

THE FAT-FREE GUIDE TO NETWORK SCANNING

# NMAP® COOKBOOK

Scanning Microsoft Windows 2003

Scanning Microsoft Windows Server 2003 SP1 or SP2

Discover 3 hosts

Discover 25+ Windows

BY NICHOLAS MARSH

Service detection performed. Please report any errors to nmap.org. Scan time: 0.09 seconds (1 host up) scanned in 0.09 seconds (1 port up) using sudo nmap -O -sV -n -F 10.10.1.46

Using Nmap 5.00 ( http://nmap.org ) at 2009-08-22 14:45 UTC

Scanning ports on 10.10.1.46:

22 closed ports

24 open ports (YMMV)

111/tcp 2.0.6

OpenSSL/4.3.1 Debian 3.0-stretch/2

Postfix/2.9.1

Apache/2.2.8 (Ubuntu)

OpenSSH/4.3.1p2

Microsoft-WebDAV-MiniShare/3.1.0.0 (Windows)

OpenNTPD/1.4.2

OpenNTPD/1.4.2

OpenNTPD/1.4.2

OpenNTPD/1.4.2

OpenNTPD/1.4.2

COVERS NMAP VERSION 5

Поваренная книга Nmap®

Краткое руководство по сетевому сканированию

Поваренная книга Nmap®

Руководство по сетевому сканированию без жира

Авторские права © Николас Марш, 2010. Все  
права защищены.

ISBN: 1449902529

EAN-13: 9781449902520

[www.NmapCookbook.com](http://www.NmapCookbook.com)

BSD® является зарегистрированной торговой маркой Калифорнийского университета в Беркли.

CentOS® является собственностью CentOS Ltd.

Debian® — зарегистрированная торговая марка компании Software in the Public Interest, Inc. Fedora® —  
зарегистрированная торговая марка Red Hat, Inc.

FreeBSD® — зарегистрированная торговая марка The FreeBSD Foundation Gentoo® —

зарегистрированная торговая марка The Gentoo Foundation Linux® — зарегистрированная

торговая марка Линуса Торвальдса. Mac OS X® — зарегистрированная

торговая марка Apple, Inc.

Windows® — зарегистрированная торговая марка корпорации Microsoft Nmap® —

зарегистрированная торговая марка Insecure.Com LLC. Red Hat® —

зарегистрированная торговая марка Red Hat, Inc.

Ubuntu® является зарегистрированной торговой маркой Canonical Ltd.

UNIX® является зарегистрированной торговой маркой The Open Group.

Все остальные товарные знаки, используемые в этой книге, являются собственностью соответствующих  
владельцев. Использование любого товарного знака в этой книге не означает присоединения или одобрения владельца  
товарного знака.

Вся информация в этой книге представлена «как есть». Никаких гарантий или гарантит не предоставляется, и  
автор/или издатель не несут ответственности за любые убытки или ущерб.



## Краткое содержание

Введение .....	15
Раздел 1: Установка Nmap.....	19
Раздел 2. Основные методы сканирования .....	33
Раздел 3: Параметры обнаружения .....	45
Раздел 4. Расширенные параметры сканирования .....	65
Раздел 5: Параметры сканирования портов.....	79
Раздел 6. Обнаружение операционной системы и служб.....	89
Раздел 7: Параметры времени .....	97
Раздел 8. Обход брандмаузов.....	115
Раздел 9: Параметры вывода.....	127
Раздел 10. Устранение неполадок и отладка.....	135
Раздел 11: Дзенмаг.....	147
Раздел 12: Механизм сценариев Nmap (NSE).....	161
Раздел 13: Ndif.....	171
Раздел 14: Советы и рекомендации.....	177
Приложение A – Шпаргалка по Nmap.....	187
Приложение B – Состояния портов Nmap.....	191
Приложение C. Перекрестная ссылка CIDR .....	193
Приложение D. Общие порты TCP/IP.....	195



# Оглавление

Введение.....	15
Условные обозначения, используемые в этой книге.....	18
Раздел 1: Установка Nmap.....	19
Обзор установки .....	20
Установка Nmap в Windows.....	21
Установка Nmap в системах Unix и Linux.....	25
Установка предварительно скомпилированных пакетов для Linux.....	25
Компиляция Nmap из исходного кода для Unix и Linux .....	26
Установка Nmap в Mac OS X.....	29
Раздел 2. Основные методы сканирования .....	33
Обзор базовых сканирования .....	34
Сканирование одной цели.....	35
Сканирование нескольких целей.....	36
Сканирование диапазона IP-адресов.....	37
Сканировать всю подсеть.....	38
Сканирование списка целей.....	39
Сканирование случайных целей.....	40
Исключение целей из сканирования .....	41
Исключение целей с помощью списка .....	42
Выполнение адресов сканирования .....	43
Сканирование цели IPv6.....	44
Раздел 3: Параметры обнаружения .....	45
Обзор параметров обнаружения .....	46
Не пинговать .....	47
Сканирование только с помощью Ping.....	48
TCP SYN-пинг .....	49
TCP ACK Ping.....	50
UDP-пинг .....	51
SCTP INIT Ping .....	52

ICMP-эх опинг .....	53
Пинг временной метки ICMP .....	54
Пинг маски адреса ICMP .....	55
Пинг IP-протокола .....	56
ARP-пинг .....	57
Трассировка.....	58
Принудительное обратное разрешение DNS.....	59
Отключить обратное разрешение DNS.....	60
Альтернативный метод поиска DNS.....	61
Укажите DNS-серверы вручную.....	62
Создание списков источников.....	63
<b>Раздел 4. Расширенные параметры сканирования .....</b>	<b>65</b>
Обзор расширенных функций сканирования .....	66
TCP SYN-сканирование .....	67
Сканирование TCP-соединения .....	68
UDP-сканирование .....	69
TCP NULL-сканирование.....	70
TCP FIN-сканирование.....	71
Рождественское сканирование.....	72
Пользовательское TCP-сканирование .....	73
Сканирование TCP ACK.....	74
Сканирование IP-протокола.....	75
Отправка необработанных пакетов Ethernet.....	76
Отправка IP-пакетов.....	77
<b>Раздел 5: Параметры сканирования портов.....</b>	<b>79</b>
Обзор опций сканирования портов.....	80
Выполните быстрое сканирование.....	81
Сканировать определенные порты.....	82
Сканировать порты по имени.....	83
Сканирование портов по протоколу .....	84

Сканировать все порты.....	85
Сканировать верхние порты.....	86
Выполнение последовательного сканирования портов .....	87
<b>Раздел 6. Обнаружение операционной системы и службы.....</b>	<b>89</b>
Обзор определения версии .....	90
Обнаружение операционной системы .....	91
Отправка отпечатков TCP/IP.....	92
Попытка угадать неизвестную операционную систему .....	93
Определение версии службы .....	94
Устранение неполадок при сканировании версий .....	95
Выполнение RPC-сканирования .....	96
<b>Раздел 7: Параметры времени .....</b>	<b>97</b>
Обзор параметров синхронизации .....	98
Временные параметры .....	99
Шаблоны синхронизации.....	100
Минимальное количество параллельных операций .....	101
Максимальное количество параллельных операций.....	102
Минимальный размер группы хостов.....	103
Максимальный размер группы хостов.....	104
Начальный таймаут RTT .....	105
Максимальный таймаут RTT .....	106
Минимальное количество повторов.....	107
Установите TTL пакета.....	108
Таймаут хоста.....	109
Минимальная задержка сканирования .....	110
Максимальная задержка сканирования .....	111
Минимальная склонность передачи пакетов.....	112
Максимальная склонность передачи пакетов.....	113
Преодоление сброса пределов склонности* .....	114

Раздел 8. Обход брандмаузеров.....	115
Обзор методов обхода брандмауэра.....	116
Фрагментированные пакеты.....	117
Укажите конкретный MTU.....	118
Используйте приманку.....	119
Сканирование зомби в режиме ожидания .....	120
Укажите номер исходного порта вручную.....	121
Добавить с лучайные данные.....	122
Случайный порядок сканирования цели.....	123
Подделка MAC-адреса.....	124
Отправка неверных контрольных сумм.....	125
Раздел 9: Параметры вывода.....	127
Обзор опций вывода .....	128
Сохранение вывода в текстовый файл.....	129
Сохранение вывода в XML-файл.....	130
Grepable-вывод.....	131
Вывод всех поддерживаемых типов файлов.....	132
Отображение статистики сканирования .....	133
133t Выход.....	134
Раздел 10. Устранение неполадок и отладка.....	135
Обзор устранения неполадок и отладки .....	136
Получать помощь .....	137
Отображение версии Nmap.....	138
Подробный вывод.....	139
Отладка .....	140
Отображение кодов причин состояния порта.....	141
Отображать только открытые порты.....	142
Трассировка пакетов.....	143
Отображение конфигурации с этикеткой .....	144
Укажите, какой сетевой интерфейс использовать .....	145

Раздел 11: Дзенмар.....	147
Обзор Zenmap.....	148
Запуск к Zenmap.....	149
Основные операции Zenmap.....	150
Результаты Zenmap.....	151
Сканирование профилей.....	152
Редактор профиля .....	153
Просмотр открытых портов.....	154
Просмотр карты сети .....	155
Сохранение карты сети.....	156
Просмотр сведений об хосте.....	157
Просмотр историй сканирования .....	158
Сравнение результатов сканирования .....	159
Сохранение сканов.....	160
Раздел 12: Скриптовый движок Nmap (NSE).....	161
Обзор скриптового движка Nmap.....	162
Выполнение отдельных скриптов.....	163
Выполнение нескольких скриптов .....	164
Каталог скриптов.....	165
Выполнение скриптов по каталогу.....	166
Выполнение нескольких каталогов скриптов.....	167
Устранение неполадок в скриптах .....	168
Обновить базу данных скриптов.....	169
Раздел 13: Ndiff .....	171
Обзор Ndiff .....	172
Сравнение сканов с использованием Ndiff.....	173
Подробный режим Ndiff.....	174
Режим вывода XML .....	175
Раздел 14: Советы и рекомендации.....	177
Обзор советов и рекомендаций .....	178

Объединение нес к ольких вариантов.....	179
Сканирование в интерактивном режиме.....	180
Взаимодействие во время выполнения .....	181
Удаленное сканирование вашей сети .....	182
Вайршарк .....	183
Scanme.Insecure.org .....	184
Онлайн-ресурсы Nmap.....	185
Приложение А – Шаги алгоритма Nmap.....	187
Приложение В – Состояния портов Nmap.....	191
Приложение С. Перекрестная ссылка CIDR .....	193
Приложение D. Общие порты TCP/IP.....	195

Это руководство посвящено собществу открытого исходного кода. Без неустанных усилий среди разработчиков открытого исходного кода таких программ, как Nmap, не существовало бы. Многие из этих разработчиков посвящают большую часть времени созданию поддержки замечательные приложения с открытым исходным кодом и ничего не просят взамен.

Совместная разработка программного обеспечения с открытым исходным кодом показывает истинный потенциал человечества, если мы все будем работать вместе для достижения общечеловеческих целей.



## Введение

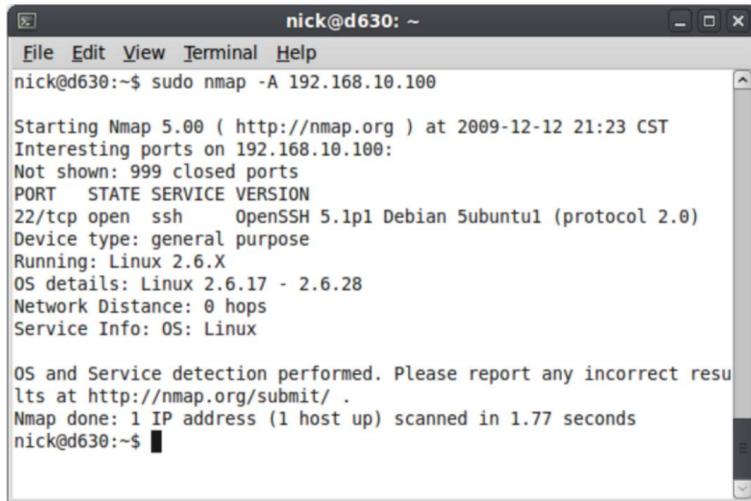
Nmap — программа с открытым исходным кодом, выпущенная под лицензией GNU General Public License.

(см. [www.gnu.org/copyleft/gpl.html](http://www.gnu.org/copyleft/gpl.html)). Этоочный инструмент для сети

администраторы, которых можно использовать для обнаружения, мониторинга и устранения неполадок TCP/IP.

системы. Nmap — бесплатная кроссплатформенная утилита сетевого сканирования, созданная Гардоном.

«Форд» Лион и активно развивается сообществом волонтеров.



```

nick@d630:~$ sudo nmap -A 192.168.10.100
Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-12 21:23 CST
Interesting ports on 192.168.10.100:
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.1p1 Debian 5ubuntu1 (protocol 2.0)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.28
Network Distance: 0 hops
Service Info: OS: Linux

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 1.77 seconds
nick@d630:~$ █

```

Типичное сканирование Nmap

Отмеченный набором утилит сетевого сканирования Nmap постоянно находится в развитии с 1997 года и постоянно совершенствуется с каждым новым выпуском. Версия

Версия Nmap 5.00 (выпущенная в июле 2009 г.) добавляет множество новых функций и улучшений.

включая:

- Улучшено определение версии службы и операционной системы (см. стр. 89).
- Улучшена поддержка Windows и Mac OS X.
- Улучшен механизм сценариев Nmap (NSE) для выполнения склонного сканирования задачи (см. стр. 161)
- Добавлено утилита Ndiff, которую можно использовать для сравнения сканов Nmap (см. стр. 171)

- Возможность графического отображения топологии сети с помощью Zenmap (см. стр. 147).
- Дополнительные языковые локализации, включая немецкий, французский и Португальский.
- Улучшение общей производительности

Проект Nmap полагается на волонтеров, которые поддерживают и развивают этот замечательный инструмент. Если вы хотите помочь улучшить Nmap, есть несколько способов принять в этом участие:

#### Продвигать Nmap

Nmap — замечательный инструмент, о котором должен знать каждый с твоей администрацией.

Несмотря на популярность, Nmap не так широко известен за пределами круга технической элиты.

Продвигайте Nmap, представьте его своим друзьям, или напишите о нем запись в блоге и

помогите распространить информацию

#### Сообщить об ошибках

Вы можете помочь улучшить Nmap, сообщая об обнаруженных вами ошибках в Nmap.

Разработчики. Проект Nmap предоставляет для этого список ошибок, который можно найти

онлайн по адресу [www.seclists.org/nmap-dev](http://www.seclists.org/nmap-dev).

#### Примечание

Тысячи людей по всему миру используют Nmap. Кроме того, разработчики Nmap очень заняты люди. Прежде чем сообщить об ошибке или обратиться за помощью вы следует выполнить поиск на веб-сайте Nmap по адресу [www.insecure.org/search.html](http://www.insecure.org/search.html), чтобы убедиться, что вашей проблеме еще не сообщалось и она не была решена.

#### Внести код

Если вы хакеры и у вас есть свободное время, вы можете принять участие в

разработке Nmap. Чтобы узнать больше о внесении кода в проект Nmap

посетите [www.nmap.org/data/HACKING](http://www.nmap.org/data/HACKING).

### Отправка отпечатков TCP/IP

Если вы не программист, вы все равно можете улучшить Nmap, отправив любые неизвестные отпечатки TCP/IP, которые вы обнаруживаете во время сканирования. Процесс этого обсуждается на стр. 92. Отправлять отпечатки пальцев легко, и это помогает улучшить программное обеспечение Nmap. Возможности определения версии и операционной системы. Посетите [www.nmap.org/submit/](http://www.nmap.org/submit/), для получения дополнительной информации или для представления своих открытий.

### Спонсор Nmap

Проект Nmap не принимает пожертвования. Однако если у вас есть ох рана спутствующая слуга, которую вы хотели бы продвигать, вы можете спонсировать Nmap, купив рекламный пакет на сайте [insecure.org](http://insecure.org). Для получения дополнительной информации посетите [www.insecure.org/advertising.html](http://www.insecure.org/advertising.html).

Условные обозначения, используемые в этой книге

C:\>nmap scanme.insecure.org

Nmap работает в системах Microsoft Windows

\$ nmap scanme.insecure.org

Nmap работает под не привилегированной учетной записью для Unix/Linux/Mac OS X

# nmap scanme.insecure.org

Nmap работает в системах Unix/Linux/Mac OS X от имени пользователя root.

\$ sudo nmap scanme.insecure.org

Использование команды sudo для повышения привилегий в Unix/Linux/Mac OS X

Примечание

Пользователи Windows могут открыть команду sudo, если она используется в примерах, например если оно используется не является необходиимо и не будет работать в системах на базе Microsoft.

# nmap -T2 scanme.insecure.org

Использование аргументов командной строки с Nmap

Важный

Аргументы командной строки Nmap чувствительны к регистру. Опция -T2 – (см. стр. 100) в приведенном выше примере не совпадает с -t2 и будет приведет к ошибке, если указан в неправильном регистре.

...

Дополнительные выходные данные Nmap усечены (для экономии места)

Секция 1:

Установка Нап

## Обзор установки

Nmap имеет свои корни в среде Unix и Linux, но в последнее время стал более совместим с операционной системой Microsoft Windows и Mac OS X от Apple. Система несмотря на то, что большое внимание уделяется тому, чтобы сделать Nmap универсальным для всех платформ, реальность такова, что вы можете столкнуться с ошибками, ошибками и снижением производительности. Проблемы при использовании Nmap в нетрадиционной системе. Это касается главным образом системы Windows и Mac OS X, имеющие различные особенности, которые не являются присущими в типичной системе Unix или Linux.

Примечание автора: порт Nmap для Windows значительно улучшился в версии Nmap 5.0.

Увеличение производительности и надежности делает Nmap для Windows таким же надежным, как и его Linuxковый аналог. К сожалению порт Mac OS все еще немногосыроват. Край. Многие проблемы с Nmap в Mac OS X возникают из-за проблем в операционной системе Apple. Последняя версия (Mac OS X 10.6). Наблюдая за списком разработчиков Nmap, я могу подтвердить, что разработчики знают об этих проблемах и работают над их решением. Эти проблемы, несомненно, будут решены со временем по мере разработки версии Nmap. 5.00 продолжается.

Пропустите процедуры установки для вашей платформы:

Установка Nmap в Windows

Страница 21

Установка Nmap в Linux

Страница 25

Установка Nmap из исходного кода (Unix и Linux) Страница 26

Установка Nmap в Mac OS X

Страница 29

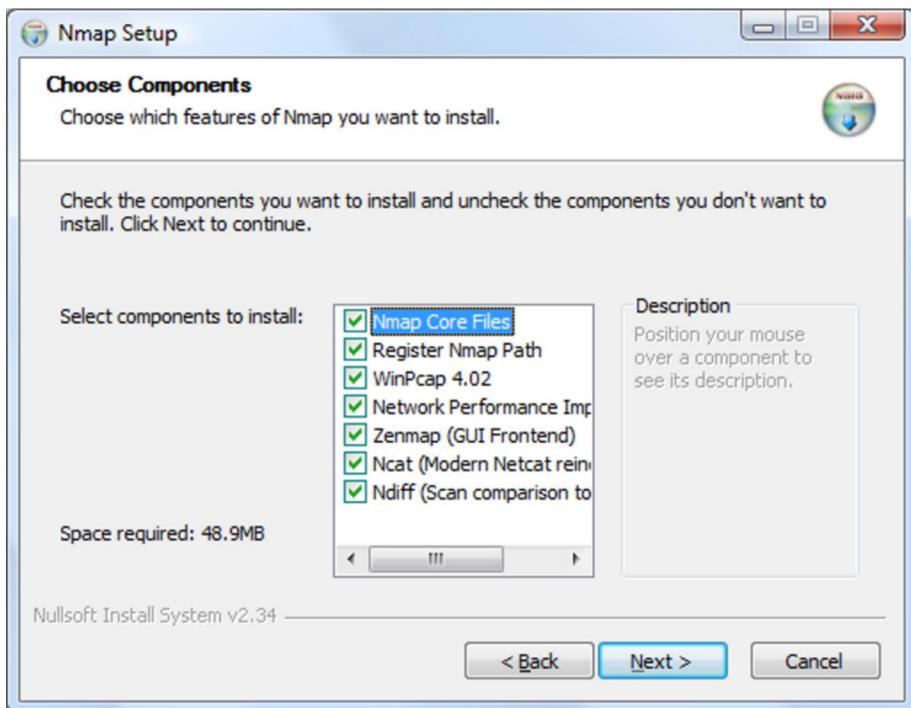
## Установка Nmap в Windows

### Шаг 1

Загрузите версию Nmap для Windows с сайта [www.nmap.org](http://www.nmap.org).

