



[Главная](#) >> [Инструкции](#) >> Как пользоваться Nmap для сканирования сети

Как пользоваться Nmap для сканирования сети

Обновлено: 27 ноября 2020 Опубликовано: 27 ноября, 2016 от [admin](#), 13 комментариев, время чтения: 8 минут

Обнаружили ошибку в тексте? Сообщите мне об этом. Выделите текст с ошибкой и нажмите Ctrl+Enter.

Nmap - это очень популярный сканер сети с открытым исходным кодом, который может использоваться как в Windows, так и в Linux. Программа Nmap или Network Mapper была разработана Гордоном Луоном и на данный момент используется специалистами по безопасности и системными администраторами по всему миру.

Эта программа помогает системным администраторам очень быстро понять какие компьютеры подключены к сети, узнать их имена, а также посмотреть какое программное обеспечение на них установлено, какая операционная система и какие типы фильтров применяются. Функциональность программы может быть расширена за счет собственного скриптового языка, который позволяет администраторам автоматизировать много действий.

Например, с помощью скриптов можно автоматически обнаруживать новые уязвимости безопасности в вашей сети. Nmap может использоваться с хорошими и плохими намерениями, будьте аккуратны, чтобы не использовать nmap против закона. В этой инструкции мы рассмотрим как пользоваться nmap для сканирования портов в операционной системе Linux. Но сначала нужно попытаться понять как работает эта утилита.

Конфиденциальность · Условия использования

Содержание статьи

- [Как работает Nmap?](#)
- [Синтаксис Nmap](#)
- [Как пользоваться Nmap для сканирования портов в Linux](#)
- [Выводы](#)

Как работает Nmap?

В компьютерных сетях все подключенные устройства имеют свой IP адрес. Каждый компьютер поддерживает протокол ping, с помощью которого можно определить подключен ли он к сети. Мы просто отправляем ping запрос компьютеру, и если он отзывается, то считаем, что он подключен. Nmap использует немного иной подход. Компьютеры также определенным образом реагируют на те или иные сетевые пакеты, утилита просто отправляет нужные пакеты и смотрит какие хосты прислали ответ.

Но об этом вы, наверное, уже знаете. Более интересно то как Nmap узнает какие сервисы запущены на машине. Суть работы всех сетевых программ основана на портах. Чтобы получить сообщение из сети, программа должна открыть порт на вашем компьютере и ждать входящих соединений. А для отправки сообщения по сети нужно подключиться к уже другой программой (адресатом) порту. Затем программе необходимо будет открыть порт, на котором она будет ждать ответа.

Утилита nmap в процессе сканирования сети перебирает доступный диапазон портов и пытается подключиться к каждому из них. Если подключение удалось, в большинстве случаев, передав несколько пакетов программа может даже узнать версию программного обеспечения, которые ожидает подключений к этому порту. Теперь, после того, как мы рассмотрели основы, рассмотрим как пользоваться nmap для сканирования портов и сети.

Синтаксис Nmap

Команда запуска Nmap очень проста для этого достаточно передать ей в параметрах целевой IP адрес или сеть, а также указать опции при необходимости:

\$ nmap опции адрес

Теперь давайте рассмотрим основные опции, которые понадобятся нам в этой статье.

- **-sL** - просто создать список работающих хостов, но не сканировать порты nmap;
- **-sP** - только проверять доступен ли хост с помощью ping;
- **-PN** - считать все хосты доступными, даже если они не отвечают на ping;
- **-sS/sT/sA/sW/sM** - TCP сканирование;

Privacy

- **-sU** - UDP сканирование порт;
- **-sN/sF/sX** - TCP NULL и FIN сканирование;
- **-sC** - запускать скрипт по умолчанию;
- **-sI** - ленивое Idle сканирование;
- **-p** - указать диапазон портов для проверки;
- **-sV** - детальное исследование портов для определения версий служб;
- **-O** - определять операционную систему;
- **-T[0-5]** - скорость сканирования, чем больше, тем быстрее;
- **-D** - маскировать сканирование с помощью фиктивных IP;
- **-S** - изменить свой IP адрес на указанный;
- **-e** - использовать определенный интерфейс;
- **--spoof-mac** - установить свой MAC адрес;
- **-A** - определение операционной системы с помощью скриптов.

