Оглавление

Название

nmap — Утилита для исследования сети и сканер портов

Синтаксис

`nmap` [*<Тип сканирования>* ...] [*<Опции>*] { *<цель сканирования>* }

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 "сырые" IP пакеты оригинальным способом, 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 множество других характеристик. В то время, как Nmap обычно используется для проверки безопасности, многие 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 из них 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 фильтр, 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 приложением, но 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 протоколах, а не об открытых портах.

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

Типичное сканирование с использованием Nmap показано в Пример 1. Единственные аргументы, использованные в этом примере - это `-A`, для определения версии ОС, сканирования с использованием скриптов и трассировки; `-T4` для более быстрого выполнения; затем два целевых хоста.

Пример 1. Типичный пример сканирования с помощью Nmap

```
# nmap -A -T4 scanme.nmap.org playground

Starting Nmap ( https://nmap.org )
Interesting ports on scanme.nmap.org (64.13.134.52):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11

Interesting ports on playground.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
389/tcp  open  ldap?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
1002/tcp open  windows-icfw?
1025/tcp open  msrpc         Microsoft Windows RPC
1720/tcp open  H.323/Q.931   CompTek AquaGateKeeper
5800/tcp open  vnc-http      RealVNC 4.0 (Resolution 400x250; VNC port: 5900)
5900/tcp open  vnc           VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```

Сводка опций

Эта сводка опций выводится на экран, когда Nmap запускается без каких-либо опций; последняя версия всегда доступна здесь `https://nmap.org/data/nmap.usage.txt`. Эта сводка помогает людям запомнить наиболее употребляемые опции, но она не может быть заменой документации, предоставленной в данном руководстве. Некоторые опции не включены в этот список.

```
Nmap 4.76 ( https://nmap.org )
Использование: nmap [Тип(ы) Сканирования] [Опции] {цель сканирования}
```

```
ОПРЕДЕЛЕНИЕ ЦЕЛИ СКАНИРОВАНИЯ:
  Можно использовать сетевые имена, IP адреса, сети и т.д.
  Пример: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0
-255.1-254
  -
iL <имя_входного_файла>: Использовать список хостов/сетей из фай
ла
  -iR <количество_хостов>: Выбрать произвольные цели
  --exclude <хост1[,хост2][,хост3],...>: Исключить хосты/сети
  --
excludefile <имя_файла>: Исключить из сканирования список хостов
/сетей, находящийся в файле
ОБНАРУЖЕНИЕ ХОСТОВ:
  -
sL: Сканирование с целью составления списка - просто составить с
писок целей для сканирования
  -sP: Пинг сканирование - просто определить, работает ли хост
  -
PN: Расценивать все хосты как работающие - пропустить обнаружени
е хостов
  -
PS/PA/PU [список_портов]: TCP SYN/ACK или UDP пингование заданны
х хостов
  -PE/PP/PM: Пингование с использованием ICMP-
эхо запросов, запросов временной метки и сетевой маски
  -
PO [список_протоколов]: Пингование с использованием IP протокола
  -n/-
R: Никогда не производить DNS разрешение/Всегда производить разр
ешение [по умолчанию: иногда]
  --dns-
servers <сервер1[,сервер2],...>: Задать собственные DNS сервера
для разрешения доменных имён
  --system-dns: Использовать системный DNS-преобразователь
РАЗЛИЧНЫЕ ПРИЕМЫ СКАНИРОВАНИЯ:
  -
sS/sT/sA/sW/sM: TCP SYN/с использованием системного вызова Conne
ct()/ACK/Window/Maimon сканирования
  -sU: UDP сканирование
  -sN/sF/sX: TCP Null, FIN и Xmas сканирования
  --scanflags <флаги>: Задать собственные TCP флаги
  -sI <зомби_хост[:порт]>: "Ленивое" (Idle) сканирование
  -sO: Сканирование IP протокола
  -b <FTP_хост>: FTP bounce сканирование
  --traceroute: Трассировка пути к хосту
  --
reason: Выводить причину, почему Nmap установил порт в определен
ном состоянии
ОПРЕДЕЛЕНИЕ ПОРТОВ И ПОРЯДКА СКАНИРОВАНИЯ:
  -p <диапазон_портов>: Сканирование только определенных портов
    Пример: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
  -
```