### Шаг 2

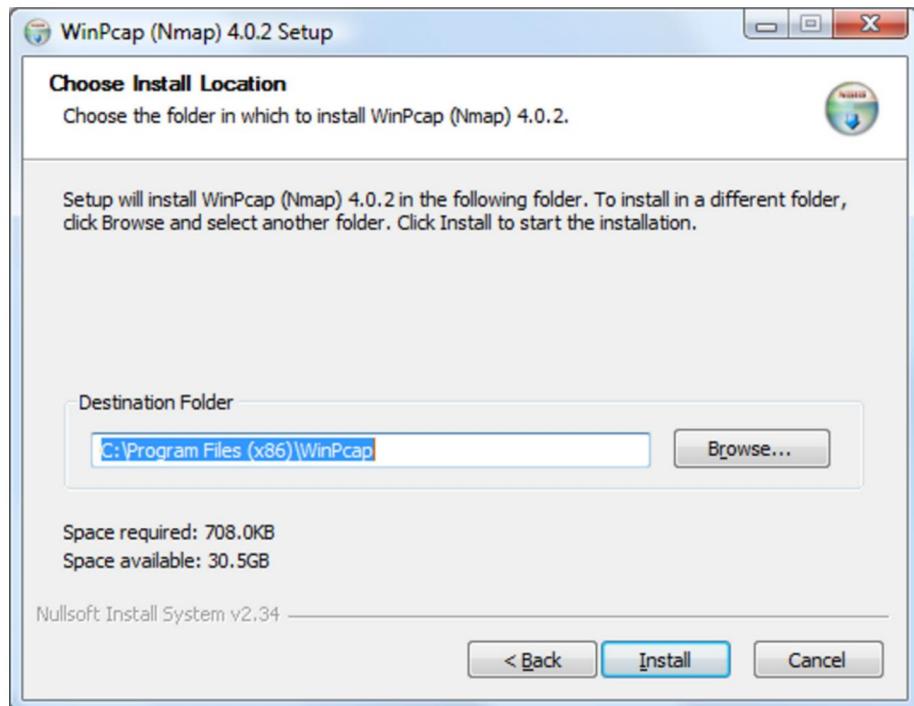
Запустите программу установки Nmap. Выберите установку по умолчанию (рекомендуется), который установит весь набор утилит Nmap.



Установщик Nmap для Windows

## Шаг 3

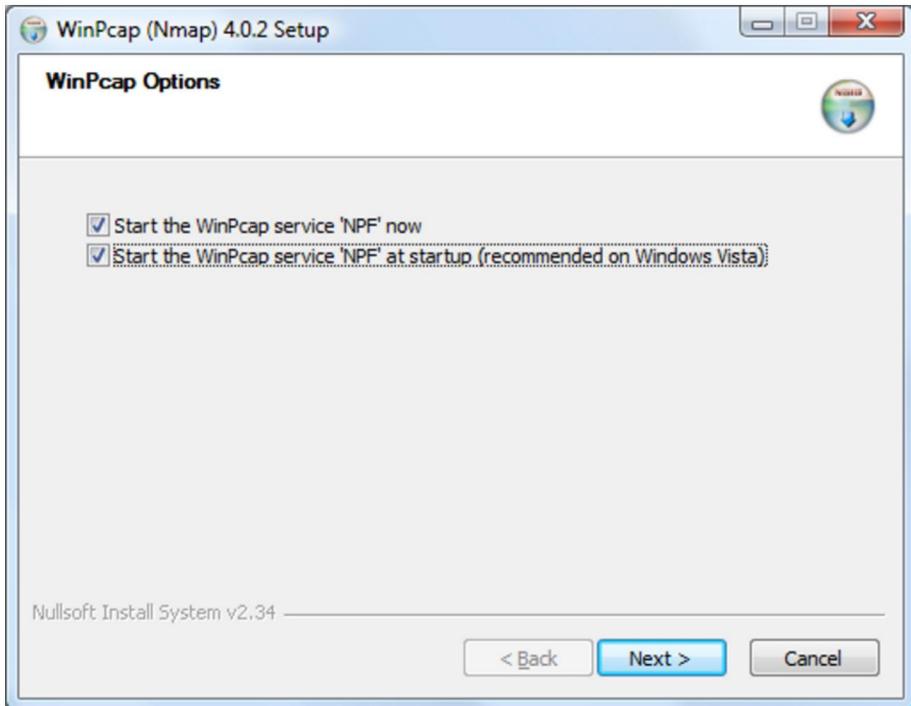
Во время установки также будет установлена вспомогательная программа WinPcap. WinPcap требуется для правильной работы Nmap на платформе Windows, поэтому не пропускайте этот шаг.



WinPcap для установщика Windows

## Шаг 4

После завершения установки WinPcap вам будет предоставлена возможность настроить его сервисные настройки. Параметры по умолчанию позволяют запустить службу WinPcap, когда загружается Windows. Это рекомендуется, поскольку Nmap не будет работать корректно, когда служба WinPcap не запущена.



Настройки WinPcap

## Шаг 5

Technet24.ir

После успешной установки Nmap вы можете убедиться, что он работает правильно, выполнив выполнение nmap scanme.insecure.org в командной строке (нажмите я в меню «Пуск» > Программы > Стандартные > Командная строка).

```
C:\>nmap scanme.insecure.org
```

```
Запуск Nmap 5.00 ( http://nmap.org ) в 2009-08-07 09:36 Central
```

```
Летнее время
```

```
Интересные порты на scanme.nmap.org (64.13.134.52):
```

```
Не показано: 994 отфильтрованных порта.
```

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

25/TCP	закрытый smtp
--------	---------------

70/TCP	закрытый cuse link
--------	--------------------

80/TCP	открыт http
--------	-------------

110/tcp	закрыт, pop3
---------	--------------

113/tcp	закрытая авторизация
---------	----------------------

31337/tcp	закрыт Элитный
-----------	----------------

```
Nmap выполнено 1 IP-адрес (1 хост работает) сканируется за 9,25 секунды.
```

```
C:\>
```

Тестовое сканирование Nmap в Microsoft Windows

Если результаты вашего сканирования аналогичны результатам, приведенным выше, значит, вы успешно установили Nmap. Если вы получили сообщение об ошибке, обратитесь к разделу 10 этой книги за информацией. Информация об установке неполадок и отладке.

## Установка Nmap в системах Unix и Linux

Большинство популярных дистрибутивов Linux предоставляют двоичные пакеты Nmap, которые позволяют простая установка. Для установки в системах Unix требуется компиляция Nmap из исходный код (как описано на стр. 26).

### Примечание

На момент написания этой статьи Nmap версии 5.00 не был доступен для автоматическая установка в некоторых дистрибутивах Linux. Для многих установка Nmap через популярные менеджеры пакетов apt или yum установит только версия 4.x. Если в вашем дистрибутиве уже есть Nmap 5.00 репозиториях вы можете установить Nmap, используя команды, перечисленные ниже.

В противном случае обратитесь к странице 26, чтобы установить Nmap 5.00 из исходного кода.

### Установка предварительно скомпилированных пакетов для Linux

Для систем на базе Debian и Ubuntu

```
# apt-get установить nmap
```

Для систем на базе Red Hat и Fedora

```
# ня м, установи nmap
```

Для систем на базе Gentoo Linux

```
# возникаем nmap
```

Чтобы проверить, какую версию Nmap вы используете, введите следующую команду:

командной строкой:

```
# nmap -V  
Nmap версии 5.00 (http://nmap.org)
```

## Компиляция Nmap из исходного кода для Unix и Linux

В настоящее время единственный способ получить Nmap 5.00 для большинства систем Unix и Linux — это скачать исходный код с сайта nmap.org. Создание Nmap из исходного кода требует немногодополнительной работы, но оно того стоит, чтобы получить новую версию функций в последней версии Nmap. Следующие пять шагов подробно описывают процедуру установки Nmap из исходников.

### Шаг 1

Загрузите исходный код Nmap 5.00 с сайта [www.nmap.org/download.html](http://www.nmap.org/download.html). Это может быть делается через стандартный веб-браузер или из командной строки с помощью wget.

Команда wget используется в большинстве систем на базе Unix.

```
$ wget http://nmap.org/dist/nmap-5.00.tgz
--2009-08-06 19:29:35-- http://nmap.org/dist/nmap-5.00.tgz
Разрешение nmap.org... 64.13.134.48
Подключение к nmap.org|64.13.134.48|:80... подключено.
HTTP-запрос отправлен, ожидается ответ... 200 OK
Длина: 9902346 (9,4M) [приложение/x-tar]
Сохраняется: 'nmap-5.00.tgz'.

100%[=====] 9 902 346 1,39 M/c за 7,5 с
2009-08-06 19:29:42 (1,27 МБ/с) - `nmap-5.00.tgz' сохранен
[9902346/9902346]
```

Загрузка Nmap в системах Unix и Linux через командную строку

### Шаг 2

Извлеките содержимое пакета Nmap, набрав tar -xf nmap-5.00.tgz.

```
$ tar -xf nmap-5.00.tgz
...
```

Извлечение исходного кода Nmap

## Шаг 3

Нас тройте и сберите исходный код Nmap, набрав cd nmap-5.00/, а затем  
./configure && make в командной строке.

```
$ cd nmap-5.00/  
$ ./configure && make  
проверка типа системы с борками... x86_64-unknown-linux-gnu  
проверка типа хоста-системы... x86_64-unknown-linux-gnu  
проверка gcc... gcc  
проверка имененных символов файла компилятора C по умолчанию.. a.out  
проверка, работает ли компилятор C... да  
...
```

Компиляция исходного кода Nmap

## Шаг 4

Установите скомпилированный код, набрав в командной строке sudo make install.

Примечание

Для этого шага потребуется привилегии root. Вы должны войти в систему как пользователь root или  
используйте команду sudo для завершения этого шага.

```
$ sudo make install  
Пароль: *****  
/usr/bin/install -c -d /usr/local/bin /usr/local/share/man/man1  
/usr/local/share/nmap  
/usr/bin/install -c -m 755 nmap /usr/local/bin/nmap  
/usr/bin/strips -x /usr/local/bin/nmap  
/usr/bin/install -c -c -m 644 docs/nmap.1 /usr/local/share/man/man1/  
/usr/bin/install -c -c -m 644 docs/nmap.xsl /usr/local/share/nmap/  
...  
NMAP УСПЕШНО УСТАНОВЛЕН  
$
```

Установка Nmap из исходного кода

## Шаг 5

После установки Nmap вы можете убедиться, что он работает правильно, выполнив выполнение nmap localhost в командной строке.

```
$ nmap локальный хост
Запуск Nmap 5.00 ( http://nmap.org ) в 2009-08-07, 00:42 CDT.
Предупреждение: имя хоста localhost разрешается в 2 IP-адреса. Использование 127.0.0.1.
Интересные порты на 127.0.0.1:
Не показано: 993 закрытых порта.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА
22/TCP открыть SSH
25/TCP открыть SMTP
111/tcp открыть rpcbind
139/tcp открыть netbios-ssn
445/TCP открыть Microsoft-DS
631/TCP открыть IPP
2049/tcp открыть nfc

Nmap выполнено 1 IP-адрес (1 хост работает) сканируется за 0,20 секунды.
```

Тестовое сканирование Nmap в Unix/Linux

Если результаты вашего сканирования аналогичны результатам, приведенным выше, значит, вы успешно установили Nmap. Если вы получили сообщение об ошибке, обратитесь к разделу 10 этой книги за информацией. Информация об установке и отладке.

## Установка Nmap в Mac OS X

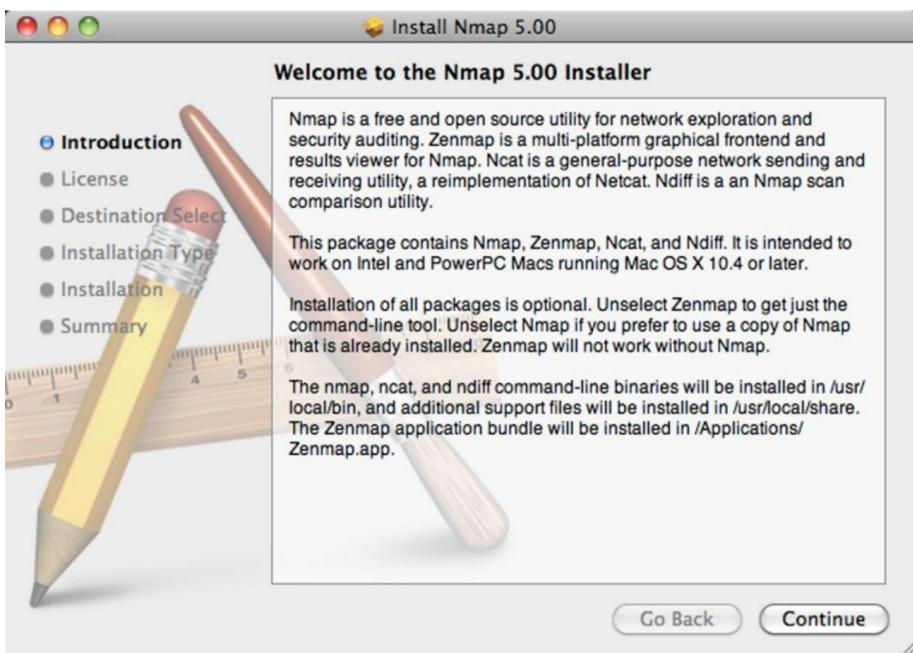
### Шаг 1

Загрузите версию Nmap для Mac OS X с сайта [www.nmap.org](http://www.nmap.org).

Примечание	Nmap 5.00 для Mac OS X — универсальный установщик, работающий как на Intel и системы PowerPC Macintosh.
------------	---

### Шаг 2

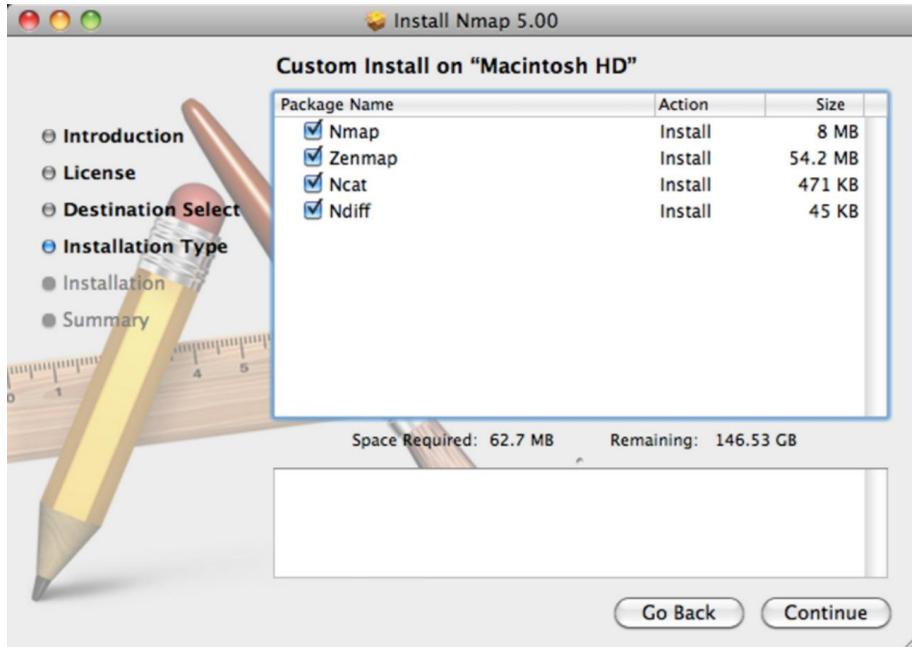
Запустите программу установки Nmap и нажмите «Продолжить». Затем примите условия лицензии программы Nmap.



Установщик Nmap для Mac OS X

### Шаг 3

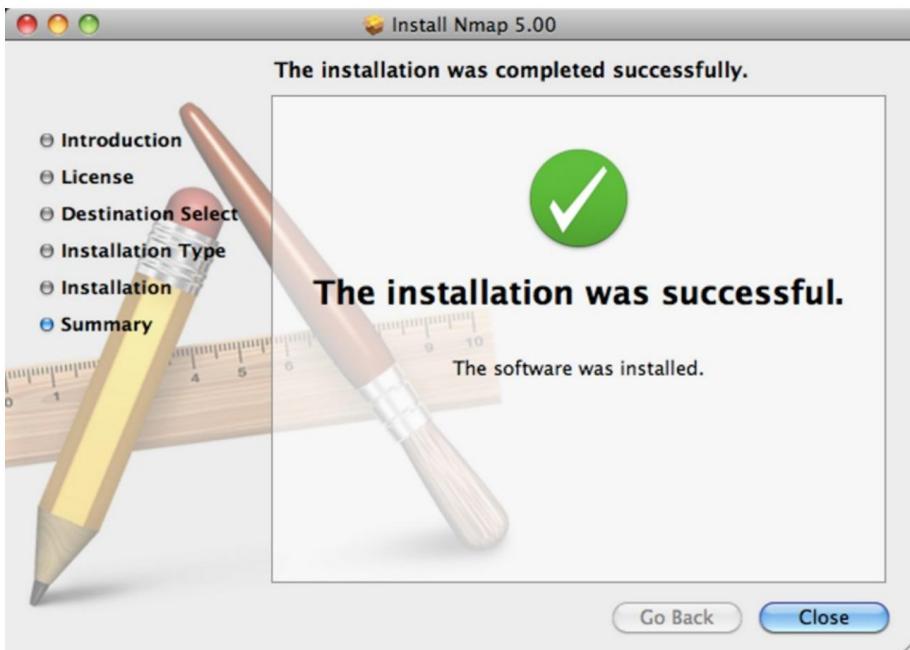
При появлении запроса на параметры установки установите выбранные по умолчанию значения отмеченными (рекомендуемые). Это установит весь набор утилит Nmap. Нажмите «Продолжить», чтобы начать процесс установки.



Параметры установки по умолчанию

## Шаг 4

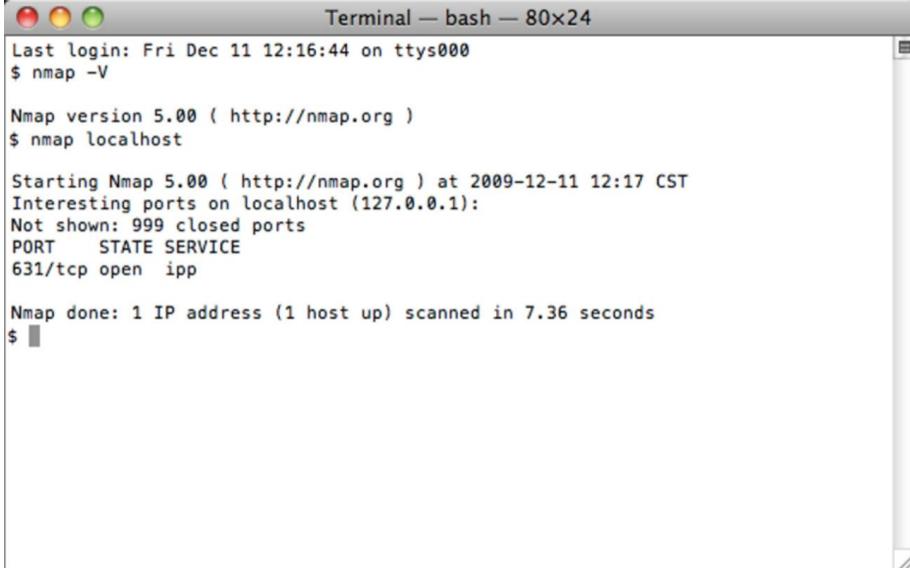
После завершения установки вы можете закрыть установщик Nmap.



Успешная установка Nmap на Mac OS X

## Шаг 5

После успешной установки Nmap вы можете убедиться, что он работает правильно, выполнив выполнение nmap localhost в приложении Mac OS X Terminal (находится в папке Приложения > Утилиты > Терминал).



```
Terminal — bash — 80x24
Last login: Fri Dec 11 12:16:44 on ttys000
$ nmap -V
Nmap version 5.00 ( http://nmap.org )
$ nmap localhost

Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-11 12:17 CST
Interesting ports on localhost (127.0.0.1):
Not shown: 999 closed ports
PORT      STATE SERVICE
631/tcp    open  ipp

Nmap done: 1 IP address (1 host up) scanned in 7.36 seconds
$
```

Тестовое сканирование Nmap в Mac OS X

Если результаты вашего сканирования аналогичны результатам, приведенным выше, значит, вы успешно установили Nmap. Если вы получили сообщение об ошибке, обратитесь к разделу 10 этой книги за информацией. Информация об установке и ошибках.

Раздел 2:

Основные методы с канирования

## Обзор базового сканирования

В этом разделе рассказывается о новых сетевых сканированиях с помощью Nmap. Прежде чем мы начнем, это важно понимать следующие понятия:

- Брандмауэры, маршрутизаторы, прокси-серверы и другие устройства безопасности могут исказить результаты сканирования Nmap. Сканирование удаленных хостов, которые не находятся на вашем локальном из-за этого есть может предоставлять вводя шум заблуждение информации.
- Некоторые параметры сканирования требуют повышенных привилегий. В Unix и Linux системах вам может потребоваться войти в систему как пользователь root или запустить Nmap, используя команду sudo.

Также следует принять во внимание несколько предупреждений:

- Сканирование сетей, на сканирование которых у вас нет разрешения, может проблемы с вашим интернет-провайдером, полицией и, возможно, даже правительство. Не переходите к сканированию веб-сайтов ФБР или Секретной службы, если только вы не хочете попасть в беду.
- Агрессивное сканирование некоторых систем может привести к их сбою что может привести к нежелательным результатам, таким как простой системы и потеря данных. Всегда сканировать критически важные системы с осторожностью.

Теперь приступим к сканированию!

## Сканировать одну цель

Запуск Nmap без параметров командной строки выполнит базовое сканирование указанной цели. Цель может быть указана как IP-адрес или имя хоста (которое Nmap попытается решить).

