.1.1/24`
	SYN пакет на 80 порт, если порт закрыт - приходит RST, если открыт - SYN/ACK. Потом отправляем RST пакет.
	Фаер может блокировать RST для закрытых сервисов, поэтому можно донастроить скан
	`nmap -sn -PS80,100-1000 <target>`
	Но SYN пакеты могут блокироваться, поэтому следующий способ

nmap -sn -PA <target>	TCP ACK сканирование. Пустой TCP-пакет с флагом ACK, на порт 80 (по умолчанию). Если хост отключен, он не должен отвечать на этот запрос. Иначе RST и будет считаться подключенным к сети. `nmap -sn -PA22,1000-65535 <target>`
nmap -sn -PU <target>	UDP сканирование. Порт 40125. Аналогично настройка портов
nmap -sn -PE <target>	Стандартное Echo сканирование.
nmap -sn -PP <target>	Echo timestamp сканирование.
nmap -sn -PM <target>	Echo reply сканирование.
nmap -sn -PY <target>	SCTP INIT сканирование. Аналогичная настройка портов.
nmap -sn -PO <target>	IP сканирование. `nmap -sn -PO1,2,17 scanme.nmap.org` Здесь 1, 2, 17 - номера протоколов
nmap -sn -PO --data-length 100 scanme.nmap.org	--data-length 100 генерация случайных данных
nmap -sn -PR <target>	ARP ping

nmap -sn -PR --spoof-mac <mac address> <target>	Подмена MAC-адреса может позволить нам подделать источник наших подключений и может быть полезна для обхода систем идентификации. MAC-адрес можно подделать во время проверки ARP-связи. Используйте --spoof-mac для установки нового MAC-адреса:
-sn --script dns-brute bobrobotirk.ru	Брутфорс по доменным именам
-sW	Похож на ACK, определяет статус порта анализируя поле TCP Window в RST ответе. Открытые больше 0, закрытые - 0.

-sI	Сканирование от лица другого узла. Старые системы увеличивают IP-ID на 1 с каждым новым исходящим пакетом. Это ключевая уязвимость.
	Хост должен мало использоваться и иметь предсказуемый IP-ID.
	Процесс сканирования одного порта:
	• Запрос "зомби" (например, SYN-пакет), сохраняется IP-ID ответа (например X)
	• Отправка пакета от имени "зомби" на целевой порт сканируемой машины. Если порт открыт, цель ответит "зомби" пакетом SYN/ACK. Если порт закрыт, цель ответит "зомби" пакетом RST.
	• Повторный запрос "зомби" и анализ нового значения IP-ID. X+1 означает, что "зомби" не отправил ни одного своего пакета. Следовательно, порт на цели фильтруется (брандмауэр молча отбросил пакет). X+2 означает, что "зомби" получил от цели ответный пакет и ответил на него своим RST. Вывод: порт на цели открыт или закрыт.
	
	Чтобы отличить открытый порт от закрытого, сканер анализирует, на какой именно пакет отреагировал "зомби".
	
	Причины использования: анонимность и обход правил фильтрации (если "зомби" доверенный)
	`sudo nmap -sI zombie.example.com target.example.com`
	
	Поиск зомби:
	Скрипт ipidseq.
	`sudo nmap -sS -p 80 --script ipidseq <target>`
	
	По умолчанию 6 пакетов. Параметр --script-args ipidseq.probes=10 улучшает качество проверки.
	Результат:
	• Incremental! Подходит. IP-ID увеличивается на постоянную величину.
	• All zeros или Constant Не подходит. В поле IP-ID всегда ноль/константа. В некоторых старых системах или специфичном сетевом оборудовании.
	• Random Не подходит.
	• Broken incremental! Увеличивается на непостоянную величину (например, +1, +2, +1, +3). Не подходит./подождать, может успокоится.
	
	Проверил роутеры DIR-650 и ASUS RT-N18U. На первом Incremental, на втором - All zeros. Пакеты, идущие сквозь, не влияют. При сканировании на целевом хосте в качестве порта источника видится http или https порт зомби.

-sn --script broadcast-ping 192.168.0.1/24	Броадкастовый пинг. Отправляется броадкастовый запрос и ждем результат. broadcast-ping.num_probes=5 количество пингов `nmap --script broadcast-ping --script-args broadcast-ping.num_probes=5` broadcast-ping.timeout=10000 таймаут broadcast-ping.interface=wlan3 интерфейс --script-args=newtargets позволяет просканировать хосты, от которых получен ответ --script-args max-newtargets=3 ограничивает кол-во сканируемых хостов
nmap --script broadcast	Запускает все скрипты категории broadcast

Можно комбинировать технологии

```
nmap -sn --send-ip -PS21,22,23,25,80,445,443,3389,8080 -PA80,443,8080 -PO1,2,4,6 -PU631,16
```

Эффективность технологий сканирования (оригинал)

Интересная статья. Проба эффективности различных комбинаций технологий на основании 1000 случайных сетей. Был сформирован список и приведены результаты различных технологий и комбинаций с процентом результативности. 100% результат - найденные любой технологией хосты. А затем - поиск комбинации технологий с наибольшим процентом попадания и времени на каждую вариацию.