```
F: Быстрое сканирование - Сканирование ограниченного количества
портов
  -
r: Сканировать порты последовательно - не использовать случайный
 порядок портов
  --top-
ports <количество_портов>: Сканировать <количество_портов> наибо
лее распространенных портов
  --port-
ratio <рейтинг>: Сканировать порты с рейтингом большим, чем <рей
тинг>
ОПРЕДЕЛЕНИЕ СЛУЖБ И ИХ ВЕРСИЙ:
  -
sV: Исследовать открытые порты для определения информации о служ
бе/версии
  --version-
intensity <уровень>: Устанавливать от 0 (легкое) до 9 (пробовать
 все запросы)
  --version-
light: Ограничиться наиболее легкими запросами (интенсивность 2)
  --version-
all: Использовать каждый единичный запрос (интенсивность 9)
  --version-
trace: Выводить подробную информацию о процессе сканирования (дл
я отладки)
СКАНИРОВАНИЕ С ИПОЛЬЗОВАНИЕМ СКРИПТОВ:
  -sC: эквивалентно опции --script=default
  --
script=<Lua скрипты>: <Lua скрипты> - это разделенный запятыми с
писок директорий, файлов скриптов или
  категорий скриптов
  --script-
args=<имя1=значение1,[имя2=значение2,...]>: Передача аргументов
скриптам
  --script-trace: Выводить все полученные и отправленные данные
  --script-updatedb: Обновить базу данных скриптов
ОПРЕДЕЛЕНИЕ ОС:
  -O: Активировать функцию определения ОС
  --osscan-
limit: Использовать функцию определения ОС только для "перспекти
вных" хостов
  --osscan-guess: Угадать результаты определения ОС
ОПЦИИ УПРАВЛЕНИЯ ВРЕМЕНЕМ И ПРОИЗВОДИТЕЛЬНОСТЬЮ:
  Опции, принимающие аргумент <время>, задаются в миллисекундах,
 пока вы не добавите 's' (секунды), 'm' (минуты),
  или 'h' (часы) к значению (напр. 30m).
  -T[0-
5]: Установить шаблон настроек управления временем (больше - быс
трее)
  --min-hostgroup/max-
hostgroup <кол_хостов>: Установить размер групп для параллельног
о сканирования
```

```
  --min-parallelism/max-
parallelism <количество_запросов>: Регулирует распараллеливание
запросов
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-
timeout <время>: Регулирует время ожидания ответа на запрос
  --max-
retries <количество_попыток>: Задает максимальное количество пов
торных передач запроса
  --host-
timeout <время>: Прекращает сканирование медленных целей
  --scan-delay/--max-scan-
delay <время>: Регулирует задержку между запросами
  --min-
rate <число>: Посылать запросы с интенсивностью не меньше чем <ч
исло> в секунду
  --max-
rate <число>: Посылать запросы с интенсивностью не больше чем <ч
исло> в секунду
ОБХОД БРАНДМАУЭРОВ/IDS:
  -f; --
mtu <значение>: Фрагментировать пакеты (опционально с заданным з
начениме MTU)
  -
D <фикт_хост1,фикт_хост2[,ME],...>: Маскировка сканирования с по
мощью фиктивных хостов
  -S <IP_адрес>: Изменить исходный адрес
  -e <интерфейс>: Использовать конкретный интерфейс
  -g/--source-
port <номер_порта>: Использовать заданный номер порта
  --data-
length <число>: Добавить произвольные данные к посылаемым пакета
м
  --ip-options <опции>: Посылать пакет с заданным ip опциями
  --ttl <значение>: Установить IP поле time-to-
live (время жизни)
  --spoof-
mac <MAC_адрес/префикс/название производителя>: Задать собственн
ый MAC адрес
  --
badsum: Посылать пакеты с фиктивными TCP/UDP контрольными суммам
и
ВЫВОД РЕЗУЛЬТАТОВ:
  -oN/-oX/-oS/-
oG <файл>: Выводить результаты нормального, XML, s|<rIpt kIddi3,
     и Grepable формата вывода, соответственно, в заданный файл
  -
oA <базовове_имя_файла>: Использовать сразу три основных формата
 вывода
  -
v: Увеличить уровень вербальности (задать дважды или более для у
величения эффекта)
  -d[уровень]: Увеличить или установить уровень отладки (до 9)
```