Синтаксис использования : nmap [цель]

```
$ nmap 192.168.10.1
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-07, 19:38 CDT.

Интересные порты на 192.168.10.1:

Найдено: 997 отфильтрованных портов.

ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА

20/tcp закрыты ftp-данные

21/TCP закрытый FTP

80/tcp открыт http

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 7,21 секунды.

Сканирование одной цели

Результат сканирования показывает состояние портов, обнаруженных на указанной цели.

В таблице ниже описания поля вывода, отображаемые при сканировании.

ПОРТ	СОСТОЯНИЕ	УСЛУГА
Номер порта/протокол	Статус порта	Тип услуги для порта

Сканирование Nmap по умолчанию проверит 1000 наиболее часто используемых портов TCP/IP.

Порты, реагирующие на запрос, классифицируются по одному из шести состояний порта: открытый, закрытый, фильтрованный, нефильтрованный, открытый фильтрованный, закрытый фильтрованный. Дополнительную информацию см. в Приложении B. Информация о государствах порта.

## Сканировать несолько целей

Nmap можно использовать для одновременного сканирования нескольких хостов. Самый простой способ сделать это значит объединить целевые IP-адреса или имена хостов в командной строке.

(через пробел).

Синтаксис использования : nmap [цель1 цель2 и т. д.]

```
$ nmap 192.168.10.1 192.168.10.100 192.168.10.101
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-07, 20:30 CDT.

Интересные порты на 192.168.10.1:

Не показано: 997 отфильтрованных портов.

ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА

20/tcp закрыты ftp-данные

21/TCP закрытый FTP

80/tcp открыть http

Интересные порты на 192.168.10.100:

Не показано: 995 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

22/TCP открыть SSH

111/tcp открыть rpcbind

139/tcp открыть netbios-ssn

445/TCP открыть Microsoft-DS

2049/tcp открыть nfc

Nmap готово: 3 IP-адреса (2 хоста подключены) сканированы за 6,23 секунды.

Сканирование нескольких целей

В приведенном выше примере показано использование Nmap для одновременного сканирования трех адресов.

время .

Кончик

Поскольку все три цели в приведенном выше примере находятся в одной подсети, вы можете использовать сокращенную запись nmap 192.168.10.1,100,101 для добиться тех же результатов.

## Сканировать диапазон IP-адресов

Для спецификаций или если можно использовать диапазон IP-адресов, как показано в пример ниже.

Синтаксис использования : nmap [диапазон IP-адресов]

```
$ nmap 192.168.10.1-100
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-07, 20:40 CDT.

Интересные порты на 192.168.10.1:

Не показано: 997 отфильтрованных портов.

ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА

20/tcp закрыты ftp-данные

21/TCP закрытый FTP

80/tcp открыть http

Интересные порты на 192.168.10.100:

Не показано: 995 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

22/TCP открыть SSH

111/tcp открыть rpcbind

139/tcp открыть netbios-ssn

445/TCP открыть Microsoft-DS

Nmap готово: 100 IP-адресов (2 хоста) сканируются за 25,84 секунды.

### Сканирование диапазона IP-адресов

В этом примере Nmap поручено сканировать диапазон IP-адресов из

От 192.168.10.1 до 192.168.10.100. Вы также можете использовать диапазоны для сканирования нескольких сетей/подсети. Например, ввод nmap 192.168.1-100.\* приведет к сканированию всех с IP-сети от 192.168.1.\* до 192.168.100.\*.

#### Примечание

Звездочка — это подстановочный знак, обозначающий все допустимые диапазоны от 0-255.

## Сканировать все подсети есть

Nmap можно использовать для сканирования всей подсети с использованием CIDR (бесклассовый междоменный маска).  
Маршрутизация).

Синтаксис использования : nmap [Сеть/CIDR]

```
$ nmap 192.168.10.1/24
```

Запуск Nmap 5.00 (http://nmap.org) в 2009-08-07, 20:43 CDT.

Интересные порты на 192.168.10.1:

Не показано: 996 отфильтрованных портов.

ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА

20/tcp закрыты ftp-данные

21/TCP закрытый FTP

23/tcp закрытый телнет

80/tcp открыть http

Интересные порты на 192.168.10.100:

Не показано: 995 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

22/TCP открыть SSH

111/tcp открыть rpcbind

139/tcp открыть netbios-ssn

445/TCP открыть Microsoft-DS

2049/tcp открыть nfc

Nmap готово: 256 IP-адресов (2 хоста) сканируются за 8,78 секунды.

Сканирование всей подсети класса C с использованием маски CIDR

В приведенном выше примере Nmap сканирует всю сеть 192.168.10.0, используя

Обозначение CIDR. Маска CIDR состоит из сетевого адреса и маски подсети (в двоичные биты), разделенные косой чертой. См. Приложение С для перекрестной ссылки на подсеть. маски и их обозначения CIDR.

## Сканирование списка целей

Если вам нужно сканировать большое количество систем, вы можете ввести IP-адрес (или хост-имена) в текстовый файл и используйте этот файл в качестве входных данных для Nmap в командной строке.

```
$ cat список.txt
192.168.10.1
192.168.10.100
192.168.10.101
```

Целевые IP-адреса в текстовом файле

Файл list.txt, приведенный выше, содержит списки хостов, подлежащих сканированию. Каждая запись в list.txt файле должен быть разделен пробелом, табуляцией или новой строкой. Параметр -iL используется для поручите Nmap извлечь список целей из файла list.txt.

Синтаксис использования : nmap -iL [list.txt]

```
$ nmap -iL list.txt
Запуск Nmap 5.00 (http://nmap.org) в 2009-08-07, 19:44 CDT.
Интересные порты на 192.168.10.1:
Не показано: 997 отфильтрованных портов.
ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА
20/tcp закрыты ftp-данные
21/TCP закрытый FTP
80/tcp открыт http
```

Интересные порты на 192.168.10.100:

Не показано: 995 закрытых портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

22/TCP открыт SSH

...

Сканирование Nmap с использованием списка целевой с пакетификацией

Результат сканирования, показанный выше, будет выполнен для каждого хоста в файле list.txt.

## Сканировать с случайные цели

Параметр -iR можно использовать для выбора с случайных интернет-адресов для сканирования. Nmap будет с случайным образом сгенерировать указанное количество целей и попытайтесь их просканировать.

Синтаксис использования : nmap -iR [количество целей]

```
# nmap -iR 3  
Запуск Nmap 5.00 (http://nmap.org) в 2009-08-07, 23:40 CDT.
```

...

```
Nmap выполнено: 3 IP-адреса (2 хоста подключены) просканированы за 36,91 секунды.
```

Сканирование трех с случайно сгенерированных IP-адресов

### Примечание

Последование конфиденциальности мы не показываем результаты вышеуказанных сканирования в этом документе.

Книга

Выполнение nmap -iR 3 дает указание Nmap с случайным образом сгенерировать 3 IP-адреса для сканирования.

Не так уж много веских причин когда либо выполнять с случайное сканирование, если вы не работаете.

Надеюсь следовательским проектом (или просто очень скучно). Кроме того, если вы совершаете многоагрессивных действий

с случайное сканирование, у вас могут возникнуть проблемы с интернет-сервисом

провайдер.

## Исключить цели из сканирования

Опция `--exclude` используется с Nmap для исключения хостов из сканирования.

Синтаксис использования : nmap [цели] `--exclude` [цель(и)]

```
$ nmap 192.168.10.0/24 --исключить 192.168.10.100
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-08, 20:39 CDT.

Интересные порты на 192.168.10.1:

Не показано: 996 отфильтрованных портов.

ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА

20/tcp закрытые ftp-данные

21/TCP закрытый FTP

23/tcp закрытый телнет

80/tcp открыт http

...

Исключение одного IP-адреса из сканирования

Опция `--exclude` полезна, если вы хотите исключить определенные хосты при сканировании

большое количество адресов. В приведенном выше примере исключен хост 192.168.10.100.

от дальности сканируемых целей.

Опция `--exclude` принимает отдельные хосты, диапазоны или целевые сетевые блоки (используя

нотацию CIDR), как показано в следующем примере.

```
$ nmap 192.168.10.0/24 --исключить 192.168.10.100-105
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-08, 20:39 CDT.

...

Исключение диапазона IP-адресов из сканирования

## ИС КЛЮЧИТЬ Ц ЕЛИ С ПОМОЩЬЮ ПИСКА

Параметр `--excludefile` аналогичен параметру `--exclude` и может использоваться для предстavить с писок целей, которые следует исключить из сканирования сети.

```
$ КОТ С ПИСОК.txt  
192.168.10.1  
192.168.10.12  
192.168.10.44
```

Текстовый файл с хостами, которые нужно исключить из сканирования

В приведенном ниже примере показано использование аргумента `--excludefile` для исключения хосты в файле `list.txt`, показанном выше.

Синтаксис использования : nmap [цели] `--excludefile` [`list.txt`]

```
$ nmap 192.168.10.0/24 --excludefile list.txt
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-08, 20:49 CDT.

Интересные порты на 192.168.10.100:

Не показано: 995 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

22/TCP открыть SSH

111/tcp открыть rpcbind

139/tcp открыть netbios-ssn

445/TCP открыть Microsoft-DS

2049/tcp открыть nfs

Nmap выполнено: 253 IP-адреса (1 хост открыт) сканируются за 33,10 секунды.

Исключение с писок хостов из сканирования сети

В приведенном выше примере цели в файле `list.txt` исключены из сканирования .

## Выполните аг рес с ивное с канирование

Параметр -A указывает Nmap выполнить аг рес с ивное с канирование.

Синтаксис использования : nmap -A [цель]

```
# nmap -A 10.10.1.51
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-10, 09:39 CDT.

Интересные порты на 10.10.1.51:

Не показано: 999 закрытых портов.

Версия государственной службы порта

80/tcp открыт http http-конфигурация маршрутизатора Wireless-G Linksys WAP54G

|\_ html-title: 401 Несанкционированный

| http-auth: служба HTTP требует аутентификации.

| Тип аутентификации: базовый, область = Linksys WAP54G

MAC-адрес : 00:12:17:AA:66:28 (Cisco-Linksys)

Тип устройства: общего назначения

Работает: Linux 2.4.X

Сведения об ОС: Linux 2.4.18-2.4.35 (вероятно, встроенная)

Расстояние сети: 1 переход

Информация об услуге: Устройство: WAP

Обнаружение ОС и службы выполнено. Пожалуйста, сообщите о любых неправильных результатов на <http://nmap.org/submit/>.

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 9,61 секунды.

Результат аг рес с ивного сканирования

Агрессивное сканирование выбирает некоторые из наиболее частотно используемых опций в Nmap.

и представляется как простая альтернатива вводу длинной строки командной строки.

аргументы. Параметр -A является синонимом нескольких дополнительных параметров (например, -O -sC

--traceroute), к которым также можно получить доступ индивидуально и которые будут рассмотрены позже в этом документе.

Книга.

## Сканировать цель IPv6

Параметр -6 ис пользуется для сканирования цели IP версии 6.

Синтаксис использования : nmap -6 [цель]

```
# nmap -6 fe80::29aa:9db9:4164:d80e
```

Запуск Nmap 5.00 ( http://nmap.org ) в 2009-08-11 15:52 Central

Летнее время

Интересные порты на fe80::29aa:9db9:4164:d80e:

Не показано: 993 закрытых порта.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

135/tcp открыть msrpc

445/TCP открыть Microsoft-DS

5357/tcp открыт неизвестно

49152/tcp открыт неизвестно

49153/tcp открыт неизвестно

49154/tcp открыт неизвестно

49155/tcp открыт неизвестно

Nmap выполнено: 1 IP-адрес (1 x ост работает) сканируется за 227,32 секунды.

Сканирование IPv6-адреса

В приведенном выше примере показаны результаты сканирования цели IP версии 6. Большинство

Параметры Nmap поддерживают IPv6, за исключением сканирования нескольких целей с использованием

диапазоны и CIDR, поскольку они бес смыслены в сетях IPv6.

Примечание

Их система, и целями систе должны поддерживать протокол IPv6.

чтобы сканирование -6 работало.

Раздел 3:

Параметры обнаружения

## Обзор параметров обнаружения

[Technet24.ir](#)

Прежде чем сканировать порт цели, Nmap попытается отправить эх-запросы ICMP, чтобы увидеть если хост «жив». Это может сэкономить время при сканировании нескольких хостов, поскольку Nmap не тратит время на попытки проверить хосты, которые не подключены к сети. Поэтому что ICMP-запросы часто блокируются брандмауэрами, Nmap также попытается подключиться к порту 80 и 443, поскольку эти общие порты веб-сервера часто открыты (даже если ICMP нет).

Параметры обнаружения по умолчанию полезны при сканировании защищенных систем могут предпринять для тестирования сканирования. В следующем разделе описаны альтернативные методы обнаружения хоста, которое позволяет выполнять более полное обнаружение, когда имеются достаточно тугие цели.

Краткое описание функций, описанных в этом разделе:

Особенность	Вариант
Не пинговать	-PN
Выполните сканирование только с помощью Ping	-SP
TCP SYN-пинг	-PS
TCP ACK-пинг	-X флаг
UDP-пинг	-MOG
SCTP-инциализирующий пинг	-LJ
ICMP-эхопинг	-NA
Проверка метки времени ICMP	-TP
Пинг маски адреса ICMP	-BЕЧЕРА
Пинг IP-протокола	-ПОСЛЕ
ARP-пинг	-ниар
Трассировка	--traceroute
Принудительное обратное разрешение DNS	-Р
Отключить обратное разрешение DNS	-Н
Альтернативный поиск DNS	--system-dns
Укажите DNS-серверы вручную	--dns-серверы
Создать список хостов	-с Л

## Не пинговать

По умолчанию прежде чем Nmap попытается просканировать систему на наличие открытых портов, она сначала пингует цель, чтобы узнать, находятся ли она в сети. Этап сканирования помогает сэкономить время при сканировании, поскольку приводит к пропуску целей, которые не отвечают.

```
$ nmap 10.10.5.11
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-13, 08:43 CDT.

Примечание. Кажется, хост не работает. Если он действительно работает, но блокирует наш пинг-зонды, попробуйте -PN.

Nmap выполнено: 1 IP-адрес (0 хостов работает) сканируется за 3,16 секунды.

Результаты сканирования Nmap, когда целевая система не отвечает на

Пинг и Nmap. Опция -PN указывает Nmap пропустить проверку обнаружения по умолчанию и выполните полное сканирование портов на цели. Это полезно при сканировании хостов, которые защищены брандмауэром, который блокирует пинг-зонды.

Синтаксис использования : nmap -PN [цель]

```
$ nmap -PN 10.10.5.11
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-13, 08:43 CDT.

Интересные порты на 10.10.5.11:

Не показано: 999 отфильтрованных портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

3389/TCP открыть MS-Term-Serv

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 6,51 секунды.

Выход сканирования Nmap с отключенным обнаружением ping

Указав опцию -PN для той же цели, Nmap может сканировать с исключением

открытые порты в непроверенной системе.

Сканирование только с помощью ping

Опция `-sP` ис пользуется для выполнения простой проверки связи с указанным хостом.

Синтаксис использования : nmap -sP [цель]

```
$ nmap -sP 192.168.10.2/24
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-08, 20:54 CDT.

Хост 192.168.10.1 работает (задержка 0,0026 с).

Хост 192.168.10.100 работает (задержка 0,00020 с).

Хост 192.168.10.101 работает (задержка 0,00026 с).

Nmap готово: 256 IP-адресов (3 хоста) сканируются за 3,18 секунды.

Выход сканирования только с помощью ping

Эта опция полезна, если вы хотите выполнить быстрый поиск целевой сети.

Чтобы увидеть, какие хосты находятся в сети, без фактического сканирования цели (целей) на наличие открытых портов.

В приведенном выше примере все 254 адреса в подсети 192.168.10.0 проверяются и

отображаются результаты с живых хостов.

При сканировании локальной сети вы можете запустить Nmap с правами root для

дополнительная функция проверки связи. При этом опция `-sP` выполнит ARP.

пропингуйте и верните MAC-адреса обнаруженных систем.

Синтаксис использования : nmap -sP [цель]

```
# nmap -sP 192.168.10.2/24
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-08 21:00 CDT.

Хост 192.168.10.1 работает (задержка 0,0037 с).

MAC-адрес : 00:16:B6:BE:6D:1D (Cisco-Linksys)

...

Выход сканирования только ping (от имени пользователя root)

## TCP SYN-пинг

Опция `-PS` выполняет проверку с помощью TCP SYN.

Синтаксис использования : `nmap -PS[порт1,порт2 и т. д.] [цель]`

```
# nmap -PS scanme.insecure.org
```

Запуск Nmap 5.00 (http://nmap.org) в 2009-08-16 13:31 CDT.

Интересные порты на `scanme.nmap.org` (64.13.134.52):

Но показано: 995 отфильтрованных портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
53/TCP	открытый домен
70/TCP	закрытый сурслик
80/TCP	открыть http
113/tcp	закрытая авторизация
31337/tcp	закрыт Элитный

Nmap выполнено: 1 IP-адрес (1 x остановлен) просканирован за 27,41 секунды.

Выполнение TCP SYN-пинга

Пинг TCP SYN отправляет пакет SYN в целяющую систему и ожидает ответа.

Этот альтернативный метод обнаружения полезен для систем, настроенных на блокировку стандартные ICMP-пинги.

Примечание

Порт по умолчанию для `-PS` — 80, но другие можно указать с помощью параметра следующий синтаксис: `nmap -PS22,25,80,443 и т. д.`

## TCP ACK-пинг

-PA выполняет проверку связи TCP ACK для указанной цели.

Синтаксис использования : nmap -PA[порт1,порт1 и т. д.] [цель]

```
# nmap -PON 192.168.1.254
```

Запуск Nmap 5.00 (http://nmap.org) в 2009-08-16 13:31 CDT.

Интересные порты на домашнем (192.168.1.254):

Не показано: 998 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

80/tcp открыть http

443/TCP открыть https

MAC-адрес : 00:25:3C:5F:5A:89 (2-проводной)

Nmap выполнено: 1 IP-адрес (1 x осто работает) сканируется за 0,81 секунды.

Выполнение TCP ACK ping

Опция -PA заставляет Nmap отправлять пакеты TCP ACK указанным хостам. Этот метод пытается обнаружить хости, отвечающие на TCP-соединения, которые отсутствуют в попытке добиться ответа от цели. Как и другие пинги опции, это полезно в ситуациях, когда другие стандартные пинг и ICMP блокируются.

### Примечание

Порт по умолчанию для -PA — 80, но другие можно указать с помощью следующий синтаксис: nmap -PA22,25,80,443 и т. д.

## UDP-пинг

Опция -PU выполняет проверку связи UDP в целевой системе.

Синтаксис использования : nmap -PU[порт1,порт2 и т. д] [цель]

```
# nmap -PU 192.168.1.254
```

```
Запуск Nmap 5.00 ( http://nmap.org ) 16 авг уста 2009 г., 13:30 CDT.
```

```
Интересные порты на домашнем (192.168.1.254):
```

```
Не показано: 998 закрытых портов.
```

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
80/tcp	открыть http
443/TCP	открыть https

```
Nmap выполнено 1 IP-адрес (1 хост работает) сканируется за 0,81 секунды.
```

Выполнение UDP-пинга

Этот метод обнаружения отправляет пакеты UDP в попытке запросить ответ от цели. Хотя большинство систем с межсетевым экраном блокируют этот тип соединения, некоторые плохонячие системы могут позволить это, если они настроены только на фильтрацию TCP связи.

Примечание

Порт по умолчанию для -PU — 40125. Остальные можно указать с помощью следующий синтаксис: nmap -PU22,25,80,443 и т. д

SCTP-инициализирующий пинг

Параметр -PY указывает Nmap выполнить пинг SCTP INIT.

Синтаксис использования : nmap -PY[порт1,порт1 и т. д.] [цель]

```
# nmap -PY 192.168.1.254
```

Запуск к Nmap 5.00 (<http://nmap.org>) в 2009-08-16, 13:28 CDT.

Интересные порты на домашнем (192.168.1.254):

Не показано: 998 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

80/tcp открыть http

443/TCP открыть https

MAC-адрес : 00:25:3C:5F:5A:89 (2-проводной)

Nmap выполнено: 1 IP-адрес (1 x открыт) сканируется за 0,79 секунды.

Выполнение SCTP INIT ping

Этот метод обнаружения пытается найти хосты с помощью Stream Control.

Протокол передачи (SCTP). SCTP обычно используется в системах на базе IP.

телефония .

Примечание

Порт по умолчанию для -PY — 80. Другие можно указать с помощью следующий синтаксис : nmap -PY22,25,80,443 и т. д.

## ICMP-ЭХ О-ПИНГ

Опция -PE выполняет эх опинг ICMP (протокол управления с общим Интернетом) на указанную систему.

Синтаксис использования : nmap -PE [цель]

```
# nmap -PE 192.168.1.254
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-16, 13:26 CDT.

Интересные порты на домашнем (192.168.1.254):

Не показано: 998 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

80/tcp открыть http

443/TCP открыть https

MAC-адрес : 00:25:3C:5F:5A:89 (2-проводной)

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 1,89 секунды.

Выполнение эх опинга ICMP

Опция -PE отправляет стандартный ICMP-пинг цели, чтобы проверить, отвечает ли она. Этот тип обнаружения лучше всего работает в локальных сетях, где могут передаваться пакеты ICMP с небольшими ограничениями. Однако многие интернет-хосты настроены не отвечать на ICMP-пакеты по соображениям безопасности.