Теперь, когда мы рассмотрели все основные опции, давайте поговорим о том, как выполняется сканирование портов порт.

Как пользоваться Nmap для сканирования портов в Linux

Дальше рассмотрим примеры порт. Сначала давайте рассмотрим как найти все подключенные к сети устройства, для этого достаточно использовать опцию **-sL** и указать маску нашей сети. в моем случае это 192.168.1.1/24. Маску вашей локальной сети вы можете найти, выполнив команду:

```
$ ip addr show
```



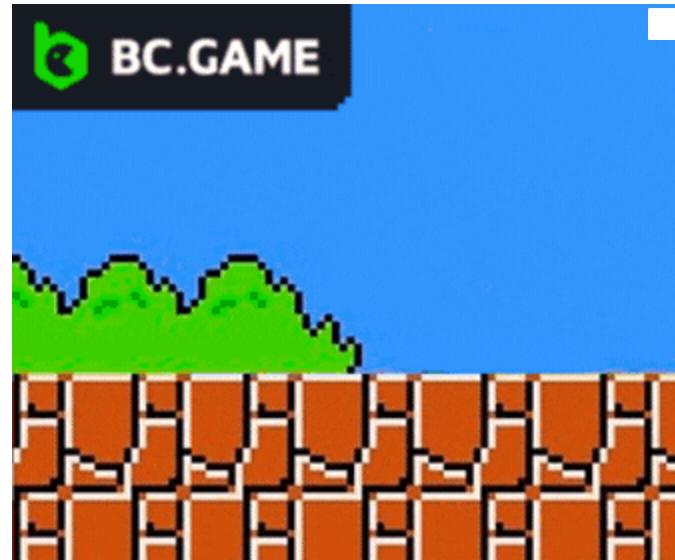
Privacy

```
sergiy@dhcppc0:~> ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether bc:ae:c5:be:8b:b7 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.2/24 brd 192.168.1.255 scope global eth0
            valid_lft forever preferred_lft forever
        inet6 fe80::beae:c5ff:febe:8bb7/64 scope link
            valid_lft forever preferred_lft forever
3: vmnet1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:50:56:c0:00:01 brd ff:ff:ff:ff:ff:ff
        inet 172.16.173.1/24 brd 172.16.173.255 scope global vmnet1
            valid_lft forever preferred_lft forever
        inet6 fe80::250:56ff:fec0:1/64 scope link
            valid_lft forever preferred_lft forever
4: vmnet8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:50:56:c0:00:08 brd ff:ff:ff:ff:ff:ff
        inet 172.16.16.1/24 brd 172.16.16.255 scope global vmnet8
            valid_lft forever preferred_lft forever
        inet6 fe80::250:56ff:fec0:8/64 scope link
            valid_lft forever preferred_lft forever
5: vboxnet0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 0a:00:27:00:00:00 brd ff:ff:ff:ff:ff:ff
sergiy@dhcppc0:~>
```

Из вывода для используемого интерфейса возьмите число после слеша, а до слэша укажите ip вашего роутера. Команда на сканирование сети nmap будет выглядеть вот так:

```
$ nmap -sL 192.168.1.1/24
```