```
  --
open: Показывать только открытые (или возможно открытые) порты
  --packet-trace: Отслеживание принятых и переданных пакетов
  --iflist: Вывести список интерфейсов и роутеров (для отладки)
  --log-
errors: Записывать ошибки/предупреждения в выходной файл нормаль
ного режима
  --append-
output: Добавлять выходные данные в конец, а не перезаписывать в
ыходные файлы
  --resume <имя_файла>: Продолжить прерванное сканирование
  --
stylesheet <путь/URL>: Устанавливает XSL таблицу стилей для прео
бразования XML вывода в HTML
  --webxml: Загружает таблицу стилей с Nmap.Org
  --no-stylesheet: Убрать объявление XSL таблицы стилей из XML
РАЗЛИЧНЫЕ ОПЦИИ:
  -6: Включить IPv6 сканирование
  -
A: Активировать функции определения ОС и версии, сканирование с
использованием скриптов и трассировку
  --
datadir <имя_директории>: Определяет место расположения файлов N
map
  --send-eth/--send-ip: Использовать сырой уровень Ethernet/IP
  --
privileged: Подразумевать, что у пользователя есть все привилеги
и
  --
unprivileged: Подразумевать, что у пользователя нет привилегий д
ля использования сырых сокетов
  -V: Вывести номер версии
  -h: Вывести эту страницу помощи
ПРИМЕРЫ:
  nmap -v -A scanme.nmap.org
  nmap -v -sP 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -PN -p 80
ДЛЯ СПРАВКИ ПО ДРУГИМ ОПЦИЯМ, ОПИСАНИЙ И ПРИМЕРОВ СМОТРИТЕ MAN С
ТРАНИЦУ
```

Различные опции

В этой секции описываются некоторые важные (и не очень важные) опции, которые не подходят к другим категориям.

`-6` (Включает IPv6 сканирование)

> Начиная с 2002 года Nmap имеет поддержку протокола IPv6 для своих наиболее используемых функций. В частности, пинг сканирование (только TCP), выявление возможности установки соединения и определение версии имеют поддержку протокола IPv6. Синтаксис команд

такой же как и обычный за исключением того, что вы добавляете опцию `-6`. Конечно же, вы должны использовать синтаксис IPv6, если вы указываете адрес, а не имя хоста. Адрес может выглядеть как `3ffe:7501:4819:2000:210:f3ff:fe03:14d0`, поэтому лучше использовать имена хостов. Вывод выглядит так же как и обычный, только на линии «интересных портов» будет IPv6 адрес.

Хотя протокол IPv6 еще не завоевал весь мир, в некоторых (обычно Азиатских) странах он используется интенсивно, и большинство современных операционных систем поддерживают его. Чтобы использовать Nmap с протоколом IPv6, и источник и цель сканирования должны быть настроены на работу с ним. Если ваш ISP (как большинство из них) не предоставляет вам IPv6 адрес, вы можете использовать широко распространенный и работающий с Nmap сервис Tunnel Brokers. Я использую бесплатный сервис на `http://www.tunnelbroker.net`. Другие подобные сервисы перечислены на Wikipedia.

`-A` (Опции агрессивного сканирования)

Этой опцией активируется набор агрессивных опций сканирования. Я еще не решил до конца, какие же опции будут использоваться. Сейчас этот набор включает определение ОС (`-O`), сканирование с целью определения версии (`-sV`), сканирование с использованием скриптов (`-sC`) и трассировку (`--traceroute`). Возможно в будущем будут добавлены другие функции. Целью является создание всестороннего набора опций сканирования, чтобы людям не надо было запоминать большое количество флагов. Тем не менее, т.к. сканирование с использованием скриптов с настройками по умолчанию расценивается как "назойливое", вам не следует использовать опцию `-A` для сканирования целевых сетей без разрешения. Эта опция активирует только возможности, но не устанавливает опции времени (timing) (такие как `-T4`) или опции вербального вывода (`-v`), которые вы, возможно, хотели бы использовать.

`--datadir` *<имя_директории>* (Определяет место расположения файлов Nmap)

Во время работы Nmap получает некоторые данные из файлов `nmap-service-probes`, `nmap-services`, `nmap-protocols`, `nmap-rpc`, `nmap-mac-prefixes` и `nmap-os-db`. Если место расположение какого-либо из этих файлов было задано конкретно (используя опции `--servicedb` или `--versiondb`), то оно используется для этого файла. Далее Nmap ищет эти файлы в директории, заданной опцией `--datadir` (если задана). Если файлы не были найдены там, то Nmap ищет их в директории, определенной переменной окружения NMAPDIR . Далее идут `~/.nmap` для реальных и действующих в данный момент UIDs (только POSIX системы) или расположение исполняемого файла Nmpa (только Win32), и