### Примечание

Опция -PE автоматически подразумевается, если нет других опций ping.  
указано.

## Проверка метки времени ICMP

Опция -PP выполняет проверку связи с меткой времени ICMP.

Синтаксис использования : nmap -PP [цель]

```
# nmap -PP 192.168.1.254
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-16, 13:27 CDT.

Интересные порты на домашнем (192.168.1.254):

Не показано: 998 закрытых портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
80/tcp	открыть http
443/TCP	открыть https

Nmap выполнено 1 IP-адрес (1 x осталось работает) сканируется за 1,83 секунды.

Выполнение проверки метки времени ICMP

Хотя большинство систем с межсетевым экраном настроены на блокировку этих запросов ICMP, некоторые неправильно настроенные системы могут по-прежнему отвечать на запросы временных меток ICMP. Этот делает -PP полезным для попыток получить ответы от целей, защищенных брандмаузером.

## Пинг маски адреса ICMP

Опция -PM выполняет проверку связи по маске адреса ICMP.

Синтаксис использования : nmap -PM [цель]

```
# nmap -PM 192.168.1.254
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-16, 13:26 CDT.

Интересные порты на домашнем (192.168.1.254):

Не показано: 998 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

80/tcp открыть http

443/TCP открыть https

MAC-адрес : 00:25:3C:5F:5A:89 (2-проводной)

Nmap выполнено: 1 IP-адрес (1 x остается) сканируется за 1,92 секунды.

Выполнение проверки связи по маске адреса ICMP

Этот нетрадиционный ICMP-запрос (похожий на опцию -PR) пытается проверить связь с указанным хостом с использованием альтернативных регистров ICMP. Этот тип пинга иногда может проскользнуть мимо брандмауэра, настроенного на блокировку стандартных echo-запросов.

## Пинг IP-протокола

[Technet24.ir](#)

Опция -РО выполняет проверку связи по протоколу IP.

Синтаксис использования : nmap -РО[протокол1,протокол2 и т. д.] [цель]

```
# nmap -PO 10.10.1.48
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-17, 09:38 CDT.

Интересные порты на 10.10.1.48:

Не показано: 994 закрытых порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
21/TCP открытый FTP	
22/TCP открыть SSH	
25/TCP открыть SMTP	
80/tcp открыть http	
111/tcp открыть rpcbind	
2049/tcp открыть нfc	
MAC-адрес : 00:0C:29:D5:38:F4 (VMware)	

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 1,97 секунды.

Выполнение проверки связи по IP-протоколу

Пинг протокола IP отправляет пакеты с указанным протоколом в цель. Если нет

протоколы указаны, протоколы по умолчанию 1 (ICMP), 2 (IGMP) и 4 (IP-in-IP).

использовал. Чтобы выполнить проверку связи с использованием специального набора протоколов, используйте следующий синтаксис:

nmap -РО1,2,4 и т. д.

Примечание

Полный список номеров интернет-протокола можно найти в Интернете по адресу:

[www.iana.org/assignments/protocol-numbers/](http://www.iana.org/assignments/protocol-numbers/)

## ARP-пинг

Опция -PR указывает Nmap выполнить ARP (протокол разрешения адресов).

Пинг наукающийся.

Синтаксис использования : nmap -PR [цель]

```
# nmap -PR 192.168.1.254
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-16, 13:16 CDT.

Интересные порты на 192.168.1.254:

Не показано: 998 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

80/tcp открыть http

443/TCP открыть https

MAC-адрес : 00:25:3C:5F:5A:89 (2-проводной)

Nmap выполнено 1 IP-адрес (1 x ост работает) сканируется за 0,81 секунды.

Выполнение ARP-пинга

Опция -PR автоматически подразумевается при сканировании локальной сети. Этот тип обнаружения проходит намного быстрее, чем другие методы проверки связи, описанные в этом руководстве. Это также имеет дополнительное преимущество, заключающееся в большей точности, поскольку узлы локальной сети не могут блокировать ARP-запросы (даже если они находятся за брандмауэром).

### Примечание

Сканирование APR не может быть выполнено на объектах, которые не находятся на нашем локальном сервере. подсеть.

## Трас с ировка

Параметр --traceroute можно использовать для отслеживания сетевого пути к указанному

хся ин.

Синтаксис использования : nmap --traceroute [цель]

```
# nmap --traceroute scanme.insecure.org
```

Запуск Nmap 5.00 (http://nmap.org) в 2009-08-16 13:01 CDT.

Интересные порты на scanme.nmap.org (64.13.134.52):

Не показано 996 отфильтрованных портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

53/TCP открытый домен

70/TCP закрытый суперник

80/tcp открытый http

113/tcp закрыта авторизация

TRACEROUTE (с использованием порта 113/tcp)

АДРЕС НОР RTT

1 0,91 дом (192.168.1.254)

2 24.40 99-60-32-2.lightspeed.wchtk.sbcglobal.net (99.60.32.2)

3 23,12 76.196.172.4

4 22,69 151.164.94.52

5 32,79 ex3-p12-0.eqdtx.sbcglobal.net (69.220.8.53)

6 32,74 asn2828-XO.eqdtx.sbcglobal.net (151.164.249.134)

...

13 74,90 ip65-46-255-94.z255-46-65.customer.algx.net (65.46.255.94)

14 75.01 scanme.nmap.org (64.13.134.52)

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 33,72 секунды.

Результат сканирования трас с ировки

Отображаемая информация аналогична командам трас с ировки маршрута или трас с ировки пути.

встречается в системах Unix и Linux, с дополнительным бонусом в виде трас с ировки Nmap.

Функционально преосоздает эти команды.

## Принудительное обратное разрешение DNS

Параметр -R указывает Nmap все его да выполнять обратное разрешение DNS на целевой IP-адрес.

Синтаксис использования : nmap -R [цель]

```
# nmap -R 64.13.134.52
```

Запуск Nmap 5.00 ( http://nmap.org ) в 2009-08-13 17:22 Central

Летнее время

Интересные порты на scanme.nmap.org (64.13.134.52):

Не показано: 993 отфильтрованных порта.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

25/TCP закрытый smtp

53/TCP открытый домен

70/TCP закрытый сурслик

80/TCP открытый http

110/tcp закрыт, pop3

113/tcp закрытая авторизация

31337/tcp закрыт Элитный

Nmap выполнено: 1 IP-адрес (1 x ост работает) сканируется за 9,38 секунды.

Вывод сканирования Nmap с включенным обратным DNS

По умолчанию Nmap выполняет обратный DNS только для хостов, которые находятся в сети. -R \_

Опция полезна при выполнении разведки блока IP-адресов как

Nmap пытается разрешить обратную информацию DNS каждого IP-адреса.

Информация обратного DNS может скрывать интересную информацию целевом IP-адресе.

адрес (даже если он не в сети или блокирует зонды Nmap).

Примечание

Параметр -R может значительно снизить производительность сканирования.

## Отключить обратное разрешение DNS

Параметр -n используется для отключения обратного разрешения DNS.

Синтаксис использования : nmap -n [цель]

```
# nmap -n 64.13.134.52
```

```
Запуск Nmap 5.00 ( http://nmap.org ) в 2009-08-13 17:23 Central
```

Летнее время

Интересные порты на 64.13.134.52:

Не показано: 993 отфильтрованных порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

25/TCP	закрытый smtp
--------	---------------

53/TCP	открытый домен
--------	----------------

70/TCP	закрытый cullsик
--------	------------------

80/TCP	открытый http
--------	---------------

110/tcp	закрыт, pop3
---------	--------------

113/tcp	закрытая авторизация
---------	----------------------

31337/tcp	закрыт Элитный
-----------	----------------

```
Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 8,48 секунды.
```

Выход сканирования Nmap с отключенным обратным DNS

Обратный DNS может значительно замедлить сканирование Nmap. Использование опции -n

значительно сокращает время сканирования — особенно при сканировании большого количества хостов.

Эта опция полезна, если вам не нужна информация DNS для цели.

системы и предпочитаю выполнять сканирование, которое дает более быстрые результаты.

## Альтернативный метод поиска DNS

Опция `--system-dns` указывает Nmap использовать преобразователь DNS хост-системы.

вместо собственного внутреннего метода.

Синтаксис использования: `nmap --system-dns [цель]`

```
$ nmap --system-dns scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-09, 21:47 CDT.

Интересные порты на `scanme.nmap.org` (64.13.134.52):

Не показано: 972 закрытых порта, 26 фильтруемых портов.

ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА

53/TCP открытый домен

80/tcp открыть http

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 19,86 секунды.

Выход сканирования Nmap с использованием системного преобразователя DNS

Этот параметр используется редко, поскольку он намного медленнее, чем метод по умолчанию. Он может, однако, оказаться полезным при устранении проблем DNS с помощью Nmap.

### Примечание

Системный преобразователь всегда используется для сканирования IPv6, поскольку Nmap еще не сделал этого. полностью алисован с собственным внутренним преобразователем IPv6.

## Укажите DNS-серверы вручную

Опция `--dns-servers` используется для ручного указания DNS-серверов для запроса при сканировании.

Синтаксис использования : `nmap --dns-servers [сервер1, сервер2 и т. д.] [цель]`

```
$ nmap --dns-servers 208.67.222.222,208.67.220.220 scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-09, 22:40 CDT.

Интересные порты на `scanme.nmap.org` (64.13.134.52):

Не показано 998 закрытых портов.

ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА

53/TCP открытый домен

80/tcp открыть http

Nmap выполнено 1 IP-адрес (1 x остается) сканируется за 32,07 секунды.

Указание DNS-серверов вручную

По умолчанию Nmap будет использовать DNS-серверы, настроенные в вашей локальной системе, для разрешения имен. Опция `--dns-servers` позволяет указать один или несколько альтернативные серверы для запроса Nmap. Это может быть полезно для систем, которые не настроены DNS или если вы хотите, чтобы результаты поиска сканирования появились в файл журнала локально настроенного DNS-сервера.

### Примечание

В настоящее время этот параметр недоступен для сканирования IPv6.

## Создать список хостов

Опция `-sL` отображает список и выполнит обратный поиск к DNS указанного IP-адреса.

Синтаксис использования : `nmap -sL [цель]`

```
$ nmap -sL 10.10.1.1/24
```

```
Запуск Nmap 5.00 (http://nmap.org) в 2009-08-14, 13:56 CDT.
Хост 10.10.1.0 не сканируется
Хост router.nmapcookbook.com (10.10.1.1) не сканируется
Хост server.nmapcookbook.com (10.10.1.2) не сканируется
Хост 10.10.1.3 не сканируется
Хост 10.10.1.4 не сканируется
Хост mylaptop.nmapcookbook.com (10.10.1.5) не сканируется
Хост 10.10.1.6 не сканируется
Хост 10.10.1.7 не сканируется
Хост 10.10.1.8 не сканируется
Хост mydesktop.nmapcookbook.com (10.10.1.9) не сканируется
Хост mydesktop2.nmapcookbook.com (10.10.1.10) не сканируется
Хост 10.10.1.11 не сканируется
Хост 10.10.1.12 не сканируется
Хост 10.10.1.13 не сканируется
Хост 10.10.1.14 не сканируется
Хост 10.10.1.15 не сканируется
Хост 10.10.1.16 не сканируется
Хост 10.10.1.17 не сканируется
...
```

Вывод списка хостов, сканированных Nmap

Приведенное выше сканирование показывает результаты DNS-имен для указанных систем. Этот сканирование полезно для определения IP-адресов и DNS-имен для указанного цели, не отправляя им никаких пакетов. Многие DNS-имена могут раскрыть интересная информация об IP-адресе, включая то, для чего он используется и где он находится. расположается.



## Раздел 4:

Расширенные параметры сканирования

## Обзор рас ширенных функций сканирования

Nmap поддерживает несколько типов сканирования, выбираемых пользователем. По умолчанию Nmap будет выполнять базовое сканирование TCP в каждой целевой системе. В некоторых ситуациях это может быть необъективно выполнить более сложное сканирование TCP (или даже UDP) в попытке найти необычные службы или для обхода брандмауэра. Эти расширенные типы сканирования описаны в этой секции.

Краткое описание функций, описанных в этом разделе:

Особенность	Вариант
TCP SYN-сканирование	-SS
Сканирование TCP-соединения	-C T
UDP-сканирование	-c U
TCP NULL-сканирование	-CH
TCP FIN-сканирование	-CF
Родственное сканирование	-sX
TCP ACK-сканирование	-B
Пользовательское TCP-сканирование	--scanflags
Сканирование IP-протокола	-tak
Отправка необработанных пакетов Ethernet	--send-eth
Отправлять IP-пакеты	--send-ip

### Примечание

Вы должны войти в систему с правами root/администратора (или использовать команду sudo команда) для выполнения многих операций сканирования, обсуждаемых в этом разделе.

## TCP SYN-сканирование

Опция `-sS` выполняет сканирование TCP SYN.

Синтаксис использования : nmap `-sS [цель]`

```
# nmap -sS 10.10.1.48
```

Запуск Nmap 5.00 ( <http://nmap.org> ) в 25 авг уст 2009 г., 11:01 CDT.

Интересные порты на 10.10.1.48:

Не показано: 994 закрытых порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

21/TCP открытый FTP

22/TCP открытый SSH

25/TCP открытый SMTP

80/tcp открыть http

111/tcp открыть rpcbind

2049/tcp открыть nfs

MAC-адрес : 00:0C:29:D5:38:F4 (VMware)

Nmap выполнено: 1 IP-адрес (1 x ост работает) сканируется за 1,73 секунды.

Выполнение сканирования TCP SYN

Сканирование TCP SYN является опцией по умолчанию для привилегированных пользователей (пользователей, работающих с правами root на Unix/Linux или администраторов в Windows). Сканирование TCP SYN по умолчанию пытается определить 1000 наиболее часто используемых портов TCP, отправив пакет SYN на цель и слушаем ответ. Этот тип сканирования называется скрытым, поскольку он не пытается открыть полноценное соединение с удаленным хостом. Этот запрещает многим системам регистрировать попытку подключения при сканировании.

## Примечание

Скрытность работы не гарантируется. Современные программы перехвата пакетов а продвинутые межсетевые экраны теперь могут обнаруживать сканирование TCP SYN.

## Сканирование TCP-соединения

Опция `-sT` выполняет сканирование TCP-соединения.

Синтаксис использования: `nmap -sT [цель]`

```
$ nmap -sT 10.10.1.1
```

Запуск Nmap 5.00 (<http://nmap.org>) 31 августа 2009 г., 13:06 CDT.

Интересные порты на 10.10.1.1:

Не показано: 998 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

80/tcp открыть http

443/TCP открыть https

Nmap выполнено: 1 IP-адрес (1 x остается) сканируется за 0,56 секунды.

Выполнение сканирования TCP-соединения

Сканирование `-sT` является типом сканирования по умолчанию для непривилегированных пользователей. Он также используется, когда сканирование целей IPv6. TCP Connect Scan — это простой зонд, который пытается напрямую подключаться к удаленной системе без использования скрытности (как описано в разделе стр. 67).

Кончик

Обычно лучше всего запустить Nmap с правами root, когда это возможно.

поскольку он выполнит сканирование TCP SYN (-sS), которое может обеспечить более точную информацию о состоянии порта и работает значительно быстрее.

## UDP-сканирование

Опция -sU выполняет сканирование UDP (протокол пользовательских действий рамм).

Синтаксис использования : nmap -sU [цель]

```
# nmap -sU 10.10.1.41
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-09-06, 21:20 CDT.

Интересные порты на 10.10.1.41:

Не показано: 984 закрытых порта.

ПОРТ	СОСТОЯНИЕ	УСЛУГА
7/udp	открытъ	эхо
9/udp	открытое   отфильтрованное, отбросить	
13/udp открытъ		дневное время
19/udp открытъ		партни
37/udp открытъ		время
69/udp открытъ   отфильтрованный tftp		
111/udp open   фильтрованный rpcbind		
137/udp open   filtered netbios-ns		
138/udp open   фильтровано netbios-dgm		
177/udp открытъ   отфильтровано xdmcp		
514/udp open   отфильтрованный системный журнал		
518/udp открытъ   отфильтровано ntalk		
1028/udp открытъ   отфильтровано ms-lsa		
1030/udp открытъ   отфильтровано iad1		
2049/udp open   отфильтрованная nfs		
MAC-адрес : 00:60:B0:59:B6:14 (Hewlett-Packard CO.)		

Nmap выполнено: 1 IP-адрес (1 x открыт) работает сканируется за 1,91 секунды.

Выполнение UDP-сканирования

В приведенном выше примере показаны результаты сканирования UDP. Хотя TCP является наиболее широком используемый протокол, многие сетевые службы (такие как DNS, DHCP и SNMP) по-прежнему используют UDP. При проведении сетевого аудита всегда полезно проверить службы TCP и UDP, чтобы получить более полное представление о цели и хостах.

## TCP-сканирование NULL

Опция `-sN` выполняет сканирование TCP NULL.

Синтаксис использования : nmap -sN [цель]

```
# nmap -SN 10.10.1.48
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-10-01, 13:19 CDT.

Интересные порты на 10.10.1.48:

Не показано: 994 закрытых порта.

ПОРТ	СОСТОЯНИЕ	УСЛУГА
21/tcp	открытый   фильтрованный	ftp
22/tcp	открытый   фильтрованный	ssh
25/tcp	открыто отфильтровано	smtp
80/tcp	открытый   фильтрованный	http
111/tcp	open   фильтрованный	rpcbind
2049/tcp	открытого отфильтровано	nfs
MAC-адрес :	00:0C:29:D5:38:F4	(VMware)

Nmap выполнено: 1 IP-адрес (1 x отработал) сканируется за 1,54 секунды.

Выполнение сканирования TCP NULL

Сканирование TCP NULL приводит к тому, что Nmap отправляет пакеты без включенных флагов TCP. Это можно сделать, установив для заголовка пакета значение 0. Отправка NULL-пакетов в цель является методом обмана системы с брандмаузером для генерации ответа.

**Примечание** Не все системы реагируют наonden этого типа.

См. также: `--scanflags` (стр. 73)

## TCP FIN-сканирование

Опция `-sF` выполняет сканирование TCP FIN.

Синтаксис использования : nmap -sF [цель]

```
# nmap -sF 10.10.1.48
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-10-01, 13:21 CDT.

Интересные порты на 10.10.1.48:

Не показано: 994 закрытых порта.

ПОРТ	СОСТОЯНИЕ	УСЛУГА
21/tcp	открытый   фильтрованный	ftp
22/tcp	открытый   фильтрованный	ssh
25/tcp	открыто отфильтровано	smtp
80/tcp	открытый   фильтрованный	http
111/tcp	open   фильтрованный	rpcbind
2049/tcp	открыто отфильтровано	nfs
MAC-адрес : 00:0C:29:D5:38:F4 (VMware)		

Nmap выполнено: 1 IP-адрес (1 x открыт) работает сканируется за 1,59 секунды.

Выполнение сканирования TCP FIN

При сканировании `-sF` Nmap помечает бит TCP FIN активным при отправке пакетов в попытке запустить TCP ACK от указанной цели в системе. Это еще один метод отправки неожиданных пакетов цели в попытке получить результаты из системы, защищенной брандмауэром.

## Примечание

Не все системы реагируют наonden этого типа.

См. также: `--scanflags` (с стр. 73)

Рождественское с канирование

Флаг -sX выполняет рождественское с канирование.

Синтаксис использования : nmap -sX [цель]

```
# nmap -sX 10.10.1.48
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-10-01, 13:34 CDT.

Интересные порты на 10.10.1.48:

Не показано: 994 закрытых порта.

ПОРТ	СОСТОЯНИЕ	УСЛУГА
21/tcp	открытый   фильтрованный	ftp
22/tcp	открытый   фильтрованный	ssh
25/tcp	открыто отфильтровано	smtp
80/tcp	открытый   фильтрованный	http
111/tcp	open  фильтрованный	rpcbind
2049/tcp	открытого отфильтровано	nfs

MAC-адрес : 00:0C:29:D5:38:F4 (VMware)

Nmap выполнено: 1 IP-адрес (1 x отработал) сканируется за 2,89 секунды.

Выполнение «Рождественское с канирование»

При рождественском сканировании Nmap отправляет пакеты с URG, FIN и PSH и активированными флагами.

Это имеет эффект «зажжения» пакета, как рождественская елка и может

время от времени запрашивать ответ от системы, защищенной брандмауэром.

Примечание: Не все системы реагируют на зонды этого типа.

См. также: --scanflags (стр. 73)

## Пользовательское TCP-сканирование

Опция `--scanflags` используется для выполнения выборочного сканирования TCP.

Синтаксис использования : `nmap --scanflags [флаги] [цель]`

```
# nmap --scanflags SYNURG 10.10.1.127
```

Запуск Nmap 5.00 ( <http://nmap.org> ) 12 ноября 2009 г., 14:53 CST.

Интересные порты на 10.10.1.127:

Не показано: 996 отфильтрованных портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
139/tcp	открыть netbios-ssn
445/TCP	открыть Microsoft-DS
3389/tcp	закрыт ms-term-serv
5900/TCP	открыть VNC
MAC-адрес : 00:14:22:59:3D:DE (Dell)	

Nmap выполнено: 1 IP-адрес (1 x активен) сканируется за 4,67 секунды.

Ручное указание флагов TCP

Опция `--scanflags` позволяет пользователю определять выборочное сканирование с использованием одного или нескольких TCP.