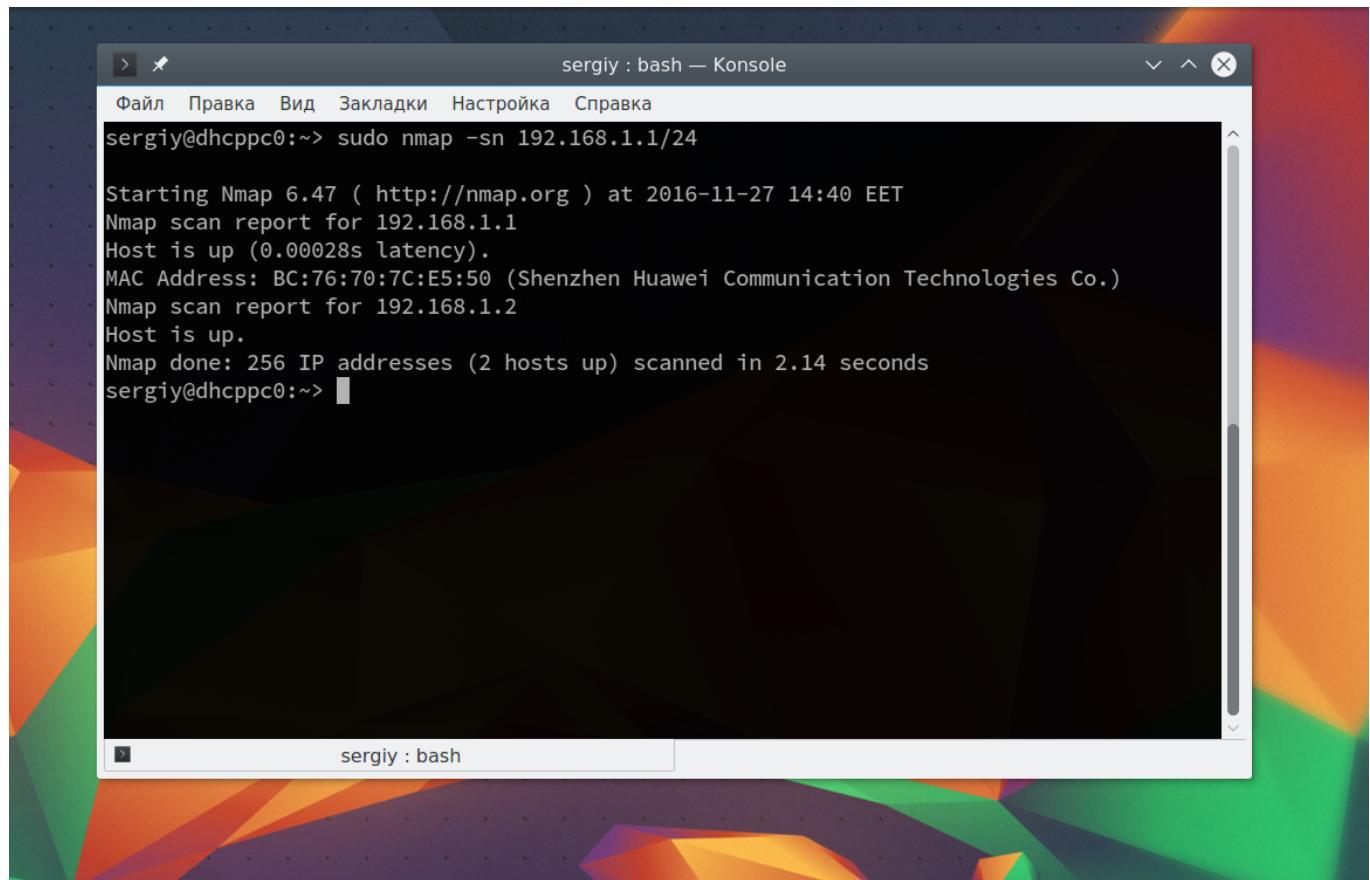
```
Nmap scan report for 192.168.1.236
Nmap scan report for 192.168.1.237
Nmap scan report for 192.168.1.238
Nmap scan report for 192.168.1.239
Nmap scan report for 192.168.1.240
Nmap scan report for 192.168.1.241
Nmap scan report for 192.168.1.242
Nmap scan report for 192.168.1.243
Nmap scan report for 192.168.1.244
Nmap scan report for 192.168.1.245
Nmap scan report for 192.168.1.246
Nmap scan report for 192.168.1.247
Nmap scan report for 192.168.1.248
Nmap scan report for 192.168.1.249
Nmap scan report for 192.168.1.250
Nmap scan report for 192.168.1.251
Nmap scan report for 192.168.1.252
Nmap scan report for 192.168.1.253
Nmap scan report for 192.168.1.254
Nmap scan report for 192.168.1.255
Nmap done: 256 IP addresses (0 hosts up) scanned in 13.50 seconds
```



Иногда это сканирование может не дать никаких результатов, потому что некоторые операционные системы имеют защиту от сканирования портов. Но это можно обойти, просто использовав для сканирования `ping` всех ip адресов сети, для этого есть опция `-sn`:

```
$ nmap -sn 192.168.1.1/24
```