далее `/usr/local/share/nmap` или `/usr/share/nmap`. В последнюю очередь Nmap будет искать эти файлы в текущей директории.

`--servicedb <файл_служб>` (Задает определенный файл служб)

Указывает Nmap использовать заданный файл служб вместо файла `nmap-services`, который поставляется вместе с Nmap. Использование этой опции также подразумевает использование опции быстрого сканирования (`-F`). Смотрите описание `--datadir` для более подробной информации о файлах данных Nmap.

`--versiondb <файл_запросов_служб>` (Задает определенный файл запросов для служб)

Указывает Nmap использовать заданный файл запросов для служб вместо файла `nmap-service-probes`, который поставляется вместе с Nmap. Смотрите описание `--datadir` для более подробной информации о файлах данных Nmap.

`--send-eth` (Использовать сырой уровень ethernet)

Указывает Nmap посылать пакеты с использование более низкого сырого уровня ethernet, а не с использованием более высокого уровня IP (сетевого). По умолчанию Nmap выбирает тот способ, который больше подоходит для используемой платформы. Сырые сокеты (уровень IP) в общем случае более эффективны для Unix машин, в то время как использование ethernet фреймов необходимо для операционных систем Windows, т.к. Microsoft отключила в них поддержку сырых сокетов. Nmap по-прежнему использует сырые IP пакеты на Unix не смотря на эту опцию, когда нет другого выбора (как в случае с не-ethernet соединениями).

`--send-ip` (Использовать сырой уровень IP)

Указывает Nmap посылать пакеты с использование сырых IP сокетов, а не с использованием более низкого уровня ethernet фреймов. Это дополнение к опции `--send-eth` описанной выше.

`--privileged` (Подразумевать, что у пользователя есть все привилегии)

Указывает Nmap, что у нее есть необходимые привилегии для использования сырых сокетов, пакетного сниффинга и сходных операций, которые обычно требуют привилегий пользователя root на Unix системах. По умолчанию Nmap завершает работу, если были запрошены такие опреации, но `geteuid` не нуль. Опцию `--privileged` хорошо использовать на системах с возможностями ядра Linux или подобных, которые могут быть сконфигурированы так, что непривилегированные

пользовтели смогут осуществлять сканирование с использованием сырых сокетов. Удостоверьтесь, что эта опция указана перед любыми опциями требующими привилегий (сканирование SYN, определение ОС и т.д.). Переменная окурежния `NMAP_PRIVILEGED` может быть установлена как равнозначная альтернатива опции `--privileged`.

`--unprivileged` (Подразумевать, что у пользователя нет привилегий для использования сырых сокетов)

Эта опция противоположна `--privileged`. Указывает Nmap, что у пользователя нет привилегий для использования сырых сокетов и сниффинга. Полезна для тестирования, отладки или когда по какой-то причине на вашей системе не работае механизм сырых сокетов. Переменная окружения `NMAP_UNPRIVILEGED` может быть установлена как равнозначная альтернатива опции `--unprivileged`.

`--release-memory` (Освободить память перед завершением работы)

Эта опция полезна только во время отладки утечки памяти. Заставляет Nmap освободить занянутю память перед завершением работы, что облегчает задачу обнаружения действительной утечки памяти. В обычном режиме работы Nmap пропускает этот шаг, так ОС делает это самостоятельно при закрытии процесса.

`-V`; `--version` (Вывести номер версии)

Выводит номер версии Nmap и завершает работу.

`-h`; `--help` (Вывести страницу помощи)

Выводит небольшую страницу помощи с наиболее часто используемыми командами и опциями. Запуск Nmap без аргументов приводит к такому же результату.

Определение цели сканирования

В командной строке Nmap все, что не является опцией (или аргументом опции), рассматривается как цель сканирования. В простейшем случае для сканирования используется IP адрес или сетевое имя целевой машины.

Иногда необходимо просканировать целую сеть. Для этого Nmap поддерживает CIDR адресацию. Вы можете добавить /*<кол-во бит>* к IP адресу или сетевому имени и Nmap просканирует каждый IP адрес, для которого первые *<кол-во бит>* такие же как и у заданного хоста. Например, 192.168.10.0/24 просканирует 256 хостов между 192.168.10.0 (бинарное: `11000000 10101000 00001010 00000000`) и 192.168.10.255 (бинарное: `11000000 10101000 00001010 11111111`) включительно. 192.168.10.40/24