флаг и заголовка. Можно использовать любую комбинацию флагов, перечисленных в таблице ниже.

с опцией `--scanflags`. Например: `nmap --scanflags FINACK` (без пробела)

активирует флаги FIN и ACK TCP.

Флаг	Применение
СИН	Синхронизировать
ПРИЕМНИК	Подтверждение
ПШ	Толкать
УРГ	Срочный
РСТ	Перезагрузить
КОНЕЦ	Законченный

Флаг и заголовок TCP

## TCP ACK-сканирование

Опция `-sA` выполняет сканирование TCP ACK.

Синтаксис использования : nmap -sA [цель]

```
# nmap -sA 10.10.1.70
```

Запуск Nmap 5.00 (http://nmap.org) 18 декабря 2009 г., 10:33 CST.

Интересные порты на 10.10.1.70:

Не показано: 994 отфильтрованных порта

ПОРТ	СОСТОЯНИЕ	УСЛУГА
139/tcp	нефильтрованный	netbios-ssn
445/tcp	нефильтрованный	microsoft-ds
2967/tcp	нефильтрованный	symantec-av
5900/tcp	нефильтрованный	vnc
19283/tcp	нефильтрованный	неизвестный
19315/tcp	нефильтрованное	неизвестное
MAC-адрес : 00:0C:F1:A6:1F:16 (Intel)		

Nmap выполнено 1 IP-адрес (1 x остается) сканируется за 5,33 секунды.

Выполнение сканирования TCP ACK

Опция `-sA` можно использовать, чтобы определить, защищена ли целевая система

брандмауэр. При выполнении сканирования TCP ACK Nmap будет проверять цель и искать

ответы РСТ. Если ответ не получен, система считается отфильтрованной. Если

система возвращает пакет RST, тогда он помечается как нефильтрованный. В приведенном выше

примере 994 порта помечены как фильтруемые, что означает, что система, скорее всего, защищена

через брандмауэр. Для 6 отображаемых нефильтрованных портов, скорее всего, действуют правила

брандмауэра цели, который позволяет им быть открытыми или закрытыми.

**Примечание** Опция `-sA` не показывает, является ли нефильтрованные порты

открытый или закрытый. Единственная цель – определить, работает ли система

фильтрует порты.

## Сканирование IP-протокола

Опция `-sO` выполняет сканирование IP-протокола.

Синтаксис использования : `nmap -sO [цель]`

```
# nmap -sO 10.10.1.41
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-09-06, 21:32 CDT.

Интересные протоколы на 10.10.1.41:

Найдено: 253 открытых фильтрованных протоколов.

Протокол государственнослужебные

1        открыть ICMP

6        открыть TCP

17      открыть UDP

MAC-адрес : 00:60:B0:59:B6:14 (Hewlett-Packard CO.)

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 2,81 секунды.

Выход сканирования IP-протокола

Сканирование IP-протокола отображает IP-протоколы, которые поддерживаются на целевом устройстве.

система. Наиболее распространеными протоколами в современных сетях являются ICMP, TCP,

и UDP, как показано в приведенном выше примере. Использование опции `-sO` полезно для

быстро определить, какие типы сканирования вы хотите выполнить на выбранной цели

системы на основе поддерживаемых ему протоколов.

Кончик

Полный список IP-протоколов можно найти на сайте IANA по адресу:

[www.iana.org/assignments/protocol-numbers/](http://www.iana.org/assignments/protocol-numbers/).

Отправка не обработанных пакетов Ethernet

Опция `--send-eth` указывает Nmap использовать необработанные пакеты Ethernet при сканировании.

Синтаксис использования : nmap --send-eth [цель]

```
$ nmap --send-eth 10.10.1.51
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-10-01, 14:19 CDT.

Интересные порты на 10.10.1.51:

Не показано: 997 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

80/TCP открыть http

443/TCP открыть https

49152/tcp открыт неизвестно

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 0,22 секунды.

Сканирование с использованием необработанных пакетов Ethernet

Включение этой опции указывает Nmap обходить уровень IP в вашей системе и отправлять необработанные пакеты Ethernet на канальном уровне. Это можно использовать для решения проблем с сетью IP вашей системы.

Примечание

Опция `--send-eth` автоматически подразумевается Nmap там, где это необходимо.

Он редко используется в качестве аргумента командной строки.

См. также: `--send-ip` (стр. 77).

## Отправлять IP-пакеты

Опция `--send-ip` указывает Nmap использовать IP-пакеты при сканировании.

Синтаксис использования : `nmap --send-ip [цель]`

```
$ nmap --send-ip 10.10.1.51
```

Запуск к Nmap 5.00 (<http://nmap.org>) в 2009-10-01, 14:15 CDT.

Интересные порты на 10.10.1.51:

Не показано: 997 закрытых портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

80/TCP	открыть http
--------	--------------

443/TCP	открыть https
---------	---------------

49152/tcp	открыт неизвестно
-----------	-------------------

Nmap выполнено: 1 IP-адрес (1 x остается) сканируется за 0,19 секунды.

Сканирование с использованием IP-пакетов

Включение этой опции заставляет Nmap сканировать, используя стек IP локальной системы вместо генерации необработанных пакетов Ethernet.

### Примечание

Опция `--send-ip` автоматически подразумевается Nmap там, где это необходимо. Редко используется в качестве аргумента командной строки.

См. также: `--send-eth` (стр. 76)



Раздел 5:

Опции с канирования портов

## Обзор опций с канирования портов

Всего имеется 131 070 портов TCP/IP (65 535 TCP и 65 535 UDP). Нмар, автор по умолчанию сканирует только 1000 наиболее часто используемых портов. Это сделано для экономии времени при сканировании нескольких целей, поскольку большинство портов находятся за пределами топ-1000 и используется редко. Однако иногда вам может потребоваться сканировать за пределами стандартного диапазона портов для поиска необычных служб или портов, некоторые были перенаправлены другое место. В этом разделе описаны параметры, которые позволяют этому и другим портам специфические особенности.

Кончик

Полный список портов TCP/IP можно найти на веб-сайте IANA по адресу:  
[www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers).

Краткое описание функций, описанных в этом разделе:

Особенность	Вариант
Выполните быстрое сканирование	-F
Сканировать определенные порты	-p [порт]
Сканировать порты по имени	-p [имя ]
Сканировать порты по протоколу	-p U:[порты UDP],T:[порты TCP]
Сканировать все порты	-P «*»
Сканировать основные порты	--top-ports [число]
Выполните последовательное сканирование портов	-P

Выполните быстрое сканирование

Опция -F указывает Nmap выполнить сканирование только 100 наиболее частотных ся используемые порты.

Синтаксис использования : nmap -F [цель]

```
$ nmap -F 10.10.1.44
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-13, 10:13 CDT.

Интересные порты на 10.10.1.44:

Не показано: 91 закрытый порт.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
25/TCP	открыть smtp
53/TCP	открытый домен
80/TCP	открыть http
135/tcp	открыть msrpc
139/tcp	открыть netbios-ssn
445/TCP	открыть Microsoft-DS
3389/TCP	открыть MS-Term-Serv
8000/tcp	открыть http-alt
10000/tcp	открыть snet-sensor-mgmt

Nmap выполнено: 1 IP-адрес (1 x сканируется) сканируется за 2,43 секунды.

Выход «быстро» сканирования

Nmap по умолчанию сканирует 1000 наиболее частотных используемых портов. Опция -F уменьшает это число до 100. Это может значительно ускорить сканирование, сокращая при этом большинство частотных используемых портов.

Сканировать определенные порты

Опция `-r` ис пользуется для указания Nmap сканировать указанные порты.

Синтаксис пользования : nmap -r [порт] [цель]

```
$ nmap -r 80 10.10.1.44
```

Запуск к Nmap 5.00 (<http://nmap.org>) в 2009-08-13, 10:10 CDT.

Интересные порты на 10.10.1.44:

ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА

80/tcp открыть http

Nmap выполнено: 1 IP-адрес (1 x открыт работает) сканируется за 0,12 секунды.

Указание одного порта для сканирования

В приведенном выше примере показано ис пользование `-r` для сканирования порта 80. Помимо сканирования один порт, вы можете сканировать несколько отдельных портов (через запятую или диапазон портов, как показано в следующем примере.

Синтаксис пользования : nmap [порт1,порт2 и т. д. |диапазон портов] [цель]

```
$ nmap -r 25,53,80-200 10.10.1.44
```

Запуск к Nmap 5.00 (<http://nmap.org>) в 2009-08-13, 10:10 CDT.

Интересные порты на 10.10.1.44:

Не показано: 118 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

25/TCP открыть SMTP

53/TCP открытый домен

80/tcp открыть http

135/tcp открыть msrpcs

139/tcp открыть netbios-ssn

Nmap выполнено: 1 IP-адрес (1 x открыт работает) сканируется за 0,15 секунды.

Указание нескольких портов для сканирования

В этом примере опция `-r` ис пользуется для сканирования портов с 25, 53 и 80 по 200.

## Сканировать порты по имени

Опция `-n` можно использовать для сканирования портов по имени.

Синтаксис использования : `nmap -p [имена портов] [цель]`

```
$ nmap -p smtp,http 10.10.1.44
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-17, 10:37 CDT.

Интересные порты на 10.10.1.44:

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
25/TCP	открыть SMTP
80/tcp	открыть http
8008/tcp	закрыт http

Nmap выполнено: 1 IP-адрес (1 x остается) сканируется за 0,10 секунды.

Сканирование портов по имени

В приведенном выше примере показан поиск открытых портов SMTP и HTTP по имени.

используя опцию `-n`. Указанные имена должны соответствовать службе в

файл `nmap-services`. Обычно это находится в `/usr/local/share/nmap/` в Unix/Linux.

системах или `C:\Program Files\Nmap\` в системах Windows.

Подстановочные знаки также можно использовать при указании службы по имени. Например,

выполнение `nmap -p "http*"` 10.10.1.44 будет сканировать все порты, начинающиеся с `http`.

(включая `http` и `https`).

### Примечание

Вы должны заключить подстановочный знак в кавычки, чтобы ваша система могла не интерпретировать его как подстановочный знак оболочки.

## Сканировать порты по протоколу

Указание префикса T: или U: с опцией -р позволяет вам искать определенный порт. и комбинация протоколов.

Синтаксис использования : nmap -р U:[порты UDP],T:[порты TCP] [цель]

```
# nmap -sU -sT -p U:53,T:25 10.10.1.44
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-18, 12:52 CDT.

Интересные порты на 10.10.1.44:

ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА

25/TCP открыт SMTP

53/udp открытый домен

MAC-адрес : 00:14:22:0F:3C:0E (Dell)

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 0,19 секунды.

Сканирование определенных портов по протоколу

Использование синтаксиса -р U:53,T:25 указывает Nmap выполнить UDP-сканирование порта 53 и TCP-сканирование порта 25.

Примечание

Nmap по умолчанию сканирует только TCP-порты. Чтобы сканировать как TCP, так и UDP-порты, вам нужно будет включить дополнительные типы сканирования, такие как -sU и -sT, которые описаны в разделе 4 этой книги.

Сканировать все порты

**-P \_** Параметр — это подстановочный знак, используемый для сканирования всех 65 535 портов TCP/IP на указанном цели.

Синтаксис использования : nmap -P \_ [цель]

```
# nmap -P _ 10.10.1.41
```

Запуск Nmap 5.00 ( http://nmap.org ) в 2009-12-16 14:07 Central

Обычное время

Интересные порты на 10.10.1.41:

Не показано: 4204 закрытых порта.

ПОРТ	СОСТОЯНИЕ	УСЛУГА
7/TCP	открыт	эх о
9/TCP	открыт	отказаться я
13/TCP открыт	дневное время	
19/TCP открыт	партни	
21/TCP открыт	FTP	
23/TCP открыт	туннел	
25/TCP открыто	смтп	
37/TCP открыт	время	
111/TCP открыт	rpcbind	
113/TCP открыт	авторизация	
139/TCP открыт	нетбиос -ssn	
512/TCP открыт	руководитель	
513/TCP открыт	авторизоваться я	
514/TCP открыт	оболочка	
515/TCP открыт	принтер	
543/TCP открыт	я бы забил	
...		

Сканирование всех портов целивой системы

#### Примечание

Вы должны заключить подстановочный знак в кавычки, чтобы ваша система могла не интерпретировать его как подстановочный знак оболочки.

Сканировать с новыми порты

Опция `--top-ports` используется для сканирования указанного количества портов с самым высоким рейтингом.

Синтаксис использования : `nmap --top-ports [число] [цель]`

```
# nmap --top-ports 10 10.10.1.41
```

Запуск Nmap 5.00 ( <http://nmap.org> ) 15 декабря 2009 г., 13:46 CST.

Интересные порты на 10.10.1.41:

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

21/TCP открытый FTP

22/TCP закрытый SSH

23/tcp открыть телнет

25/TCP открыть SMTP

80/tcp закрыт http

110/tcp закрыт, pop3

139/tcp открыть netbios-ssn

443/TCP закрыт https

445/tcp закрыт Microsoft-DS

3389/tcp закрыт ms-term-serv

MAC-адрес : 00:60:B0:59:B6:14 (Hewlett-Packard CO.)

Nmap выполнено: 1 IP-адрес (1 x ост работает) сканируется за 0,22 секунды.

Выполнение сканирования верхних портов находит порты с самым высоким рейтингом.

По умолчанию Nmap сканирует 1000 наиболее частотно используемых портов. Опция `-F` (см.

стр. 81) уменьшает это число до 100. Используя опцию `--top-ports`, вы можете указать

любое количество портов с самым высоким рейтингом для сканирования.

В приведенном выше примере показано использование опции `--top-ports` для сканирования 10 лучших портов.

порты; однако можно использовать любое число. Например: `nmap --top-ports 500` будет

сканировать 500 наиболее частотно используемых портов, и `nmap --top-ports 5000` будет сканировать

5000 наиболее частотно используемых портов.

Выполните последовательное сканирование портов

Опция `-r` выполняет последовательное сканирование портов указанной цели.

Синтаксис использования : `nmap -r [цель]`

```
$ nmap -r 10.10.1.48
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-13, 13:02 CDT.

Интересные порты на 10.10.1.48:

Не показано: 994 закрытых порта.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

21/TCP открытый FTP

22/TCP открытый SSH

25/TCP открытый SMTP

80/tcp открыть http

111/tcp открыть rpcbind

2049/tcp открыть nfs

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 0,49 секунды.

Выполнение последовательного сканирования портов

Алгоритм сканирования Nmap по умолчанию randomизирует порядок сканирования портов. Это полезно для обхода брандмаузеров и систем предотвращения вторжений. Параметр `-r` определяет это функциональность и инструктирует Nmap последовательно искать открытые порты в числовых значениях .

заказ.

Примечание

Результаты сканирования `-r` не совсем очевидны, поскольку Nmap всегда сортирует конечный результат каждого сканирования. Сочетание опции `-v` с `-r` позволит отображать последовательное обнаружение портов в режиме реального времени.



## Раздел 6:

Обнаружение операций ионной системы и служб

## Обзор определения версии

Одна из самых замечательных (и невероятно полезных) функций Nmap — это возможность обнаруживать операционные системы и службы в удаленных системах. Эта функция анализирует ответы от сканируемых целей и попытки определить работающий хост.

Системы и установленных служб.

Процесс идентификации целевой операционной системы и версий программного обеспечения известный как снятие отпечатков пальцев TCP/IP. Хотя это и не точная наука, Nmap разработчики позаботились о том, чтобы создание отпечатков пальцев в TCP/IP было точным и надежной функцией. И, как и большинство функций Nmap, определение версии может быть управляется с помощью аргументов, которые рассматриваются в этом разделе.

**Краткое описание функций, описанных в этом разделе:**

Особенность	Вариант
Обнаружение операционной системы	-O
Попытка угадать неизвестную ОС	--osscan-guess
Определение версии службы	-c B
Выполните сканирование RPC	--version-trace
Устранение неполадок при сканировании версий	-c P

## Обнаружение операционной системы

Параметр -O включает функцию обнаружения операционной системы Nmap.

Синтаксис использования : nmap -O [цель]

```
# nmap -O 10.10.1.48
```

```
Запуск Nmap 5.00 ( http://nmap.org ) в 2009-08-11 13:09 Central
```

```
Летнее время
```

```
...
```

```
MAC-адрес : 00:0C:29:D5:38:F4 (VMware)
```

```
Тип устройства: общего назначения
```

```
Работает: Linux 2.6.X
```

```
Сведения об ОС: Linux 2.6.9-2.6.28.
```

```
Расстояние сети: 1 переход
```

```
...
```

Выход функции обнаружения операционной системы Nmap

Как показано выше, Nmap (в большинстве случаев) способен идентифицировать рабочий систему на удаленной цели. Обнаружение операционной системы осуществляется путем анализа ответов цели на набор предсказуемых характеристик, которые можно использовать для определения типа ОС в удаленной системе.

Для правильной работы обнаружения ОС должен быть хотя бы один открытый и один закрытый порт в целиовой системе. При сканировании нескольких целей параметр -osscan-limit опция можно комбинировать с -O, чтобы указать Nmap не сканировать хосты ОС, которые не соответствуют этому критерию

Кончик

Опция -v можно комбинировать с -O для отображения дополнительной информации.

Nmap обнаруживает удаленную систему.

## Отправка отпечатков TCP/IP

Если Nmap не может определить операционную систему на цели, он предоставит отпечаток пальца, который можно отправить в базу данных ОС Nmap по адресу [www.nmap.org/submit/](http://www.nmap.org/submit/). Пример ниже демонстрирует вывод Nmap в этом случае.

сценарий.

```
# nmap -O 10.10.1.11
```

Запуск Nmap 5.00 ( <http://nmap.org> ) в 2009-12-16 14:16 Central

Обычное время

...

Нет точных сведений ОС для хоста (если вы знаете, какая ОС на нем работает, см. <http://nmap.org/submit/>).

Отпечаток TCP/IP:

```
CC:CAH(V=5.00%D=12/16%OT=3001%CT=1%CU=32781%PV=Y%DS=1%G=Y%M=00204A%TM=4B29
OC:4048%P=i686-pc-windows-windows)SEQ(CI=I%II=I%TS=U)OPS(O1=M400%O2=%O3=%O4
OC:=%O5=%O6=)OPS(O1=M400%O2=M400%O3=%O4=%O5=%O6=)OPS(O1=%O2=M400%O3=M400%O4
OC:=%O5=%O6=)OPS(O1=%O2=%O3=M400%O4=%O5=%O6=)OPS(O1=M400%O2=%O3=M400%O4=%O5
OC:=%O6=)WIN(W1=7FF%W2=0%W3=0%W4=0%W5=0%W6=0)WIN(W1=7FF%W2=7FF%W3=0%W4=0%W5
OC:=0%W6=0)WIN(W1=0%W2=7FF%W3=7FF%W4=0%W5=0%W6=0)WIN(W1=0%W2=0%W3=7FF%W4=0%
OC:W5=0%W6=0)WIN(W1=7FF%W2=0%W3=7FF%W4=0%W5=0%W6=0)ECN(R=Y%DF=Y%T=40% B=0%O=
OC %CC=N%Q=T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=T1(R=Y%DF=Y%T=40%S=O%A=O
OC %F=AS%RD=0%Q=)T1(R=Y%DF=Y%T=40%S=Z%A=S+%F=AR%RD=0%Q=)T2(R=Y%DF=Y%T=40%W=
OC :0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
OC :)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=
OC :S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF
OC :=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=Y%T=40%IPL=38%UN=0%RIPL=G
OC %RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=40%CD=S)
```

...

Отпечаток TCP/IP, созданный Nmap

Отправив сгенерированный отпечаток пальца и правильно определив целевую систему операционной системы, вы можете помочь повысить точность обнаружения ОС Nmap. функция в будущем выгружена.

## Попытка угадать неизвестную операционную систему

Если Nmap не может точно определить ОС, вы можете заставить ее угадать, используя опцию `--osscan-guess`.