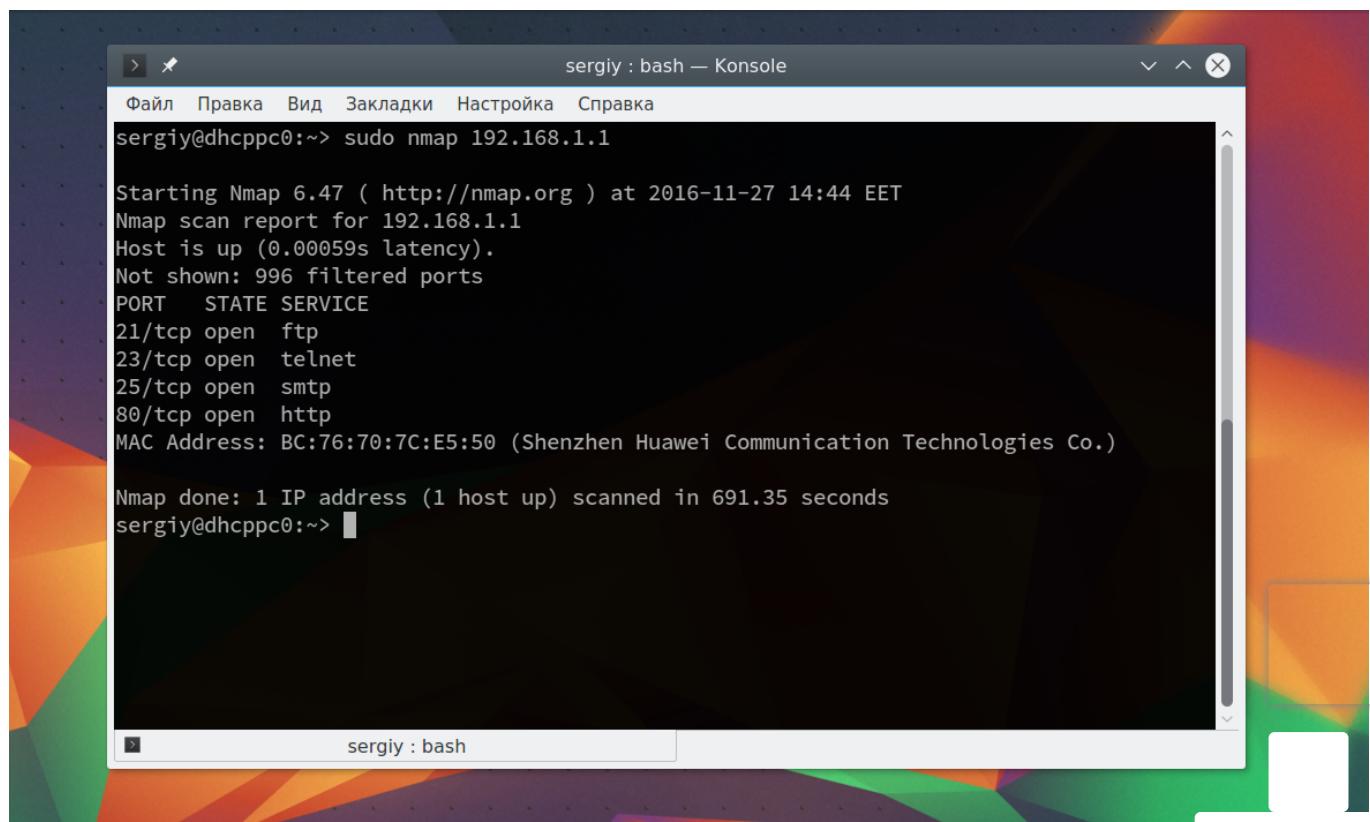
Privacy



```
sergiy@dhcppc0:~> sudo nmap -sn 192.168.1.1/24
Starting Nmap 6.47 ( http://nmap.org ) at 2016-11-27 14:40 EET
Nmap scan report for 192.168.1.1
Host is up (0.00028s latency).
MAC Address: BC:76:70:7C:E5:50 (Shenzhen Huawei Communication Technologies Co.)
Nmap scan report for 192.168.1.2
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.14 seconds
sergiy@dhcppc0:~>
```