сделает абсолютно то же самое. Зная, что IP адрес scanme.nmap.org 64.13.134.52, при записи типа scanme.nmap.org/16 будет произведено сканирование 65,536 IP адресов между 64.13.0.0 и 64.13.255.255. Наименьшее допустимое значение /0, при котором будет просканирован весь Интернет. Наибольшее значение /32, при котором будет просканирован только заданный хост или IP адрес, т.к. все адресные биты заблокированы.

CIDR нотация коротка, однако не всегда достаточно гибка. Например, вы хотите просканировать 192.168.0.0/16, но пропустить все IP-адреса, оканчивающиеся на .0 или .255, т.к. обычно это широковещательные адреса. Nmap может осуществить такое сканирование путем задания диапазонов в октетах. Вместо определния обычного IP адреса, вы можете определить для каждого октета либо разделенный запятыми список чисел, либо диапазон. Например, 192.168.0-255.1-254 пропустит все адреса в диапазоне оканчивающиеся на .0 и .255. Диапазоны не обязательно задавать только в последних октетах: при записи 0-255.0-255.13.37 будет произведено сканирование всех адресов в Интернете оканчивающихся на 13.37. Такой тип сканирования может быть полезен для исследования просторов Интернета.

IPv6 адреса могут быть определны только в форме, полностью соответствующей правильной форме записи IPv6 адресов. CIDR и использование диапазонов в октетах не применимо к IPv6 адресам, т.к. они редко используются.

Вы можете передавать в командной строке Nmap различные варианты определения целей, не обязательно одного типа. Команда **nmap scanme.nmap.org 192.168.0.0/16 10.0.0,1,3-7.0-255** сделает то, что вы ожидаете.

Цели сканирования обычно задаются в командной строке, и существуют различные опции контроля выбора целей:

`-iL <имя_файла>` (Ввод из списка)

Считывает цели из *<имя_файла>*. Хотя передача большого списка хостов для сканирования является обычным явлением, это не удобно. Например, ваш DHCP сервер передают вам список из 10,000 используемых им на данный момент адресов, и вы хотите его просканировать. Или, возможно, вы хотите просканировать все IP адреса, *кроме* переданных им, чтобы выявить несанкционированное использование статических IP адресов. Просто сгенерируйте список хостов для сканирования и передайте имя файла в Nmap как аргумент для опции `-iL`. Записи в файле могут находиться в любой приемлимой для Nmap форме (IP адреса, сетевые имена, CIDR, IPv6, или диапазоны в октетах). Каждая запись должна быть отделена пробелом или несколькими, символами табуляции либо символами перехода на новую строку. Вы можете передать в качестве аргумента дефис(-) как имя файла, если хотите, чтобы Nmap считывал список хостов из стандартного ввода, а не из файла.

`-iR <кол-во хостов>` (Выбирает произвольные цели)

Для сканирования в пределах всего Интернета или каких-либо исследований, вам, возможно, понадобится выбрать цели произвольно. Аргумент *<кол-во хостов>* определяет сколько необходимо сгенерировать IP адресов. Неподходящие IP адреса, такие как частные, широковещательные или нелокализованные диапазоны адресов автоматически пропускаются. Аргумент `0` может быть передан для бесконечного сканирования. Имейте в виду, что некоторым системным

администраторам может не понравиться неразрешенное сканирование их сетей и они могут пожаловаться. Используйте эту опцию на свой страх и риск! Если в дождливый денек вам будет скучно, попробуйте команду **nmap -sS -PS80 -iR 0 -p 80** для сканирования произвольных веб-серверов.

`--exclude <хост1>[,<хост2>[,...]]` (Исключить хосты/сети)

Определяет разделенный запятыми список целей, которые необходимо исключить из сканирования, даже если они являются частью заданного вами диапазона сканирования. Передаваемый список использует стандартный синтаксис Nmap, поэтому может содержать сетевые имена, CIDR адресацию, диапазоны в октетах и т.д. Эта опция может быть полезна, если сеть, которую вы хотите просканировать, содержит сервера или системы, негативно реагирующие на сканирование портов, или подсети, администрируемые другими людьми.

`--excludefile <имя_файла>` (Исключить список из файла)