Синтаксис использования: `nmap -O --osscan-guess [цифра]`

```
# nmap -O --osscan-guess 10.10.1.11
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-17, 13:25 CDT.

Интересные порты на 10.10.1.11:

Не показано: 999 закрытых портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

3001/TCP открытый Несуществует

MAC-адрес: 00:20:4A:69:FD:94 (Pronet GmbH)

Адрессивная ОС догадывается: устройство мониторинга энергопотребления Enerdis Enerium 200 или Проектор Mitsubishi XD1000 (96%), внешний последовательный порт Lantronix UDS200

сервер устройств (96%), встроенный сервер последовательных устройств Lantronix XPort-03

(прошивка 6.1.0.3) (95%), NTP-сервер Larus 54580 (95%), Lantronix

Evolution OS (93%), сервер внешних последовательных устройств Lantronix UDS1100

(92%), встроенный сервер Ethernet устройств Lantronix XPort (90%),

устройство мониторинга и калибровки Stonewater Control Systems (88%),

FreeBSD 6.3-RELEASE (88%), Crestron MC2E, MP2E, PRO2 или QM-RMC

система управления и автоматизации (2-я серия) (87%)

...

Предполагаемый вывод операционной системы Nmap

В приведенном выше примере отображается список возможных совпадений с операционной системой цели. система. Каждое предложение указано с процентом уверенности, которое Nmap имеет в поставленный матч.

Кончик

Опция `--fuzzy` — это синоним, который можно использовать для легкого запоминания языка для функции `--osscan-guess`.

## Определение версии с службы

Параметр -sV включает функцию определения версии сервиса Nmap.

Синтаксис использования : nmap -sV [цель]

```
# nmap -sV 10.10.1.48
```

Запуск Nmap 5.00 ( http://nmap.org ) в 2009-08-11 12:49 Central

Летнее время

Интересные порты на 10.10.1.48:

Не показано: 996 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ ВЕРСИЯ

21/TCP открытый FTP

vsftpd 2.0.6

22/TCP открыть SSH

OpenSSH 4.7p1 Debian 8ubuntu1.2 (протокол 2.0)

25/TCP открыть SMTP

Портфикс smtpd

80/tcp открытый http Apache httpd 2.2.8 ((Ubuntu))

MAC-адрес : 00:0C:29:D5:38:F4 (VMware)

Информация о службе: Хост: 10.10.1.48; ОС: Unix, Linux

Обнаружение с службы выполнено. Пожалуйста, сообщите о любых неверных результатах по адресу <http://nmap.org/submit/>.

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 8,33 секунды.

Выход функции определения версии сервиса Nmap

Опция -sV пытается определить поставщика и версионного программного обеспечения для любых открытых портов, которые он обнаруживает. Результаты приведенного выше сканирования показывают поставщика программного обеспечения и номер версии сервисов, которые Nmap смог успешно идентифицировать.

Примечание Определение версии Nmap намеренно пропускает некоторые проблемные порты

(конкретно 9100-9107). Это можно обойти, объединив

Параметр --allports с -sV, который указывает Nmap не использовать какие-либо порты из определения версии.

Устранение неполадок при сканировании версий

Опцию `--version-trace` можно включить для отображения подробной активности сканирования версий.

Синтаксис использования : `nmap -sV --version-trace [цель]`

```
$ nmap -sV --version-trace 10.10.1.48
```

Запуск Nmap 5.00 (http://nmap.org) в 2009-08-13, 13:16 CDT.

ПОРТЫ : исользование 1000 наиболее открытых портов (TCP:1000, UDP:0, SCTP:0).

----- Отчет о времени -----

Группы хостов: мин 1, макс 100000

RTT-таймауты: инициализация 1000, мин 100, макс 10000

Максимальная задержка сканирования : TCP 1000, UDP 1000, SCTP 1000

параллелизм: мин 0, макс 0

Максимальное количество попыток : 10, таймаут хоста 0

Минимальная скорость: 0, максимальная скорость: 0

NSE: Загрузил 3 скрипта для сканирования .

Общая скорость отправки: 319,95 пакетов/с.

Максимальное значение `max_successful_trypacket` для 10.10.1.48 увеличено до 1 (отбрасывание пакетов).

Общая скорость отправки: 756,69 пакетов/с.

NSOCK (1.6000 с) TCP-соединение запрошено на 10.10.1.48:21 (IOD #1) EID 8

NSOCK (1.6000 с) TCP-соединение запрошено на 10.10.1.48:22 (IOD #2) EID 16

NSOCK (1.6000 с) TCP-соединение запрошено на 10.10.1.48:25 (IOD #3) EID 24

NSOCK (1.6000 с) TCP-соединение запрошено на 10.10.1.48:80 (IOD #4) EID 32

NSOCK (1.6000 с) TCP-соединение запрошено на 10.10.1.48:111 (IOD #5) EID 40

NSOCK (1.6000 с) TCP-соединение запрошено на 10.10.1.48:2049 (IOD #6) EID 48

NSOCK (1,6000 с) nssock\_loop() запущен (без таймаута). Ожидается 6 с событий

Обратный вызов NSOCK (1.6010s): CONNECT SUCCESS для EID 8 [10.10.1.48:21]

...

Вывод трафика сканирования версий

Опция `--version-trace` может быть полезна при отладке проблем или для получения

дополнительная информация о целевой системе. Для получения дополнительной информации о

устранение неполадок и отладка Nmap см. Раздел 10.

## Выполните сканирование RPC

Опция -sR выполняет сканирование RPC (удаленный вызов процедур) на указанной цели.

Синтаксис использования : nmap -sR [цель]

```
$ nmap -sR 10.10.1.176
```

Запуск Nmap 5.00 (http://nmap.org) в 2009-08-13 14:22 Central

Летнее время

Интересные порты на 10.10.1.176:

Не показано 995 закрытых портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА	ВЕРСИЯ
22/TCP	открыть SSH	
111/tcp	открыть rpcbind (rpcbind V2) 2 (rpc #100000)	
139/tcp	открыть netbios-ssn	
445/TCP	открыть Microsoft-DS	
2049/tcp	открытый nfs (nfs V2-4)	2-4 (RPC № 100003)
MAC-адрес : 00:16:EA:F0:92:50 (Intel)		

Nmap выполнено 1 IP-адрес (1 хост активен) сканируется за 3,01 секунды.

Выходные данные сканирования RPC

Результаты сканирования -sR выше отображают информацию о запущенных службах RPC.

В целевой системе, RPC чаще всего используется с системами Unix и Linux.

специально для службы NFS (система файловой системы). В этом примере NFS версии 2

Службы RPC обнаруживаются на портах 111 и 2049.

Раздел 7:

Параметры времени

## Обзор параметров с их реализацией

Многие функции Nmap имеют настраиваемые параметры с их реализацией. Эти параметры времени могут быть использованы для ускорения или замедления операций сканирования в зависимости от ваших потребностей. При сканировании большого количества хостов в быстрой сети вам может потребоваться увеличить количество параллельных операций для получения более быстрых результатов. Альтернативно, при сканировании медленные сети (или Интернет), возможно, вы захотите замедлить сканирование, чтобы получить более точные результаты или для обхода систем обнаружения вторжений. Этап секция обсуждается параметры, доступные для этих функций с их реализацией.

Краткое описание функций, описанных в этом разделе:

Особенность	Вариант
Шаблоны времени	-T[0-5]
Установите TTL пакета	--ttl
Минимальное количество параллельных операций	--min-параллелизм
Максимальное количество параллельных операций	--max-параллелизм
Минимальный размер группы хостов	--min-hostgroup
Максимальный размер группы хостов	--max-hostgroup
Максимальное время ожидания RTT	--max-rtt-таймаут
Начальный таймаут RTT	--initial-rtt-timeout
Максимальное количество повторов	--max-повторных попыток
Таймаут хоста	--host-timeout
Минимальная задержка сканирования	--scan-delay
Максимальная задержка сканирования	--max-scan-delay
Минимальная скорость передачи пакетов	--min-ставка
Максимальная скорость передачи пакетов	--max-ставка
Победить сброс ограничений скорости	--defeat-rst-ratelimit

## Временные параметры

По умолчанию параметры времени Nmap принимаются в миллисекундах. Вы также можете указать параметры времени в секундах, минутах или часах, добавив квалификатор аргумент времени. В таблице ниже приведены примеры использования параметра времени синтаксиса.

Параметр	Определение	Пример	Значение
(никто)	Миллисекунды (1/1000 секунды)	500	500 миллисекунд
с	Секунды	300 с	300 секунд
м	Минуты	5 м	5 минут
час	Часы	1 час	1 час

Параметры спецификации времени Nmap

Пример: Опция --host-timeout (см. стр. 108) использует параметр времени. Кажите я тиминутный таймаут, вы можете использовать любую из следующих форм времени  
Спецификация:

```
nmap --host-timeout 300000 10.10.5.11
nmap --host-timeout 300 с 10.10.5.11
nmap --host-timeout 5 м 10.10.5.11
```

Поскольку  $300000 = 300 \text{ с} = 5 \text{ м}$ , любая из приведенных выше команд даст тот же результат.

Tech.net24.ip

## Шаблоны времени

Параметр -T используется для указания шаблона с инх ронизац ии для сканирования Nmap.

Синтаксис использования : nmap -T[0-5] [ц ель]

```
$ nmap -T4 10.10.1.1
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-12, 16:59 CDT.

Интересные порты на 10.10.1.1:

Не показано: 998 закрытых портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
80/tcp	открыть http
443/TCP	открыть https

Nmap выполнено: 1 IP-адрес (1 x ост работает) сканируется за 0,48 секунды.

Использование шаблона времени

Шаблоны с инх ронизац ии — это удобные ярлыки для различных вариантов с инх ронизац ии (обсуждаются позже в разделе этапа цикла). Существует шесть шаблонов (с номерами от 0 до 5), которые можно использовать для ускорения работы. сканирование (для более быстрого получения результатов) или для замедления сканирования (для обхода брандмаузеров). Стол ниже описывает каждый шаблон с инх ронизац ии.

Шаблон	Имя	Примечания
-T0	параноик	Очень медленно
-T1	подлый	Полезно для обхода систем обнаружения вторжений.
-T2	вежливый	Маловероятно, что они помешают целевой системе.
-T3	нормальный	Это шаблон времени по умолчанию
-T4	агрессивный	Дает более быстрые результаты в локальных сетях
-T5	безумный	Очень быстрое и агрессивное сканирование

Шаблоны времени Nmap

## Минимальное количество параллельных операций

Опция `--min-parallelism` используется для указания минимального количества параллельных операций сканирования портов. Nmap должен выполнять в любой момент времени.

Синтаксис использования : `nmap --min-parallelism [число] [цель]`

```
# nmap --min-parallelism 100 10.10.1.70
```

Запуск Nmap 5.00 ( <http://nmap.org> ) в 2009-12-17, 09:02 CST.

Интересные порты на 10.10.1.70:

Не показано: 994 отфильтрованных порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
139/tcp	открыть netbios-ssn
445/TCP	открыть Microsoft-DS
2967/tcp	закрыт symantec-av
5900/TCP	открыть VNC
19283/tcp	закрыт неизвестно
19315/tcp	закрыт неизвестно
MAC-адрес	: 00:0C:F1:A6:1F:16 (Intel)

Nmap выполнено 1 IP-адрес (1 хост работает) сканируется за 3,43 секунды.

Указание минимального количества параллельных операций

Nmap автоматически настраивает параметры параллельного сканирования в зависимости от условий сети.

В некоторых редких случаях вам может потребоваться указать собственные настройки. Приведенный выше пример инструктирует Nmap всегда выполнять не менее 100 параллельных операций в любой момент времени.

### Примечание

При ручной настройке параметра `--min-parallelism` может увеличиться скорость сканирования.

производительности, установка слишком высокого значения может привести к неточным результатам.

## Максимальное количество параллельных операций

Опция `--max-parallelism` используется для управления максимальным количеством параллельных операций сканирования портов Nmap будет выполнять в любой момент времени.

Синтаксис использования : `nmap --max-parallelism [число] [цель]`

```
# nmap --max-parallelism 1 10.10.1.70
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-12-17, 09:03 CST.

Интересные порты на 10.10.1.70:

Не показано 994 отфильтрованных порта.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

139/tcp открыть netbios-ssn

445/TCP открыть Microsoft-DS

2967/tcp закрыт symantec-av

5900/TCP открыть VNC

19283/tcp закрыт неизвестно

19315/tcp закрыт неизвестно

MAC-адрес : 00:0C:F1:A6:1F:16 (Intel)

Nmap выполнено: 1 IP-адрес (1 хост активен) просканирован за 213,76 секунды.

Указание максимального количества параллельных операций

В приведенном выше примере `--max-parallelism 1` используется для ограничения Nmap, чтобы только один операция выполняется единовременно. Это сканирование будет значительно медленным, но будет менее может привести к перегрузке целиовой системы потоком пакетов.

## Минимальный размер группы хостов

Опция `--min-hostgroup` используется для указания минимального количества целей.

Nmap должен сканировать параллельно.

Синтаксис использования : nmap --min-hostgroup [число] [цели]

```
# nmap --min-hostgroup 30 10.10.1.0/24
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-11-10, 10:17 CST.

Интересные порты на 10.10.1.1:

Не показано: 998 закрытых портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
80/tcp	открыть http
443/TCP	открыть https

MAC-адрес : 00:06:B1:12:0D:14 (Sonicwall)

Интересные порты на 10.10.1.2:

Не показано: 998 закрытых портов.

ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА
23/tcp

открыть telnet

80/tcp открыть http

MAC-адрес : 00:19:B9:A6:ED:D9 (Dell)

...

Указание минимального размера группы хостов

Nmap будет выполнять сканирование параллельно, чтобы сэкономить время при сканировании нескольких целей.

Например диапазон или все подсети. По умолчанию Nmap автоматически регулирует размер групп хостов в зависимости от типа выполнения сканирования и сети.

Условия . Указав опцию `--min-hostgroup`, Nmap попытается сократить размеры группы, превышающие указанное число.

## Максимальный размер группы хостов

Опция `--max-hostgroup` используется для указания максимального количества целей.

Nmap должен сканировать параллельно.

Синтаксис использования : nmap `--max-hostgroup [число] [цели]`

```
# nmap --max-hostgroup 10 10.10.1.0/24
```

Запуск Nmap 5.00 (http://nmap.org) в 2009-11-10, 10:18 CST.

Интересные порты на 10.10.1.1:

Не показано: 998 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

80/tcp открыть http

443/TCP открыть https

MAC-адрес : 00:06:B1:12:0D:14 (Sonicwall)

Интересные порты на 10.10.1.2:

Не показано: 998 закрытых портов.

ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА

23/tcp открыть телнет

80/tcp открыть http

MAC-адрес : 00:19:B9:A6:ED:D9 (Dell)

...

Указание максимального размера группы хостов

В отличие от опции `--min-hostgroup`, опция `--max-hostgroup` управляет

максимальное количество хостов в группе. Эта опция полезна, если вы хотите уменьшить

нагрузки на сеть или избежание перегрузки каких-либо «красных флагков» в различных сетях.

продукты безопасности.

## Начальный таймаут RTT

[Technet24.ir](#)

Опция `--initial-rtt-timeout` управляет начальным таймаутом RTT (время прохождения туда и обратно). Значение, используемое Nmap.

Синтаксис использования : `nmap --initial-rtt-timeout [время] [цель]`

```
# nmap --initial-rtt-timeout 5000 scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) 16 декабря 2009 г., 16:23 CST.

Интересные порты на `scanme.nmap.org` (64.13.134.52):

Найдено 998 отфильтрованных портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

53/TCP	открытый домен
--------	----------------

80/TCP	открыть http
--------	--------------

Nmap выполнено 1 IP-адрес (1 хост работает) сканируется за 8,31 секунды.

Указание начального значения таймаута RTT, используемого Nmap

Шаблон с инструкцией по умолчанию (-T3; см. стр. 100) имеет значение `--initial-rtt-timeout`, равное

1000 миллисекунд. Увеличение значения уменьшит количество пакетов.

повторные передачи из-за таймаутов. Уменьшив значение, вы можете ускорить сканирование;

но делайте это с осторожностью. Установка слишком малого значения таймаута RTT может свести на нет любые потенциальный прирост производительности и приводит к неточным результатам.

## Максимальное время ожидания RTT

Опция `--max-rtt-timeout` используется для указания максимального значения RTT (туда и обратно).

Time) таймаут для ответа пакета.

Синтаксис использования : nmap --max-rtt-timeout [время] [цель]

```
# nmap --max-rtt-timeout 400 scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-11-14, 12:57 CST.

Интересные порты на [scanme.nmap.org](http://scanme.nmap.org) (64.13.134.52):

Не показано 993 отфильтрованных порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

25/TCP	закрытый smtp
--------	---------------

53/TCP	открытый домен
--------	----------------

70/TCP	закрытый cuse
--------	---------------

80/TCP	открытый http
--------	---------------

110/tcp	закрыт, pop3
---------	--------------

113/tcp	закрытая авторизация
---------	----------------------

31337/tcp	закрыт Элитный
-----------	----------------

Nmap выполнено: 1 IP-адрес (1 x сканируется) за 8,11 секунды.

Указание максимального таймаута RTT в 400 миллисекунд.

Nmap по умолчанию динамически настраивает параметры таймаута RTT для достижения лучших результатов.

Максимальное время ожидания RTT по умолчанию составляет 10 секунд. Ручная настройка максимального RTT

меньшее значение таймаута позволит сократить время сканирования (особенно при сканировании больших блоков).

адресов). Указание большого максимального таймаута RTT не позволит Nmap

слишком рано сдаваться при сканировании медленных /ненадежных соединений. Типичные значения

составляют от 100 миллисекунд для быстрых /надежных сетей до 10 000 миллисекунд для

медленные/ненадежные соединения .

Максимальное количество повторов

Опция `--max-retries` используется для управления максимальным количеством зондов.

Nmap пытается выполнить повторную передачу.

Синтаксис использования : nmap --max-retries [число] [цель]

```
# nmap --max-retries 1 scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-11-10, 09:59 CST.

Интересные порты на [scanme.nmap.org](http://scanme.nmap.org) (64.13.134.52):

Не показано: 993 отфильтрованных порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

25/TCP	закрытый smtp
--------	---------------

53/TCP	открытый домен
--------	----------------

70/TCP	закрытый culls
--------	----------------

80/TCP	открыть http
--------	--------------

110/tcp	закрыт, pop3
---------	--------------

113/tcp	закрытая авторизация
---------	----------------------

31337/tcp	закрыт Элитный
-----------	----------------

Nmap выполнено: 1 IP-адрес (1 x остается) сканируется за 7,55 секунды.

Указание максимального количества повторов

По умолчанию Nmap автоматически регулирует количество повторных передач зонда.

В зависимости от условий сети. Опция `--max-retries` можно использовать, если вы хотите

передопределите настройки по умолчанию или устраните проблемы с подключением. Указание

большое число может увеличить время, необходимое для завершения сканирования, но приведет к

более точные результаты. Уменьшив `--max-retries`, вы можете ускорить сканирование –

хотя вы можете не получить точных результатов, если Nmap сдается слишком быстро.

## Установите TTL пакета

Опция `--ttl` используется для указания TTL (срок жизни) для указанного сокамирования (в миллисекунды).

Синтаксис использования : `nmap --ttl [время] [цель]`

```
# nmap --ttl 500 scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-24, 13:19 CDT.

Интересные порты на [scanme.nmap.org](http://scanme.nmap.org) (64.13.134.52):

Не показано 993 отфильтрованных порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

25/TCP	закрытый smtp
--------	---------------

53/TCP	открытый домен
--------	----------------

70/TCP	закрытый cuse
--------	---------------

80/TCP	открытый http
--------	---------------

110/tcp	закрыт, pop3
---------	--------------

113/tcp	закрытая авторизация
---------	----------------------

31337/tcp	закрыт Элитный
-----------	----------------

Nmap выполнено: 1 IP-адрес (1 x сканируется) сканируется за 7,04 секунды.

Указание параметра TTL, равного 500 миллисекундам

Пакеты, отправленные с использованием этой опции, будут иметь указанное значение TTL. Этот вариант полезен при сканировании целей намедленных соединений, когда обычные пакеты могут истечь потайм-ауту прежде чем получить ответ.

## Таймаут хоста

Опция `--host-timeout` задаваяет Nmap отказываться от медленных хостов после указанного времени.

Синтаксис пользования : `nmap --host-timeout [время] [цель]`

```
# nmap --host-timeout 1m 10.10.5.11
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-10-09, 13:29 CDT.

Пропуск хоста 10.10.5.11 из-за таймаута хоста

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 60,19 секунды.

Вывод сканирования Nmap при указании таймаута в 1 минуту

Сканирование хоста может занять много времени, если он расположен в медленной или не надежной сети.

Системы, защищенные множественными экранами, различивающимися скоростью, также могут потребовать значительных затрат.

количество времени на сканирование. Опция `--host-timeout` указывает Nmap отказаться от

целевую систему, если она не может быть завершена по истечении указанного интервала времени. В приведенном выше

Например, сканирование занимает больше одной минуты (согласно стандарту 1m).

параметр), который задаваяет Nmap прекратить сканирование. Этот вариант особенно

полезно при сканировании нескольких систем через глобальную сеть или подключение к Интернету.

### Примечание

Nmap выполняет параллельные операции при сканировании нескольких целей. Если один хост отвечает долго, скорее всего, Nmap сканирование других хостов в это время. Это уменьшает потенциальные узкие места, которые могут создать медленные хости.

### Предупреждение

Если указана опция `--host-timeout`, Nmap не будет отображать никаких возникает, если хост превышает таймаут (даже если он обнаружил открытые порты).

**Минимальная задержка сканирования**

Опция `--scan-delay` указывает Nmap приостановить работу на указанный интервал времени между зондами.

Синтаксис использования : `nmap --scan-delay [время] [цель]`

```
# nmap --scan-delay 5s scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-11-04, 13:29 CST.

Интересные порты на 64.13.134.52:

Не показано: 993 отфильтрованных порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

25/TCP	закрытый smtp
--------	---------------

53/TCP	открытый домен
--------	----------------

70/TCP	закрытый cullsник
--------	-------------------

80/TCP	открытый http
--------	---------------

110/tcp	закрыт, pop3
---------	--------------

113/tcp	закрытая авторизация
---------	----------------------

31337/tcp	закрыт Элитный
-----------	----------------

Nmap выполнено: 1 IP-адрес (1 хост активен) просканирован за 229,28 секунды.

Указание минимальной задержки сканирования в 5 секунд.

Некоторые системы используют ограничение скорости, что может затруднить попытки сканирования Nmap.

Nmap автоматически регулирует задержку сканирования по умолчанию в системах, где скорость обнаружено ограничение. В некоторых случаях может быть полезно указать собственную задержку сканирования, если вы знаете, что используется ограничение скорости или IDS (системы обнаружения вторжений). В приведенном выше примере задержка сканирования в 5 секунд структурирует Nmap ждать пять секунд между зондами.