Как видите, теперь программа обнаружила активные устройства в сети. Дальше мы можем сканировать порты nmap для нужного узла запустив утилиту без опций:

\$ sudo nmap 192.168.1.1



```
sergiy@dhcppc0:~> sudo nmap 192.168.1.1
Starting Nmap 6.47 ( http://nmap.org ) at 2016-11-27 14:44 EET
Nmap scan report for 192.168.1.1
Host is up (0.00059s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
MAC Address: BC:76:70:7C:E5:50 (Shenzhen Huawei Communication Technologies Co.)

Nmap done: 1 IP address (1 host up) scanned in 691.35 seconds
sergiy@dhcppc0:~>
```

Privacy

Теперь мы можем видеть, что у нас открыто несколько портов, все они используются каким-либо сервисом на целевой машине. Каждый из них может быть потенциально уязвимым, поэтому иметь много открытых портов на машине небезопасно. Но это еще далеко не все, что вы можете сделать, дальше вы узнаете как пользоваться nmap.

Чтобы узнать более подробную информацию о машине и запущенных на ней сервисах вы можете использовать опцию `-sV`. Утилита подключится к каждому порту и определит всю доступную информацию:

```
$ sudo nmap -sV 192.168.1.1
```

```

sergiy : bash — Konsole <2>
Файл Правка Вид Закладки Настройка Справка
sergiy@dhcppc0:~> sudo nmap -sV 192.168.1.1
root's password:

Starting Nmap 6.47 ( http://nmap.org ) at 2016-11-27 14:59 EET
Nmap scan report for 192.168.1.1
Host is up (0.00050s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
23/tcp    open  telnet?
25/tcp    open  smtp?
80/tcp    open  http    RomPager UPnP/1.0

```

На нашей машине запущен `ftp`, а поэтому мы можем попытаться рассмотреть эту службу подробнее с помощью стандартных скриптов nmap. Скрипты позволяют проверить порт более детально, найти возможные уязвимости. Для этого используйте опцию `-sC` и `-r` чтобы задать порт:

```
$ sudo nmap -sC 192.168.56.102 -p 21
```

Мы выполняли скрипт по умолчанию, но есть еще и другие скрипты, например, найти все скрипты для `ftp` вы можете командой:

```
$ sudo find /usr/share/nmap/scripts/ -name '*.nse' | grep ftp
```

Затем попытаемся использовать один из них, для этого достаточно указать его с помощью опции `--script`. Но сначала вы можете посмотреть информацию о скрипте:

[Privacy](#)

```
$ sudo nmap --script-help ftp-brute.nse
```

```
sergiy : bash — Konsole
Файл Правка Вид Закладки Настройка Справка
sergiy@dhcppc0:~> nmap --script-help ftp-brute.nse
Starting Nmap 6.47 ( http://nmap.org ) at 2016-11-27 15:10 EET
ftp-brute
Categories: intrusive brute
http://nmap.org/nsedoc/scripts/ftp-brute.html
    Performs brute force password auditing against FTP servers.

    Based on old ftp-brute.nse script by Diman Todorov, Vlatko Kosturjak and Ron Bowes.
sergiy@dhcppc0:~>
```

Этот скрипт будет пытаться определить логин и пароль от FTP на удаленном узле. Затем выполните скрипт:

```
$ sudo nmap --script ftp-brute.nse 192.168.1.1 -p 21
```

```
sergiy@dhcppc0:~> nmap --script ftp-brute.nse 192.168.1.1
Starting Nmap 6.47 ( http://nmap.org ) at 2016-11-27 15:11 EET
Nmap scan report for 192.168.1.1
Host is up (0.00057s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-brute:
| Accounts
|   admin:admin - Valid credentials
| Statistics
|   Performed 370 guesses in 75 seconds, average tps: 6
|_ ERROR: Too many retries, aborted ...
Nmap done: 1 IP address (1 host up) scanned in 75.88 seconds
sergiy@dhcppc0:~>
```

В результате скрипт подобрал логин и пароль, `admin/admin`. Вот поэтому не нужно использовать параметры входа по умолчанию.