Эта опция делает то же самое, что и `--exclude`, за исключением того, что цели для исключения находятся в разделенном пробелами, символами табуляции или символами перехода на новую строку *<файле>*, а не в командной строке.

Основы сканирования портов

Хотя Nmap постоянно наращивала функциональность, изначально утилита разрабатывалась как эффективный сканер портов, и она по-прежнему сохраняет свои основные функции. Простой командой **nmap *<цель сканирования>*** будет произведено сканирование более чем 1660 TCP портов на *<целевой машине>*. В то время как многие сканеры портов традиционно разделяют все порты на закрытые и открытые, Nmap имеет более подробную шкалу деления. Она подразделяет порты на шесть состояний: `открыт`, `закрыт`, `фильтруется`, `не фильтурется`, `открыт|фильтруется` или `закрыт|фильтруется`.

Эти состояния не являются собственно характеристиками самих портов, а лишь описывают, как Nmap видит их. Например, сканирование из той же сети, что и цель, может показать, что порт `135/tcp` открыт, в то время как сканирование из Интернета в то же время и с теми же опциями может показать, что порт `фильтруется`.

Шесть состояний портов распознаваемых Nmap
открыт (open)

Приложение принимает запросы на TCP соединение или UDP пакеты на этот порт. Обнаружение этого состояния обычно является основной целью сканирования. Люди разбирающиеся в безопасности знают, что каждый открытый порт это прямой путь к осуществлению атаки. Атакующие хотят использовать открытые порты, а администраторы пытаются закрыть их или защитить с помощью брадмауэров так, чтобы не мешать работе обычных пользователей. Октрытые порты также

интересны с точки зрения сканирования, не связанного с безопасностью, т.к. они позволяют определить службы доступные в сети.

закрыт (closed)

Закрытый порт доступен (он принимает и отвечает на запросы Nmap), но не используется каким-либо приложением. Они могут быть полезны для установления, что по заданному IP адресу есть работающий хост (определение хостов, ping сканирование), или для определения ОС. Т.к. эти порты достижимы, может быть полезным произвести сканирование позже, т.к. некоторые из них могут открыться. Администраторы могут заблокировать такие порты с помощью брандмауэров. Тогда их состояние будет определено как фильтруется, что обсуждается далее.

фильтруется (filtered)

Nmap не может определить, открыт ли порт, т.к. фильтрация пакетов не позволяет достичь запросам Nmap этого порта. Фильтрация может осуществляться выделенным брадмауэром, правилами роутера или брандмауэром на целевой машине. Эти порты бесполезны для атакующих, т.к. предоставляют очень мало информации. Иногда они отвечают ICMP сообщениями об ошибке, такими как тип 3 код 13 (destination unreachable: communication administratively prohibited (цель назначения недоступна: связь запрещена администратором)), но чаще встречаются фильтры, которые отбрасывают запросы без предоставления какой-либо информации. Это заставляет Nmap совершить еще несколько запросов, чтобы убедиться, что запрос был отброшен фильтром, а не затором в сети. Это очень сильно замедляет сканирование.

не фильтруется (unfiltered)

Это состояние означает, что порт доступен, но Nmap не может определить открыт он или закрыт. Только ACK сканирование, используемое для определения правил брандмауэра, может охарактеризовать порт этим состоянием. Сканирование не фильтруемых портов другими способами, такими как Window сканирование, SYN сканирование или FIN сканирование может помочь определить, является ли порт открытым.

открыт|фильтруется (open|filtered)

Nmap характеризует порт таким состоянием, когда не может определить октрыт порт или фильтруется. Это состояние возникает при таких типах сканирования, при которых открытые порты не отвечают. Отсутствие ответа также может означать, что пакетный фильтр не пропустил запрос или ответ не был получен. Поэтому Nmap не может определить наверняка открыт порт или фильтруется. При сканировании UDP, по IP протоколу,

FIN, NULL, а также Xmas порт может быть охарактеризован таким состоянием.

закрыт|фильтруется (closed|filtered)

Это состояние используется, когда Nmap не может определить закрыт порт или фильтруется. Используется только при сканировании IP ID idle типа.