Максимальная задержка сканирования

-max-scan-delay используется для указания максимального времени, в течение которого Nmap должен подождать между зондами.

Синтаксис использования : nmap --max-scan-delay [время] [цель]

```
# nmap --max-scan-delay 300 scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-11-09, 15:35 CST.

Интересные порты на [scanme.nmap.org](http://scanme.nmap.org) (64.13.134.52):

Найдено 993 отфильтрованных порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

25/TCP	закрытый smtp
--------	---------------

53/TCP	открытый домен
--------	----------------

70/TCP	закрытый cups
--------	---------------

80/TCP	открытый http
--------	---------------

110/tcp	закрыт, pop3
---------	--------------

113/tcp	закрытая авторизация
---------	----------------------

31337/tcp	закрыт Элитный
-----------	----------------

Nmap выполнено: 1 IP-адрес (1 x осто работает) сканируется за 8,14 секунды.

Указание максимальной задержки сканирования в 30 миллисекунд.

Nmap автоматически регулирует задержку сканирования в соответствии с условиями сети и/или

хосты, отличающиеся скорость. Опционо--max-scan-delay можно использовать для указания верхнего предела.

ограничить количество времени между зондами. Это может усилить сканирование, но

засчет точных результатов и дополнительной нагрузки на есть.

Минимальная с коротким передачи пакетов

Опция `--min-rate` используется для указания минимального количества пакетов Nmap.

должен отправлять в секунду.

Синтаксис использования : nmap --min-rate [число] [цель]

```
# nmap --min-rate 30 scanme.insecure.org
```

Запуск Nmap 5.00 (http://nmap.org) 10 ноября 2009 г., 14:13 CST.

Интересные порты на scanme.nmap.org (64.13.134.52):

Не показано: 993 отфильтрованных порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

25/TCP	закрытый smtp
--------	---------------

53/TCP	открытый домен
--------	----------------

70/TCP	закрытый cullsilk
--------	-------------------

80/TCP	открытый http
--------	---------------

110/tcp	закрыт, pop3
---------	--------------

113/tcp	закрытая авторизация
---------	----------------------

31337/tcp	закрыт Элитный
-----------	----------------

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 6,99 секунды.

Указание минимальной скорости передачи пакетов 30

Nmap по умолчанию автоматически регулирует скорость передачи пакетов при сканировании на основе

сетевые условия. В некоторых случаях вы можете указать свой собственный минимум.

ставка -x отя обычно это не рекомендуется. В приведенном выше примере

`--min-rate 30` указывает Nmap отправлять не менее 30 пакетов в секунду. Nmap будет

использовать номер в качестве нижнего порога, но сканирование может выполняться быстрее, если есть

условия позволяют.

Предупреждение Установка слишком высокого значения `--min-rate` может снизить точность сканирования.

Максимальная скорость передачи пакетов

Опция `--max-rate` используется для указания максимального количества пакетов Nmap.

должен отправлять в секунду.

Синтаксис пользования : nmap --max-rate [число] [цель]

```
# nmap --max-rate 30 scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-11-10, 14:14 CST.

Интересные порты на [scanme.nmap.org](http://scanme.nmap.org) (64.13.134.52):

Найдено: 993 отфильтрованных порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

25/TCP	закрытый smtp
--------	---------------

53/TCP	открытый домен
--------	----------------

70/TCP	закрытый cups
--------	---------------

80/TCP	открыть http
--------	--------------

110/tcp	закрыт, pop3
---------	--------------

113/tcp	закрытая авторизация
---------	----------------------

31337/tcp	закрыт Элитный
-----------	----------------

Nmap выполнено: 1 IP-адрес (1 x остается) сканируется за 68,51 секунды.

Указание максимальной скорости передачи пакетов 30

В приведенном выше примере указание `--max-rate 30` указывает Nmap больше не отправлять

это 30 пакетов в секунду. Это может значительно замедлить сканирование, но может быть

полезно при попытке обойти систему обнаружения вторжений или цели, использующие

ограничение скорости.

Кончик	Чтобы выполнить очень скрытое сканирование, используйте <code>--max-rate 0.1</code> , который указывает Nmap отправлять один пакет каждые десять секунд
--------	---

Победить сброс огра ничений с корости

-defeat-rst-ratelimit ис поль зуе ться для поражения целей, которые применяют ограничение с корости к RST.  
(сброс) пакетов.

Синтакс ис пользования : nmap --defeat-rst-ratelimit [цель]

```
# nmap --defeat-rst-ratelimit scanme.insecure.org
```

Запуск Nmap 5.00 (http://nmap.org) 10 ноя бря 2009 г., 15:14 CST.

Интересные порты на scanme.nmap.org (64.13.134.52):

Не показано: 993 отфильтрованных порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

25/TCP	закрытый smtp
--------	---------------

53/TCP	открытый домен
--------	----------------

70/TCP	закрытый суслик
--------	-----------------

80/TCP	открытый http
--------	---------------

110/tcp	закрыт, pop3
---------	--------------

113/tcp	закрытая авторизация
---------	----------------------

31337/tcp	закрыт Элитный
-----------	----------------

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 7,71 секунды.

Обход ограничений с корости RST

Опция --defeat-rst-ratelimit может быть полезна, если вы хотите усилить сканирование

цели, реализующие ограничения с корости пакетов RST. Однако это может привести к неточным результатам  
результаты и поэтому ис поль зуе ться редко.

**Примечание** Опция --defeat-rst-ratelimit ис поль зуе ться редко, поскольку в большинстве случаев

Nmap автоматически обнаружит хости, ограничивающие корость, и настроит се бя .

Соответственно.

Раздел 8:

Обх од брандмауэров

## Обзор методов обх ода брандмауэра

Брандмауэры и системы предотвращения вторжений предназначены для предотвращения атак таких инструментов, как Nmap. от получения точного представления о системах, которые они защищают. Nmap включает в себя ряд функций, предназначенных для обхода этой защиты. В этом разделе обсуждаются различные методы уклонения, встроенные в Nmap.

**Краткое описание функций, описанных в этом разделе:**

Особенность	Вариант
Фрагментированные пакеты	-f
Укажите конкретный MTU	--mtu
Используйте приманку	-D
Сканирование зомби в режиме сканирования	-I
Вручную укажите исходный порт	--source-port
Добавить случайные данные	--data-length
Случайный порядок сканирования цели	--randomize-hosts
Подделать MAC-адрес	--spoof-mac
Отправлять неверные контрольные суммы	--badsum

## Фрагментированные пакеты

[Technet24.ir](#)

Опция `-f` используется для фрагментации зондов на 8-байтовые пакеты.

Синтаксис использования : `nmap -f [цель]`

```
# nmap -f 10.10.1.48
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-11-11, 10:10 CST.

Интересные порты на 10.10.1.48:

Не показано: 994 закрытых порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

21/TCP открытый FTP

22/TCP открытый SSH

25/TCP открытый SMTP

80/tcp открыть http

111/tcp открыть rpcbind

2049/tcp открыть nfs

MAC-адрес : 00:0C:29:D5:38:F4 (VMware)

Nmap выполнено: 1 IP-адрес (1 x ост работает) сканируется за 1,52 секунды.

Сканирование цели с использованием фрагментированных пакетов

Опция `-f` указывает Nmap отправлять небольшие 8-байтовые пакеты, таким образом фрагментируя

исследовать множество очень маленьких пакетов. Эта опция не особенно полезна в повседневной жизни.

ситуации; однако это может быть полезно при попытке уклониться от некоторых старых или

неправильно настроенные брандмауэры.

Кончик

Некоторые операционные системы могут потребовать комбинированного использования `--send-eth`.  
с `-f` для правильной передачи фрагментированных пакетов.

## Укажите конкретный MTU

Опция `--mtu` ис пользуется для указания пользовательского MTU (максимальной единицы передачи).

Синтаксис использования : `nmap --mtu [номер] [цель]`

```
# nmap --mtu 16 10.10.1.48
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-11-11, 10:11 CST.

Интересные порты на 10.10.1.48:

Не показано: 994 закрытых порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
21/TCP открытый FTP	
22/TCP открыть SSH	
25/TCP открыть SMTP	
80/tcp открыть http	
111/tcp открыть rpcbind	
2049/tcp открыть нfc	
MAC-адрес : 00:0C:29:D5:38:F4 (VMware)	

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 0,34 секунды.

### Указание конкретного MTU

Опция `--mtu` аналогична опции `-f` (обсуждается на стр. 117), за исключением того, что она позволяет

вы можете указать свой собственный MTU, который будет использоваться во время сканирования. Это создает фрагментированную пакеты, которые потенциально могут быть сбиты с толку некоторые межсетевые экраны. В приведенном выше примере

Аргумент `--mtu 16` указывает Nmap использовать для сканирования крошечные 16-байтовые пакеты.

Примечание	MTU должен быть кратен 8 (например, 8, 16, 24, 32 и т. д.).
------------	---

Кончик	Некоторые операционные системы могут потребовать комбинированного использования <code>--send-eth</code> с <code>--mtu</code> для правильной передачи фрагментированных пакетов.
--------	---

Используйте приманку

Опция -D используется для маскировки сканирования Nmap с использованием одной или нескольких ложных целей.

Синтаксис использования : nmap -D [decoy1,decoy2 и т. д | RND:номер] [цель]

```
# nmap -D RND:10 10.10.1.48
```

Запуск Nmap 5.00 ( http://nmap.org ) в 2009-11-02, 16:41 CST.

...

Маскирование сканирования с использованием 10 случайно генерированных IP-адресов ловушек.

При выполнении ложного сканирования Nmap будет подделывать дополнительные пакеты от указанное количество адресов ловушек. Это фактически создает впечатление, что цель сканируется несколькими системами одновременно. Использование приманок позволяет фактический источник сканирования «сливается с толпой», что затрудняет отслеживание откуда идет сканирование.

В приведенном выше примере nmap -D RND:10 инструктирует Nmap сгенерировать 10 случайных приманок. Вы также можете указать адреса ловушек вручную используя следующий синтаксис :

nmap -D приманка1, приманка2, приманка3 и т. д

Прежде

Использование слишком большого количества ложных целей может привести к перегрузке сети и снижению эффективности сканирования. Кроме того, некоторые интернет-провайдеры могут фильтровать поддельный трафик, что снижает эффективность использования приманки, позволяющей скрыть вашу деятельность по сканированию

Сканирование зомби в режиме ожидания

Опция `-sI` ис используется для сканирования зомби в режиме ожидания.

Синтаксис использования : nmap -sI [хост-зомби] [цель]

```
# nmap -sI 10.10.1.41 10.10.1.252
```

Запуск Nmap 5.00 (http://nmap.org) 14 ноя бря 2009 г., 18:35 CST.

Сканирование в режиме ожидания с ис использованием зомби 10.10.1.41 (10.10.1.41:443); Класс : Инкрементный  
Интересные порты на 10.10.1.252:

Не показано: 997 закрытых | отфильтрованных портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

135/tcp открыть msrpc

139/tcp открыть netbios-ssn

445/TCP открыть Microsoft-DS

MAC-адрес : 00:25:64:D7:FF:59 (Dell)

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 8,29 секунды.

Ис пользование не работающими зомби для сканирования цели

Сканирование бездействующими зомби — это уникальная техника сканирования, позволяющая ис пользовать  
пространство систеи и ис пользуите ее для сканирования целевой систеи. В этом примере 10.10.1.41 — это  
зомби, а 10.10.1.252 — целевая систея. Сканирование работает, ис пользуя  
предлагаемую генерацию идентификатора IP-последовательности, ис пользуя некоторыми систеами. Для того чтобы  
чтобы сканирование в режиме ожидания было успешным, систея зомби должна дейстивительно прослушивать в момент  
сканирование.

При этом сканировании пробные пакеты не отправляются из вашей систеи в цель;

Примечание  
Хотя первоначальный пинг-пакет будет отправлен цели, если вы не  
объедините `-PN` с `-sI`.

Более подробную информацию сканировании зомби в режиме ожидания можно найти на веб-сайте Nmap по адресу:

[www.nmap.org/book/idlescan.html](http://www.nmap.org/book/idlescan.html).

## Вручнуюкажите номер портаисточника

Опция `--source-port`используется для ручногоуказания номераисходногопорта зонд.

Синтаксисиспользования : nmap `--source-port` [порт] [цель]

```
# nmap --source-port 53 scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) 16 декабря 2009 г., 16:41 CST.

Интересные порты на [scanme.nmap.org](http://scanme.nmap.org) (64.13.134.52):

Непоказано: 993 отфильтрованных порта.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

25/TCP	закрытый smtp
--------	---------------

53/TCP	открытый домен
--------	----------------

70/TCP	закрытый cullsник
--------	-------------------

80/TCP	открытый http
--------	---------------

110/tcp	закрыт, pop3
---------	--------------

113/tcp	закрытая авторизация
---------	----------------------

31337/tcp	закрыт Элитный
-----------	----------------

Nmap выполнено: 1 IP-адрес (1 x остается) сканируется за 7,59 секунды.

Ручноеуказаниеномера портаисточникапакета

Каждыйсегмент TCP помимо номера порта назначения содержит номер портаисточника. К тому же Nmap случайным образом выберет дослужебный исходный порт для проверки цели. Опция `--source-port` заставляет Nmap использовать указанный порт в качестве источника всех пакетов. Этот метод можно использовать для использования слабых мест в межсетевых экранах, которые неправильнонастроены на слепой прием исходных пакетов отрафика на основе определенного номера порта. Порт 20 (FTP), порт 53 (DNS) и 67 (DHCP) являются общими портами, подверженныэтому типусканирования.

**Совет.** Параметр `-S`являетсяярлыком, синонимом `--source-port`.

## Добавить с случайные данные

Опция `--data-length` можно использовать для добавления с случайных данных для проверки пакетов.

Синтаксис использования : `nmap --data-length [число] [цель]`

```
# nmap --data-length 25 10.10.1.252
```

Запуск Nmap 5.00 (http://nmap.org) 14 ноя бря 2009 г., 18:41 CST.

Интересные порты на 10.10.1.252:

Не показано: 995 отфильтрованных портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
135/tcp	открыть msrpc
139/tcp	открыть netbios-ssn
445/TCP	открыть Microsoft-DS
5800/tcp	открыть vnc-http
5900/TCP	открыть VNC

Nmap выполнено: 1 IP-адрес (1 x осталось работать) сканируется за 5,17 секунды.

Заполнение сканирования с случайными данными, чтобы избежать обнаружения

Nmap передает пакеты, которые обычно имеют определенный размер. Некоторые поставщики брандмаузеров знают, что нужно исключить этот тип предсказуемого размера пакета. Опция `--data-length` добавляет указанное количество дополнительных данных для зондов, чтобы обойти эти виды проверок. В приведенном выше примере к основному пакету добавляется 25 дополнительных байтов, направленных цели.

Случайный порядок сканирования целей

Опция `--randomize-hosts` используется для рандомизации порядка сканирования указанные цели.

Синтаксис использования : `nmap --randomize-hosts [цели]`

```
$ nmap --randomize-hosts 10.10.1.100-254
```

Интересные порты на 10.10.1.109:

Не показано: 996 отфильтрованных портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
139/tcp	открыть netbios-ssn
445/TCP	открыть Microsoft-DS
5800/tcp	открыть vnc-http
5900/TCP	открыть VNC

MAC-адрес : 00:1C:23:49:75:0C (Dell)

Интересные порты на 10.10.1.100:

Не показано: 996 отфильтрованных портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
139/tcp	открыть netbios-ssn
445/TCP	открыть Microsoft-DS
5800/tcp	открыть vnc-http
5900/TCP	открыть VNC

MAC-адрес : 00:21:9B:3F:AC:EC (Dell)

Интересные порты на 10.10.1.107:

Не показано: 997 закрытых портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
22/TCP	открыть SSH
139/tcp	открыть netbios-ssn

...

Сканирование системы в случайному порядке

Параметр `--randomize-hosts` помогает предотвратить сканирование нескольких целей.

обнаруживаются межсетевыми экранами и системами обнаружения вторжений. Это делается путем сканирования в случайному порядке, а не последовательно.

## Подделать MAC-адрес

`--spoof-mac` используется для подмены MAC-адреса (управления доступом к сетеям передачи) сетевое устройство.

Синтаксис использования : `nmap --spoof-mac [вндор|MAC|0] [цель]`

```
# nmap -sT -PN --spoof-mac 0 192.168.1.1
```

Запуск Nmap 5.00 ( <http://nmap.org> ) 15 января 2010 г., 19:48 CST.

Подмена MAC-адреса 00:01:02:25:56:AE (3com)

Интересные порты на 192.168.1.1:

Не показано: 995 отфильтрованных портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

20/tcp закрыты ftp-данные

21/TCP закрытый FTP

23/tcp закрытый телнет

80/tcp открыт http

2869/tcp открыт неизвестно

Nmap выполнено: 1 IP-адрес (1 x осто работает) сканируется за 4,78 секунды.

Использование поддельного MAC-адреса

В этом примере Nmap поручено создать случайно сгенерированный MAC-адрес 3com.

адреса. Это затрудняет отслеживание вашей активности сканирования, поскольку ваш MAC-адрес отображается в цепочку истории.

Опцией `--spoof-mac` можно управлять с помощью следующих параметров:

Аргумент 0	Функция
(ноль)	Генерирует случайный MAC-адрес
Конкретный MAC-адрес. Использует указанный MAC-адрес.	
Имя поставщика	Генерирует MAC-адрес от указанного поставщика (например, Apple, Dell, 3Com и т. д.)

Варианты подмены MAC-адреса

Отправлять неверные контрольные суммы

**Опция** `--badsum` ис пользуется для отправки пакетов с неверными контрольными суммами на указанный хост.

Синтаксис использования : nmap --badsum [цель]

```
# nmap --badsum 10.10.1.41
```

Запуск Nmap 5.00 (<http://nmap.org>) в 24 авг уста 2009 г., 16:19 CDT.

Все 1000 сканируемых портов на 10.10.1.41 фильтруются.

MAC-адрес : 00:60:B0:59:B6:14 (Hewlett-Packard CO.)

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 21,40 секунды.

Сканирование цели с использованием неверных контрольных сумм

Протокол TCP/IP ис пользует контрольные суммы для обеспечения целостности данных. Создание пакетов с плохие контрольные суммы могут в некоторых редких случаях привести к ответу плохого настроенной системы. В приведенном выше примере мы не получили никаких результатов, то есть целивая система настроена правильно. Это типичный результат при использовании `--badsum` вариант.

#### Примечание

Только плохие сконфигурированной системы ответит на пакет с плохим контрольная сумма. Тем не менее, это хороший инструмент для аудита сети. безопасости или попытка обойти брандмауэры.



Раздел 9:

Опции вывода

## Обзор опций вывода

Nmap предлагает несколько вариантов создания форматированного вывода. Помимо отображения стандартный вывод на экран, вы также можете сортировать результаты сканирования в текстовом файле XML файл или односторонний файл grepable. Эта функция может быть полезна при сканировании больших количеств систем или для сравнения результатов двух сканирований с помощью утилиты ndiff (обсуждается в разделе 13).

## Примечание

Утилита сопоставления шаблонов grep доступна только в Unix, Linux и Системы Mac OS X по умолчанию. Пользователи Windows могут загрузить порт Win32. программы GNU grep по адресу <http://gnuwin32.sourceforge.net> для использования с примерами, обсуждаемые в этом разделе.

Краткое описание функций, описанных в этом разделе:

Особенность	Вариант
Сортировать вывод в текстовый файл	-na
Сортировать вывод в файл XML	-oX
Грепаемый вывод	-и
Вывод всех поддерживаемых типов файлов	-oA
Периодический вывод статистики	--stats-каждый
133t	-ты

## СохраниТЬ вывод в текСтоВЫЙ файл

Параметр -oN соХраняЕт резульТаты сканирования в текСтоВом файле.

Синтаксис использования : nmap -oN [scan.txt] [цель]

```
$ nmap -oN scan.txt 10.10.1.1
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-13, 15:17 CDT.

Интересные порты на 10.10.1.1:

Не показано: 998 закрытых портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

80/tcp открыть http

443/TCP открыть https

Nmap выполнен 1 IP-адрес (1 хост работает) сканируется за 0,47 секунды.

Сохранение вывода Nmap в текСтоВый файл

Результаты вышеуказанных сканирования соХраняЮтся в файл scan.txt, показанный ниже.

```
$ cat scan.txt
```

# Сканирование Nmap 5.00 инициализировано четверг 13 августа 15:17:16 2009 как: nmap -oN сканирование.txt 10.10.1.1

Интересные порты на 10.10.1.1:

Не показано: 998 закрытых портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

80/tcp открыть http

443/TCP открыть https

# Nmap выполнен в четверг, 13 августа 15:17:17 2009 г. - 1 IP-адрес (1 хост работает) сканируется за 0,47 секунды

Просмотр содержимого файла scan.txt

### Примечание

Nmap перезапишет существующий выходной файл, если не будет указан параметр --append-output. опция считается с -oN.

## Сохранить вывод в файл XML

Параметр -oX сохраняет результаты сканирования в XML-файле.

Синтаксис использования : nmap -oX [scan.xml] [цель]

```
$ nmap -oX scan.xml 10.10.1.1
```

Запуск Nmap 5.00 ( http://nmap.org ) в 2009-08-13 15:19 CDT.