Также можно запустить утилиту с опцией `-A`, она активирует более агрессивный режим работы утилиты, с помощью которого вы получите большую часть информации одной командой:

```
$ sudo nmap -A 192.168.1.1
```

```

Starting Nmap 6.47 ( http://nmap.org ) at 2016-11-27 15:17 EET
Nmap scan report for 192.168.1.1
Host is up (0.00066s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp?
|_ftp-anon: ERROR: Script execution failed (use -d to debug)
|_ftp-bounce: no banner
23/tcp    open  telnet?
25/tcp    open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp    open  tcpwrapped
MAC Address: BC:76:70:7C:E5:50 (Shenzhen Huawei Communication Technologies Co.)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|phone|VoIP adapter
Running (JUST GUESSING): Cisco embedded (86%), Nokia Symbian OS (85%)
OS CPE: cpe:/h:cisco:catalyst_1900 cpe:/o:nokia:symbian_os cpe:/h:cisco:ata_188_voip_g
ateway
Aggressive OS guesses: Cisco Catalyst 1900 switch (86%), Nokia 3600i mobile phone (85%)
, Cisco ATA 188 VoIP adapter (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.66 ms  192.168.1.1

OS and Service detection performed. Please report any incorrect results at http://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.31 seconds

```

Обратите внимание, что здесь есть почти вся информация, которую мы уже видели раньше. Ее можно использовать чтобы увеличить защиту этой машины.

Выводы

В этой статье мы рассмотрели как выполняется сканирование портов nmap, а также несколько простых примеров использования этой утилиты. Эти команды nmap могут быть полезными многим системным администраторам, чтобы улучшить безопасность их систем. Но это далеко не все возможности утилиты. Продолжайте экспериментировать с утилитой чтобы узнать больше только не в чужих сетях!

Была ли эта информация полезной для вас?

Да

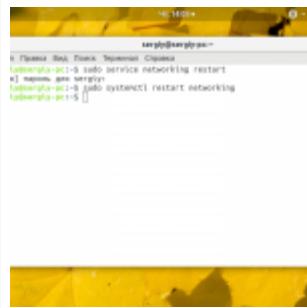
Нет

Похожие записи

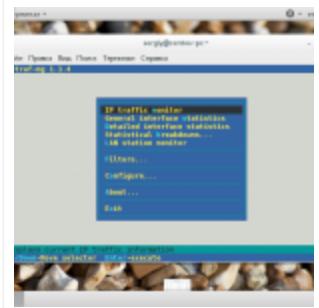
[Privacy](#)



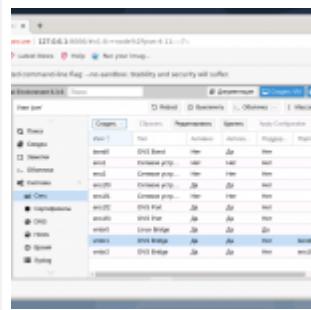
Программы сканирования



Перезапуск сети в Ubuntu



Мониторинг сети Linux



Настройка сети в Гномох

Оцените статью

(22 оценок, среднее: 4,50 из 5)

[Инструкции](#)

Об авторе



ADMIN

Основатель и администратор сайта losst.ru, увлекаюсь открытым программным обеспечением и операционной системой Linux. В качестве основной ОС сейчас использую Ubuntu. Кроме Linux, интересуюсь всем, что связано с информационными технологиями и современной наукой.

13 комментариев к “Как пользоваться Nmap для сканирования сети”



Alexander

27 ноября, 2016 в 6:03 pp

Каждый компьютер поддерживает протокол ping. Ping это утилита, а использует она протокол ICMP.

[Ответить](#)



Dmitry Paletsky

28 ноября, 2016 в 8:48 дп

Золотые слова 😊 безграмотность писателей умиляет

[Ответить](#)



Иван

28 ноября, 2016 в 5:50 дп

Мое почтение! Прошу еще ,по возможности, описать работу в Aircrack консольной версии для Линукс. а также работу с программами XHydra, Wireshark и Cain. Предполагаю, что эта информация для познавательных целей будет интересна и полезна не только мне.
Всем добра!

