nmap — свободная утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб). wiki

Установка под Ubuntu

sudo apt-get install nmap

nmap имеет богатый набор опций для сканирования как отдельного хоста так и диапазона хостов на предмет сбора разной информации. Ниже приведен список наиболее использованных мной сочетаний ключей.

Для работы большинства возможностей nmap требуется права root.

Разработчики nmap предлагают хост scanme.nmap.org для тестового сканирования.

Получение информации об портах удаленного хоста и определение операционной системы

sudo nmap -sS -P0 -sV -O scanme.nmap.org

scanme.nmap.org – сканируемый хост, может быть: IP, имя хоста или подсеть

-sS – TCP SYN сканирование (полуоткрытое)

-P0 – отключение ICMP сканирования

-sV – определение сервисов, запущенных на открытых портах

-O – определение версии операционной системы

Пропинговать диапазон адресов

sudo nmap -sP -v "192.168.1.\*"

# или

sudo nmap -sP -v 192.168.1.0/24

# или

sudo nmap -sP -v 192.168.1.1-20

-sP - ping-сканирование

Проверка одного порта или диапазона

sudo nmap -sT -p 22 scanme.nmap.org

# диапазон

sudo nmap -sT -p 20-110 scanme.nmap.org

-sT - TCP-сканирование

При сканировании можно скрыть свой IP адрес

sudo nmap -sS scanme.nmap.org -D 8.8.8.8

Сканирование списка хостов из файла

nmap -iL list.txt

Для определения открытых портов на локальной машине нужно выполнить

nmap localhost

Для принудительного закрытия определенного порта можно воспользоваться fuser

fuser -k 80/tcp

Определение разницы между двумя сканами

sudo nmap -n -PN 192.168.1.1/24 -O > scan1

sudo nmap -n -PN 192.168.1.1/24 -O > scan2

ndiff -b scan1 -o scan2

Подсчет Linux/Windows машин в сети (источник)

sudo nmap -F -O 192.168.0.1-255 | \ grep "Running: " > /tmp/os; \ echo "$(cat /tmp/os | grep Linux | wc -l) Linux device(s)"; \ echo "$(cat /tmp/os | grep Windows | wc -l) Window(s) devices"

Графический интерфейс для nmap - Zenmap, умеет визуализировать топологию сети, сохранять параметры поиска в виде профиля, находить разницу (diff) между двумя результатами поиска.

Для linux-систем можно отключить ответы на ping-запросы (ICMP echo), для этого нужно добавить в /etc/sysctl.conf следующие строки

net.ipv4.icmp\_echo\_ignore\_broadcasts = 1

net.ipv4.icmp\_echo\_ignore\_all = 1

и приминить изменения

sysctl –p

Об nmap для начинающих

2011-04-12 от ashep

Когда-нибудь задавались вопросом, откуда взломщики узнают о том, какие порты открыты в системе и какие службы доступны на этих портах? Как они это делают, не задавая вопросов администратору сервера? Это и гораздо больше можно делать при помощи маленькой утилиты под названием nmap. nmap — это сокращение от «Network Mapper», по-русски можно назвать «построитель карты сети». Nmap — поистине огромный набор инструментов «в одном флаконе» для сканирования сетей. Он может использоваться для поиска и определения запущенных в сети сервисов, определения типа используемой операционной системы, типа файрвола или же просто для быстрого определения хостов, находящихся в сети. Короче говоря, уметь пользоваться этой штуковиной лишним не будет. Nmap очень известная утилита в буквальном смысле. Когда вы с ней познакомитесь, вы можете узнать её в некоторых эпизодах кинофильмов. В этой заметке я покажу вам базовые приёмы работы с Nmap и покажу несколько примеров, как его использовать.

В большинстве современных дистрибутивов Nmap присутствует в стандартных репозиториях. Если к используемой вами системе это не относится, вы можете получить исходные коды утилиты и некоторые бинарные сборки со страницы загрузок проекта.