Вывод, который я для себя сделал на основе данных:

- Стартовый поиск адресов и портов важная процедура. Однако только один из компонентов.
- Психология и поставленные задачи критичны. Направленные и ненаправленные взломы происходят по разным алгоритмам.
- Ненаправленные взломы были, есть и будут. Оно дает шум в логах, за которым может прятаться направленный хакер.
- Время жизни важно. Сервис "на месяц" отличается от "на год".
- Одна технология дает в лучшем случае 50-60% результат. Однако непопулярные технологии могут показать защищенные от явного сканирования хосты, хотя не справиться с простыми. Поэтому либо тьма времени + высокая вероятность обнаружения, либо результат в 70-80 процентов.
- Эти данные масштабного сканирования. Эффективность от затраченного времени растет нелинейно. В районе 90% каждый дополнительный процент стоит дней.
- В случае направленного теста каждый фактор, предоставляющий дополнительную информацию (например ОС, возможные сервисы, ожидаемая степень защиты) увеличивает шансы и скорость. Возможно, нужен некий справочник/сервис, агрегирующий данные по удачным вариантам в зависимости от дополнительных условий.

- Нестандартные порты рулят, но их нужно правильно прятать. Это ограничивает ненаправленных хакеров.
- Логирование + проактивная защита как минимум поможет увидеть попытки. Однако необходим баланс между стоимостью защиты (фильтрации) и ценностью информации
- Тупое сканирование будет незаметно только в системах с отсутствием защиты.
- Данные 2009 года, сейчас рулят облака и ситуация думаю слегка поменялась.
- Возможно общедоступные сервисы стоит выносить в отдельный пул

Открытые порты

Без параметров, только адрес. По умолчанию сканирует 1024 первых порта. Статусы портов:

Open	Сервис доступен
Closed	Запросы были получены, но был сделан вывод, что на этом порту не запущена служба.
Filtered	Не было признаков того, что запросы были получены, и состояние не удалось установить. Это также указывает на то, что запросы отбрасываются в результате какой-либо фильтрации.
Unfiltered	Запросы были получены, но состояние не удалось установить. Это состояние возможно только при ACK сканировании.
Open/Filtered	Запросы отфильтрованы или порт открыт, но не удалось установить состояние.
Close/Filtered	Запросы отфильтрованы или порт закрыт, и не удалось установить состояние.

Последовательность задач при сканировании портов:

- Преобразование DNS имени в IP. Можно указать альтернативный dns сервер.

```
nmap --dns-servers 8.8.8.8,8.8.4.4 scanme.nmap.org
```

- Проверка, поднят ли хост. Чтобы пропустить:

```
nmap -Pn scanme.nmap.org
```

- Обратное преобразование IP в DNS. Чтобы пропустить:

```
nmap -n scanme.nmap.org
```

- Затем SYN (привилегированный пользователь) или TCP connect (обычный пользователь) сканирование. SYN быстрее. Однако есть еще способы сканирования портов.

Диапазоны портов:

--top-ports N	Заданное количество портов по рейтингу популярности.
nmap -p80,443 localhost	Явный список портов
nmap -p1-100 localhost	Диапазон
nmap -p- localhost	Все порты
nmap -pT:25,U:53 <target>	Порты с протоколом
nmap -p smtp <target>	По имени сервиса
nmap -p smtp* <target>	По шаблону имени сервиса
nmap -p[1-65535] <target>	Только порты, указанные в nmap в виде сервиса

Определение типа сервиса и версии

За счет базы данных "отпечатков" сервисов и ОС. Отправляются пробники, определенные в nmap-service-probes, в список предполагаемых открытых портов. Пробники выбираются в зависимости от того, насколько вероятно, что они могут быть использованы для идентификации службы.

nmap -sV <target>	Версии сервисов
nmap -sV --version-intensity 9 <target>	Уровень интенсивности поиска, 0-9
nmap -O <target>	Версия ОС. В привилегированном режиме.
nmap -O --osscan-guess <target>	Попытка угадать ОС
nmap -O --osscan-limit <target>	Вывод информации об ОС только а случае абсолютной уверенности
nmap -O -v 192.168.0.1	Расширенная информация об ОС

"Отпечатки" могут настраиваться для улучшения производительности.

Дополнительные утилиты

nping модификация ping пакетов. Мощный инструмент для тестирования фаерволов.

--icmp	тип пакета
-c 1	количество пакетов
--icmp-type 0 --icmp-code 0	тип и код пакета
--source-ip 192.168.0.5 --dest-ip 192.168.0.10	источник и приемник
--icmp-id 520	идентификатор
--icmp-seq 0	номер пакета

--data-string 'ping'	данные внутри

Zenmap графическая утилита, удобно хранить настройки параметров nmap

ncat Выполнение внешних команд различными способами после успешного установления соединения. Одним из способов является использование Lua-скриптов, которые действуют как программы и позволяют пользователям выполнять любые задачи.

```
ncat --lua-exec <path to Lua script> --listen 80
```

--sh-exec выполняет консольные команды

Ncrack взлом простых паролей

<[service-name]>://<target>:<[port-number]>

ncrack ssh://<target>:<port>

-U	файлы логинов
-P	файлы паролей
ncrack --save cracking-session <[service-name]>://<target>:<[port-number]>	сохранить незавершенный процесс
ncrack --resume cracking-session <[service-name]>://<target>:<[port-number]>	продолжить

Rainmap Lite запуск сканирования из браузера

Revision #15
Created 7 September 2025 14:46:52 by Admin
Updated 18 September 2025 16:06:12 by Admin