[Ответить](#)



Товарищ Капитан

29 ноября, 2016 в 11:25 дп

а Cain есть для линя?

[Privacy](#)

[Ответить](#)**Anton**28 ноября, 2016 в 9:56 дп

-sI - ленивое Idle сканирование, оно idle, насколько я помню, без п.

[Ответить](#)**nikotin10**3 марта, 2017 в 5:32 пп

Для nmap есть графический интерфейс, называется Zenmap.

[Ответить](#)**ivan**13 апреля, 2021 в 2:04 дп

почему у меня скрипт не запускается nmap --script ftp-brute.nse 192.168.1.1 -p 21

[Ответить](#)**Гость**14 апреля, 2021 в 8:16 дп

"Продолжайте экспериментировать с утилитой чтобы узнать больше только не в чужих сетях!" А если к примеру во время сканирования у меня открыт браузер и не один с кучей вкладок со страницами на разные сайты где смотрю новости и просто официальные сайты каких нибудь программ то открытые в этот момент сайты не зафиксируют запуск команды как попытку их сканировать? Прошу прощения за глупый вопрос. Как начинающий пользователь спрашиваю.

[Privacy](#)

[Ответить](#)[admin](#)[14 апреля, 2021 в 8:52 дп](#)

Они не зафиксируют сканирование только если их не сканировать. Какая разница что там открыто? Важно какие IP адреса сканирует программа.

[Ответить](#)[Trinidad](#)[21 апреля, 2021 в 5:25 пп](#)

Открыл в убунту 22 ssh порт, подключился, создал пользователя 'test' с паролем '123456789'. потом через бунту (по ssh подключению) просканил открытые порты у убудут (22 порт был открыт) после чего, будучи подключенным по ssh к убунту, выполнил эту команду:

```
nmap --script ssh-brute.nse 192.168.x.x -p 22 (вместо x стояли ip убунту).  
начался грубый перебор, там прописывается все варианты, которые скрипт попробовал, был вариант 'test:123456789', но скрипт просто пошел дальше...  
разве скрипт не нашел логин:пароль пользователя?  
всё это делал в локальной сети, убунту стоит на виртуалке. Может быть, дело в том, что я перебирал пароли с этого же сервера?
```

[Ответить](#)[Володя](#)[17 июня, 2023 в 8:47 пп](#)

Скорее всего там сработал таймаут, и программа не успел получить ответ об авторизации.

попробуйте покрутить доп.аргумент --script-args ssh.brute.timeout=4s

[Ответить](#)



AdVv

12 февраля, 2023 в 6:24 дп

Ключ -sL на самом деле ничего не сканирует. Он просто генерирует полный список всех хостов для данного диапазона адресов, для дальнейшей работы по нему. После чего просто завершает работу, доступность этих хостов не проверяется.

Ответить

Жека

29 декабря, 2023 в 1:17 дп

А правда, что Нео в фильме "Матрица", когда сидел за компом, то работал с nmap?