Синтаксис вызова утилиты из командной строки следующий:

nmap <опции> цель

Допустим, вам необходимо попытаться определить тип и версию запущенной ОС на удалённой системе target.host.com. Запустите Nmap с опцией '-O' (использование этой опции требует администраторских привилегий):

# nmap -O target.host.com

Опрос удалённой системы займёт некоторое время и после того, как он завершится, вы получите вывод, подобный представленному ниже:

Starting Nmap 5.21 ( http://nmap.org ) at 2010-02-27 23:52 EST

Nmap scan report for 10.0.0.1

Host is up (0.0015s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

53/tcp open domain

5009/tcp open airport-admin

10000/tcp open snet-sensor-mgmt

MAC Address: 00:11:24:6B:43:E2 (Apple Computer)

Device type: WAP|printer

Running: Apple embedded, Canon embedded, Kyocera embedded, Xerox embedded

OS details: VxWorks: Apple AirPort Extreme v5.7 or AirPort Express v6.3; Canon imageRUNNER printer (5055, C3045, C3380, or C5185); Kyocera FS-4020DN printer; or Xerox Phaser 8860MFP printer

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 10.21 seconds

Как вы видите, Nmap предоставил достаточно много информации. В представленном примере Nmap выполнил ряд тестов, на основании которых попытался определить тип и версию ОС, используемую на хосте. Приведённый выше вывод Nmap — результат сканирования роутера Apple Airport Extreme. Помимо того, что Nmap сообщил нам тип предполагаемой ОС, он также вывел информацию о сетевой удалённости устройства, MAC-адрес и производителя сетевого интерфейса, перечень открытых портов и время, затраченное на сканирование.

Ниже представлен вывод другого сканирования, хоста под управлением Ubuntu 9.10:

Starting Nmap 5.21 ( http://nmap.org ) at 2010-02-28 00:00 EST

Nmap scan report for 10.0.0.6

Host is up (0.0039s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 00:17:08:2A:D6:F0 (Hewlett Packard)

Device type: general purpose

Running: Linux 2.6.X

OS details: Linux 2.6.19 - 2.6.31

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 3.40 seconds

Здесь мы видим, что производителем сетевого интерфейса является HP, операционной системой является Linux с ядром версии в районе 2.6.19-2.6.31. Вообще, точно определить версию ядра Linux с помощью Nmap обычно невозможно.

Предупреждение

В приведённых выше примерах я сканировал свой собственный роутер и одну из рабочих станций, находящихся в моей сети, поскольку я имею на то полное право. В принципе вы можете сканировать любой хост, какой пожелаете, однако, не очень хорошая идея заниматься сканированием чужих сетей и хостов без разрешения их владельцев. Если вам нужен хочт для экспериментов, сообщество готово вам его предоставить по адресу scanme.nmap.org. Этот хост специально создан для тестирования Nmap, только если вы не собираетесь тестировать на нём атаки типа DoS.

Некоторые администраторы без понимания относятся к неожиданным сканированиям их сетей, поэтому не вылезайте за рамки и сканируйте те хосты, которые вам разрешено сканировать. Помимо всего прочего, действие некоторых агрессивных методов сканирования Nmap могут выходить за рамки правил, установленных вашим провайдером, так что будьте внимательны.

Сканирование нескольких хостов

За один запуск Nmap вы можете сканировать более одного хоста. Если в качетсве целей сканирования вы используете IP-адреса, вы можете передавать их Nmap в виде диапазонов, например: 10.0.0.1-6 или 10.0.0.0/24. Первый способ определяет диапазон IP-адресов c 10.0.0.1 по 10.0.0.6, а вторая — с 10.0.0.1 по 10.0.0.254, т. е. всю подсеть 10.0.0.0 с маской 24 в CIDR-нотации. Например, если вы хотите выполнить сканирование хостов с IP-адресами 10.0.0.1-10.0.0.42, команда будет следующей:

# nmap -O 10.0.0.1-42

Если же вы используете имена хостов вместо адресов, то просто перечислите имена через пробел:

# nmap -O host1.target.com host2.target.com

Поиск открытых портов

Если вы запустите Nmap без опций, передав ему лишь имя целевого хоста, то Nmap выполнит сканирование цели на предмет открытых сетевых портов и служб их прослушивающих. Например:

$ nmap target.hostname.com

Interesting ports on target.hostname.com (10.0.0.88):

Not shown: 1711 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

3306/tcp open mysql

Nmap done: 1 IP address (1 host up) scanned in 0.228 seconds

Здесь вы можете увидеть, что на целевом хосте открыты порты 22, 80 и 3306 с перечислением названий сервисов, сидящих на этих портах, соответственно ssh, http и mysql. Nmap распознаёт шесть состояний портов: open (открыт), closed (закрыт), filtered (порт недоступен, скорее всего фильтруется файрволом), unfiltered (порт доступен, но состояние определить не удалось), open|filtered (открыт или фильтруется файрволом), и closed|filtered (закрыт или фильтруется файрволом).

Если вам нужна более детальная информация, воспользуйтесь одинарной или двойной опцией '-v', например:

$ nmap -vv host.target.com

Initiating Ping Scan at 11:44

Scanning 10.0.0.28 [1 port]

Completed Ping Scan at 11:44, 0.00s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 11:44

Completed Parallel DNS resolution of 1 host. at 11:44, 0.00s elapsed

Initiating Connect Scan at 11:44

Scanning host.target.com (10.0.0.28) [1714 ports]

Discovered open port 22/tcp on 10.0.0.28

Discovered open port 80/tcp on 10.0.0.28

Discovered open port 3306/tcp on 10.0.0.28

Completed Connect Scan at 11:44, 0.08s elapsed (1714 total ports)

Host host.target.com (10.0.0.28) appears to be up ... good.

Interesting ports on host.target.com (10.0.0.28):

Not shown: 1711 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

3306/tcp open mysql

Read data files from: /usr/share/nmap

Nmap done: 1 IP address (1 host up) scanned in 0.104 seconds

Сканирование служб

Если вам необходимо выяснить как можно подробней, что за сервис болтается на том или ином порту, попробуйте воспользоваться опциями '-sV'. Эти опции заставляют Nmap вместо обычного сканирования портов, произвести более агрессивное сканирование, опрашивая сервисы, находящиеся на том или ином порту. Также этот метод иногда позволяет более точно определить тип и версию используемой на целевой системе ОС.

$ nmap -sV target.host.com

Starting Nmap 5.21 ( http://nmap.org ) at 2010-02-28 00:15 EST

Nmap scan report for test.host.net (XX.XXX.XXX.XX)

Host is up (0.090s latency).

Not shown: 965 closed ports, 33 filtered ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)

Service Info: OS: Linux

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 11.43 seconds

Как видно из вывода выше, Nmap определил серверы SSH-4.7 и Apache-2.2.8, находящиеся на портах 22 и 80. Также из названий версий ПО удаётся определить, что сервер работает под Ubuntu Linux. Такой метод сканирования может оказаться весьма кстати, когда вам необходимо выявить устаревшие версии ПО, работающие на ваших хостах, которые могут быть подвержены известным угрозам.

Кто живёт в моей сети?

Не уверены точно, что знаете обо всех обитателях своей сети? Попробуйте запустить Nmap с параметрами '-sP' и он выполнит обычное пинг-сканирование, определяя лишь отвечающие хосты, не прибегая к сканированию портов. Например, чтобы определить «живых» в подсети 10.0.0.0/24, достаточно простой команды:

$ nmap -sP 10.0.0.0/24

Или же, как было сказано выше, вы можете указать диапазон хостов, а не всю подсеть. Например:

$ nmap -sP 10.0.0.1-16