Ответить

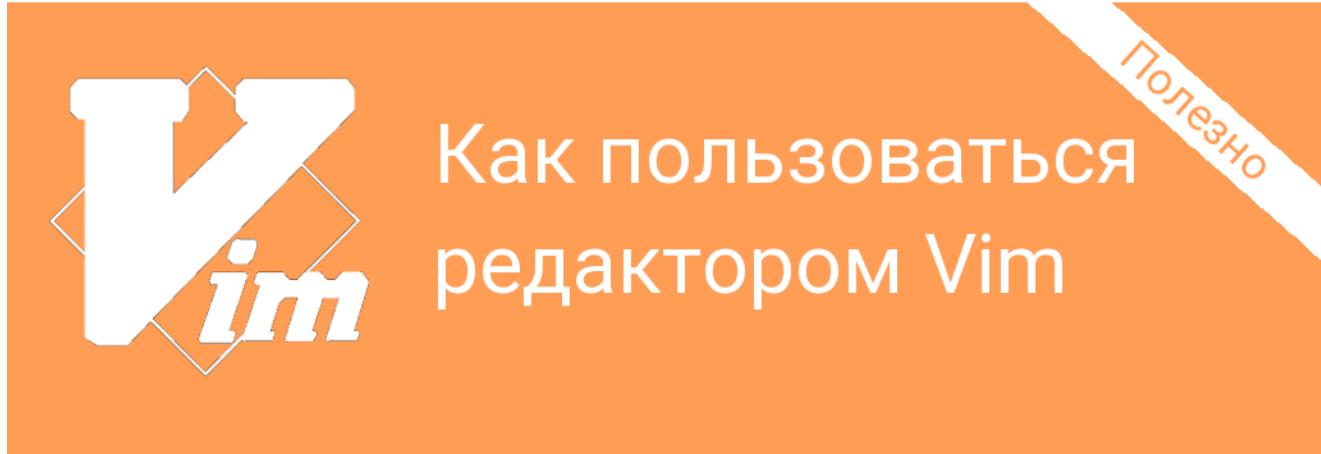
Оставьте комментарий

 Имя * Email

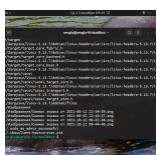
Я прочитал и принимаю политику конфиденциальности. Подробнее [Политика конфиденциальности](#) *

Privacy

[Комментировать](#)[Русский](#)[Поиск](#)[Поиск](#)[Privacy](#)

[Лучшие](#)[Свежие](#)[Теги](#)[Команда chmod в Linux](#)

2020-04-13

[Команда find в Linux](#)

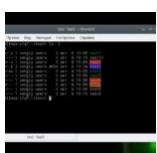
2021-10-17

[Как узнать IP-адрес в Linux](#)

2023-04-14

[Настройка Старт](#)

2021-10-01

[Права доступа к файлам в Linux](#)

2020-10-09

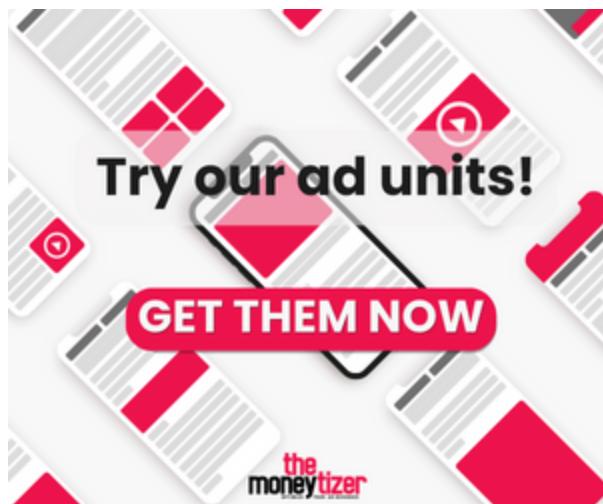
[Privacy](#)

РАССЫЛКА

Ваш E-Mail адрес

Я прочитал(а) и принимаю политику конфиденциальности

Sign up



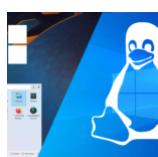
Windows

Списки



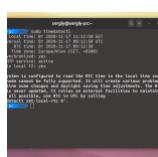
Восстановление Grub после установки Windows 10

2020-08-15



Установка Linux рядом с Windows 10 или 11

2023-02-08

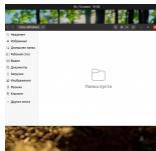


Сбивается время в Ubuntu и Windows

2023-02-18

Ошибка Ubuntu не видит сеть Windows

Privacy



2023-02-18

[Смотреть ещё](#)

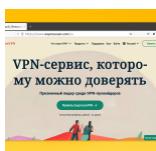
МЕТА

[Регистрация](#)[Войти](#)[Лента записей](#)[Лента комментариев](#)

СЛЕДИТЕ ЗА НАМИ В СОЦИАЛЬНЫХ СЕТЯХ



Интересное



Лучшие VPN сервисы для Linux

2022-10-10

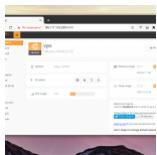


Privacy



Лучшие темы курсоров Linux

2020-12-18



Лучшие панели управления для Linux

2020-12-08



Шпаргалка по tmux

2021-10-01

©Losst 2024 CC-BY-SA [Политика конфиденциальности](#)



Privacy