Интересные порты на 10.10.1.1:

Не показано: 998 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

80/tcp открыть http

443/TCP открыть https

...

Создание выходного XML-файла

Результаты вышеуказанного сканирования сохраняются в файле scan.xml, показанном ниже.

```
$ cat scan.xml
<?xml версия ="1.0" ?>
<?xml-stylesheet href="file:///usr/local/share/nmap/nmap.xsl"
тире="текст/xsl"?>
<!-- Сканирование Nmap 5.00 начато четверг 13 авг утра 15:19:44 2009 как: nmap -oX
сканирование.xml 10.10.1.1 -->
<nmaprun Scanner="nmap" args="nmap -oX scan.xml 10.10.1.1"
start="1250194784" startstr="Чт, 13 авг утра 15:19:44 2009" version="5.00"
...>
```

Просмотр с содержимого выходного XML-файла

Полученный XML-файл имеет жестко заданные пути к файлам, которые могут работать только в системе,

где был создан файл. Параметр --webxml можно комбинировать с -oX для

создать переносимый файл для любой системы (доступом в Интернет). Вы также можете указать

альтернативная таблица стилей с использованием параметра --stylesheet . Чтобы избежать ссылки на стиль

лист вообще, используйте параметр --no-stylesheet .

## Гrepаемый вывод

Опция `-oG` включает вывод grepable.

Синтаксис использования : nmap -oG [scan.txt] [цель]

```
$ nmap -oG scan.txt -F -O 10.10.1.1/24
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-13, 15:50 CDT.

Интересные порты на 10.10.1.1:

Найдено 998 закрытых портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

80/tcp открыть http

443/TCP открыть https

...

Создание вых одног о файла grepable

Результат сканирования с ох раня ется в указанный текстовый файл, что может быть полезно при

в сочетании с инструментами синтаксического анализа текста, такими как Perl или grep (как показано ниже).

```
$ grep "Windows 98" scan.txt
```

Xос т: 10.10.1.217 Порты: 139/open/tcp//netbios-ssn///,

5800/open/tcp//vnc-http///, 5900/open/tcp//vnc/// Игнорируемое состояние:

закрыто (97)	ОС: Microsoft Windows 98 SE.	Индекс сканирования : 18
--------------	------------------------------	--------------------------

IP-адрес инфагор

Seq: Сломанный инкрементный метод с прямым порядком байтов

...

Использование утилиты grep для просмотра вых одног о файла Nmap

В приведенном выше примере утилита grep отобразит все примеры указанного текста.

находится в файле scan.txt. Это упрощает быстрый поиск конкретных

информаций при анализе результатов большого сканирования.

## Вывод всех поддерживаемых типов файлов

Параметр -oA с ох раня ет результаты сканирования в форматах text, grepable и XML.

Синтаксис использования : nmap -oA [имя файла] [цель]

```
$ nmap -oA сканирует 10.10.1.1
```

Запуск к Nmap 5.00 (<http://nmap.org>) в 2009-08-13, 16:10 CDT.

Интересные порты на 10.10.1.1:

Не показано: 998 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

80/tcp открыть http

443/TCP открыть https

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 0,66 секунды.

Создание всех одных файлов для всех доступных форматов

Все одные файлы результируют сканирования создаются соответствующими расширениями, как отображается ниже.

```
$ ls -l сканирует.*
```

```
-rw-r--r-- 1 ник ник 284 13.08.2009 16:22 scans.gnmap
-rw-r--r-- 1 ник ник 307 2009-08-13 16:22 scans.nmap
-rw-r--r-- 1 ник ник 5150 13.08.2009 16:22 scans.xml
```

Список каталогов полученных всех одных файлов

Файл	Содержание
scans.gnmap	Гrepаемый вывод
scans.nmap	Обычный текстовый вывод
сканы.xml	XML-вывод

Все одные файлы Nmap

Отображение статистики сканирования

Опция `--stats-every` можно использовать для периодического отображения статуса текущего сканирования.

Синтаксис использования : `nmap --stats-every [время] [цель]`

```
$ nmap --stats-every 5s 10.10.1.41
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-13, 16:30 CDT.

Статистика: Прошло 0:00:07; 0 x сканирование завершено (1 работает), 1 проходит сканирование с сервисом

Сроки с сервисом сканирования : выполнено около 55,00%; ETC: 16:30 (осталось 0:00:05)

Статистика: Прошло 0:00:12; 0 x сканирование завершено (1 работает), 1 проходит сканирование с сервисом

Сроки с сервисом сканирования : выполнено около 85,00%; ETC: 16:30 (осталось 0:00:02)

Статистика: Прошло 0:00:17; 0 x сканирование завершено (1 работает), 1 проходит сканирование с сервисом

Сроки с сервисом сканирования : выполнено около 90,00%; ETC: 16:30 (осталось 0:00:02)

Статистика: Прошло 0:00:22; 0 x сканирование завершено (1 работает), 1 проходит сканирование с сервисом

Сроки с сервисом сканирования : выполнено около 90,00%; ETC: 16:30 (осталось 0:00:02)

Статистика: Прошло 0:00:27; 0 x сканирование завершено (1 работает), 1 проходит сканирование с сервисом

Сроки с сервисом сканирования : выполнено около 90,00%; ETC: 16:30 (осталось 0:00:03)

Статистика: Прошло 0:00:32; 0 x сканирование завершено (1 работает), 1 проходит сканирование с сервисом

...

Выход с тату сканирования Nmap

При медленном сканировании вам может показаться долгое ожидание на экране, ничего не делая. Периоды времени. Опция `--stats-every` может решить эту проблему. В приведенном выше примере, `--stats-every 5s` указывает Nmap отображать статус текущего сканирования каждые пять секунд. Параметры времени могут быть указаны в секундах (с), минутах (м), или часах (ч), добавив с, м или ч к номеру интервала, как описано на странице 99.

## 133т Вых од

[Technet24.ir](#)

Опция -oS включает вывод «script kiddie».

Синтаксис использования : nmap -oS [scan.txt] [цель]

```
$ nmap -oS scan.txt 10.10.1.1
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-13, 15:45 CDT.

Интересные порты на 10.10.1.1:

Не показано: 998 закрытых портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

80/tcp Открыть http

443/TCP Открыть https

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 0,48 секунды.

Создание вых одног о файла «133т»

Script kiddie или «leet» talk — это вывод — загадочная форма набора текста, используемая в OS X в основном незрелые подростки на основе обычных выражений и в чатах. Эта опция включена как шутка и на самом деле бесполезна для чего, кроме как посмеяться. Результаты -oS со временем могут быть найдены в файле scan.txt, показанном ниже.

```
$ кот scan.txt
```

ЗАПУСК NMap 5.00 ( <http://nmap.org> ) 13 августа 2009 г., 15:45 CDT

!nt3r3St!ng порты On 10.10.1.1:

Н0т \$h0wn: 998 cl0\$3d p0rt\$

PORT	STATE СЕРЕВЕР
------	---------------

80/tcp Открыть hTtp

443/tcp Open https

Nmap Вы ПОЛНЕНО: 1 IP-адрес (1 хост подключен) сканирован за 0,48 \$3conds

Детский вывод скрипта Nmap

## Раздел 10:

Устранение неполадок и отладка

## Обзор с трансляции неполадок и отладки

Технические проблемы являются неотъемлемой частью использования компьютеров. Nmap не является исключением.

Иногда сканирование может не дать ожидаемого результата; вы можете получить

ошибку – или вы можете вообще не получить никакого вывода. Nmap предлагает несколько вариантов отслеживания и отладки сканирования, что может помочь определить, почему это происходит.

В следующем разделе подробно описаны эти функции и их сущность неполадок и отладки.

Краткое описание функций, описанных в этом разделе:

Особенность	Вариант
Получать помощь	-help
Показать версию Nmap	-V
Подробный вывод	-v
Отладка	-d
Отображение причины состояния порта	-- причина
Отображать только открытые порты	--открыть
Трассировка пакетов	--packet-trace
Отображение сетевых состояний	-iflist
Укажите сетевой интерфейс	-Это

## Получать помощь

Выполнение nmap -h отобразит с вводу доступных опций.

Синтаксис использования : nmap -h

```
$ nmap -h
Nmap 5.00 (http://nmap.org)
Использование: nmap [Типы сканирования] {целевая сpecificация}
ЦЕЛЕВАЯ СПЕЦИФИКАЦИЯ:
    Может передавать имена хостов, 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>: ввод из списков хостов/сетей.
-iR <количество хостов>: выбрать случайные цели.
-exclude <x host1[,x host2][,x host3],...>: исключить хосты/сети
-excludefile <исключаемый_файл>: исключить список из файла
...
...
```

Отображение справочной информации Nmap

Для получения более подробной информации вы можете прочитать страницу руководства Nmap, набрав man nmap в командной строке.

\$ человек nmap

Доступ к странице руководства Nmap в системах Unix и Linux

**Примечание** Команда nmap доступна только в системах на базе Unix, Linux и Mac OS X.

Системы. Пользователи Windows могут прочитать руководство Nmap онлайн по адресу [www.nmap.org/book/man.html](http://www.nmap.org/book/man.html).

**Кончик** Вы также можете получить помощь в Интернете, подписавшись на список рассылки Nmap по адресу: [www.seclists.org](http://www.seclists.org).

## Показать версия Nmap

Опция `-V` используется для отображения установленной версии Nmap.

Синтаксис использования : nmap -V

```
$ nmap -V
```

Nmap версия 5.00 (<http://nmap.org>)

Отображение установленной версии Nmap

При устранении проблем с Nmap вы всегда должны убедиться, что вас есть

установлена самая последняя версия. Разработаны программы с открытым исходным кодом, такие как Nmap.

вместом тем, ошибки обычно исправляются, как только они обнаруживаются. Сравнивать

установленными версиями последнюю версию документации на веб-сайте Nmap по адресу

[www.nmap.org](http://www.nmap.org), чтобы убедиться, что вы используете самую последнюю версию

этого гарантирует, что у вас будет доступ к новейшим функциям, а также к большинству ошибок.

доступна бесплатная версия.

## Подробный вывод

Опция `-v` используется для включения подробного вывода.

Синтаксис использования : `nmap -v [цель]`

```
$ nmap -v scanme.insecure.org
```

Запуск Nmap 5.00 ( <http://nmap.org> ) в 2009-08-12 15:06 CDT.

NSE: Заружено 0 скриптов для сканирования.

Начинаю пинг-сканирование в 15:06.

Сканирование 64.13.134.52 [2 порта]

Завершено пинг-сканирование в 15:06, прошло 1,87 с (всего 1 хост)

Иницирование параллельного разрешения DNS для 1 хоста в 15:06

Завершено параллельное разрешение DNS 1 хоста в 15:06, прошло 0,16 с.

Запуск сканирования подключения в 15:06

Сканирование scanme.nmap.org (64.13.134.52) [1000 портов]

Обнаружен открытый порт 53/tcp на 64.13.134.52.

Обнаружен открытый порт 80/tcp на 64.13.134.52.

Сканирование подключения завершено в 15:06, прошло 7.00 с (всего 1000 портов).

Хост scanme.nmap.org (64.13.134.52) работает (задержка 0,087 с).

Интересные порты на scanme.nmap.org (64.13.134.52):

Не показано: 998 отфильтрованных портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

53/TCP	открытый домен
--------	----------------

80/TCP	открытый http
--------	---------------

Чтение файлов данных из: /usr/local/share/nmap

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 9,41 секунды.

Сканирование Nmap с включенным подробным выводом

Подробный вывод может быть полезен при устранении проблем с подключением или если вы просто интересуетесь тем, что происходит за кулисами вашего сканирования.

Кончик

Вы можете использовать опцию `-vv` дважды (`-v -v` или `-vv`), чтобы включить дополнительную подробную информацию

вывода.

## Отладка

Опция `-d` включает вывод отладки.

Синтаксис использования : nmap -d[1-9] [цель]

```
$ nmap -d scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-08-12, 15:26 CDT.

ПОРТЫ : использование 1000 наиболее открытых портов (TCP:1000, UDP:0, SCTP:0).

----- Отчет о времени -----

Группы хостов: мин 1, макс 100000

rtt-таймауты: инициализация 1000, мин 100, макс 10000

максимальная задержка сканирования : TCP 1000, UDP 1000, SCTP 1000

параллелизм: мин 0, макс 0

максимальное количество попыток: 10, таймаут хоста: 0

минимальная скорость: 0, максимальная скорость: 0

NSE: Загружено 0 скриптов для сканирования .

Запуск пинг-сканирования в 15:26

Сканирование 64.13.134.52 [2 порта]

Завершено пинг-сканирование в 15:26, прошло 2,83 с (всего 0 xhost)

Общая скорость отправки: 1,06 пакетов/с .

Mass\_rdns: Использование DNS-сервера 10.10.1.44

Mass\_rdns: Использование DNS-сервера 10.10.1.45

Иницирование параллельного разрешения DNS для 1 xhost в 15:26

Mass\_rdns: 0,00 с 0/1 [#: 2, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]

Завершено параллельное разрешение DNS 1 xhost в 15:26, прошло 0.00с

...

Выход отладки Nmap

Вывод отладки предоставляет дополнительную информацию, которую можно использовать для отслеживания ошибок или решения проблем. Вывод по умолчанию -d обеспечивает достаточно отладку.

информации . Вы также можете указать уровень отладки 1-9, который будет использоваться с параметром -d. Параметр для увеличения или уменьшения объема вывода. Например: -d1 обеспечивает самый низкий объем вывода отладки, а -d9 — самый высокий.

## Отображение кодов причин состояния порта

Параметр --reason отображает причину, по которой порт считается находящимся в данное состояние.

Синтаксис использования : nmap --reason [цель]

```
$ nmap --reason scanme.insecure.org
```

Запуск Nmap 5.00 (http://nmap.org) в 2009-08-12 15:43 CDT.

Интересные порты на scanme.nmap.org (64.13.134.52):

Не показано: 993 отфильтрованных порта.

Причина: 993 отсутствия ответа

ПОРТ	ГОСУДАРСТВЕННАЯ УСЛУГА АПРИЧИНА
------	---------------------------------

25/TCP	закрытый smtp	conn-отказался
--------	---------------	----------------

53/TCP	с инкрементацией открытого домена	
--------	-----------------------------------	--

70/TCP	закрытый с использованием conn-отказался	
--------	--	--

80/TCP	открытый http	зрелище-о
--------	---------------	-----------

110/tcp	закрыт, pop3	conn-отказался
---------	--------------	----------------

113/tcp	закрытая авторизация	conn-отказался
---------	----------------------	----------------

31337/tcp	закрыт Elite	conn-отказался
-----------	--------------	----------------

Nmap выполнено: 1 IP-адрес (1 x открыт) работает сканируется за 8,83 секунды.

Сканирование Nmap с включенным кодом причин состояния порта

Обратите внимание на добавление поля причины в приведенном выше сканировании. Информация в этой области может быть полезна при попытке определить, почему порты цели находятся в определенном состоянии. Порты, отвечающие Syn-ack, считаются открытыми. Порты, которые отвечают conn-refused или сброс обычного закрыты. Порты, которые вообще не отвечают, обычно фильтруются (брандмауэром).

Отображать только открытые порты

Параметр `--open` указывает Nmap отображать только открытые порты.

Синтаксис использования : nmap --open [цель]

```
$ nmap --open scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-12-18, 12:47 CST.

Интересные порты на [scanme.nmap.org](http://scanme.nmap.org) (64.13.134.52):

Не показано: 993 фильтруемых порта, 5 закрытых портов.

ГОСУДАРСТВЕННАЯ СЛУЖБА ПОРТА

53/TCP открытый домен

80/tcp открыть http

Nmap выполнено: 1 IP-адрес (1 x остановлен) сканируется за 8,26 секунды.

Ограничение вывода Nmap для отображения только открытых портов

Параметр `--open` удаляет закрытые и отфильтрованные порты из результатов сканирования . Этот опция полезна, если вы хотите просмотреть результаты сканирования , чтобы отображались только отображаются открытые порты. Отображается сканирование без опции `--open` .

ниже для сравнения .

```
$ nmap scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-12-18, 12:49 CST.

Интересные порты на [scanme.nmap.org](http://scanme.nmap.org) (64.13.134.52):

Не показано: 993 отфильтрованных порта.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

25/TCP закрытый smtp

53/TCP открытый домен

70/TCP закрытый сурсик

80/TCP открыть http

110/tcp закрыт, pop3

113/tcp закрытая авторизация

...

Сканирование Nmap, отображающее открытые и закрытые порты

## Трас с ировки пакетов

Параметр `--packet-trace` указывает Nmap отображать с водку всех пакетов, отправил и получил.

Синтаксис использования : nmap --packet-trace [цель]

```
$ nmap --packet-trace 10.10.1.1
Запуск Nmap 5.00 ( http://nmap.org ) в 2009-08-13 17:14 CDT.

CONN (0,1600 c) TCP localhost > 10.10.1.1:80 => Операц ия сейчас выполняется
CONN (0,1600 c) TCP localhost > 10.10.1.1:443 => Операц ия сейчас выполняется
NSOCK (0,1610 c) UDP-сединение запрошено на 10.10.1.45:53 (IOD #1) EID 8
NSOCK (0,1610 c) Запрос начтение от IOD #1 [10.10.1.45:53] (тайм-аут: -1 мс) EID 8
NSOCK (0,1610 c) UDP-сединение запрошено на 10.10.1.44:53 (IOD #2) EID 24
NSOCK (0,1610 c) Запрос начтение от IOD #2 [10.10.1.44:53] (тайм-аут: -1 мс) EID 34
NSOCK (0,1610 c) Запрос назапись 40 байт в IOD #1 EID 43 [10.10.1.45:53]:
В!.....1.1.10.10.in-addr.arpa.....
NSOCK (0,1610 c) nssock_loop() запущен (время ожидания = 500 мс). 5 с событий ожидается
Обратный вызов NSOCK (0,1610 c): CONNECT SUCCESS для EID 8 [10.10.1.45:53]
Обратный вызов NSOCK (0,1610 c): CONNECT SUCCESS для EID 24 [10.10.1.44:53]
NSOCK (0,1610 c) Обратный вызов: УСПЕШНАЯ ЗАПИСЬ для EID 43 [10.10.1.45:53]
...
```

Выход трас с ировки пакетов

Параметр `--packet-trace` — еще один полезный инструмент для устранения неполадок с подключением.

проблемы. В приведенном выше примере отображается подробная информация о каждом пакете, отправленном на и получен от целиевой системы.

Кончик

Информация трас с ировки будет быть проектироваться по экрану. См. стр. 129 для информации о сохранении данных трас с ировки в файл для удобства просмотра.

## Отображение конфигурации сети с этих ос та

Опция `--iflist` отображает сетевые интерфейсы и маршруты, настроенные на локальном компьютере.

система.

Синтаксис использования : nmap --iflist

```
$ nmap --iflist
```

Запуск Nmap 5.00 ( <http://nmap.org> ) в 2009-08-13 17:03 CDT.

```
*****ИНТЕРФЕЙСЫ*****
РАЗРАБОТЧИК (КОРОТКИЙ) ИП/МАСКА      ТИП      ВВЕРХ МАК
это      (этот)    127.0.0.1/8      возврат по шлейфу
eth0 (eth0) 10.10.1.107/24 Ethernet вверх 00:21:70:AC:F7:E7
wlan0 (wlan0) 10.10.1.176/24 Ethernet включен 00:16:EA:F0:92:50

*****МАРШРУТЫ *****
Личное время /МАСКА      ШЛЮЗ РАЗРАБОТЧИК
10.10.1.0/0 eth0
10.10.1.0/0 wlan0
169.254.0.0/0 wlan0
0.0.0.0/0      eth0 10.10.1.1
```

Вывод списка интерфейсов

В приведенном выше примере отображается общая информация о сети и маршрутизации для местной системы. Эта опция может быть полезна для быстрого определения сетевой информации или устранение проблем с подключением.

Дополнительные команды, полезные для устранения неполадок в сети конфигурация включает ifconfig (Unix/Linux) и ipconfig (Windows). Большинство системы на базе Windows и Unix также включают команду netstat, который может предоставить дополнительную информацию о сети.

Кончик

## Укажите, какой сетевой интерфейс ис пользовать

Опция -e ис пользуется для того, чтобы вручную указать, какой сетевой интерфейс должен ис пользовать Nmap.

Синтаксис ис пользования : nmap -e [интерфейс] [цель]

```
$ nmap -e eth0 10.10.1.48
```

Запуск Nmap 5.00 ( http://nmap.org ) в 25 авг уста 2009 г., 08:30 CDT.

Интересные порты на 10.10.1.48:

Не показано: 994 закрытых порта.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

21/TCP открытый FTP

22/TCP открыть SSH

25/TCP открыть SMTP

80/tcp открыть http

111/tcp открыть rpcbind

2049/tcp открыть nfs

Nmap выполнено: 1 IP-адрес (1 x OS) работает сканируется за 0,41 секунды.

## Указание сетевого интерфейса вручную

Многие системы имеют не сколько сетевых интерфейсов. Большинство современных ноутбуков, например, иметь как обычный разъем Ethernet, так и беспроводную карту. Если вы хотите убедиться, что Nmap ис пользует предпочтительный вами интерфейс, вы можете ис пользовать -e, чтобы указать его в командной строке. В этом примере -e ис пользуется, чтобы заставить Nmap сканировать через интерфейс eth0 на мультиразмещенной OS-системе.

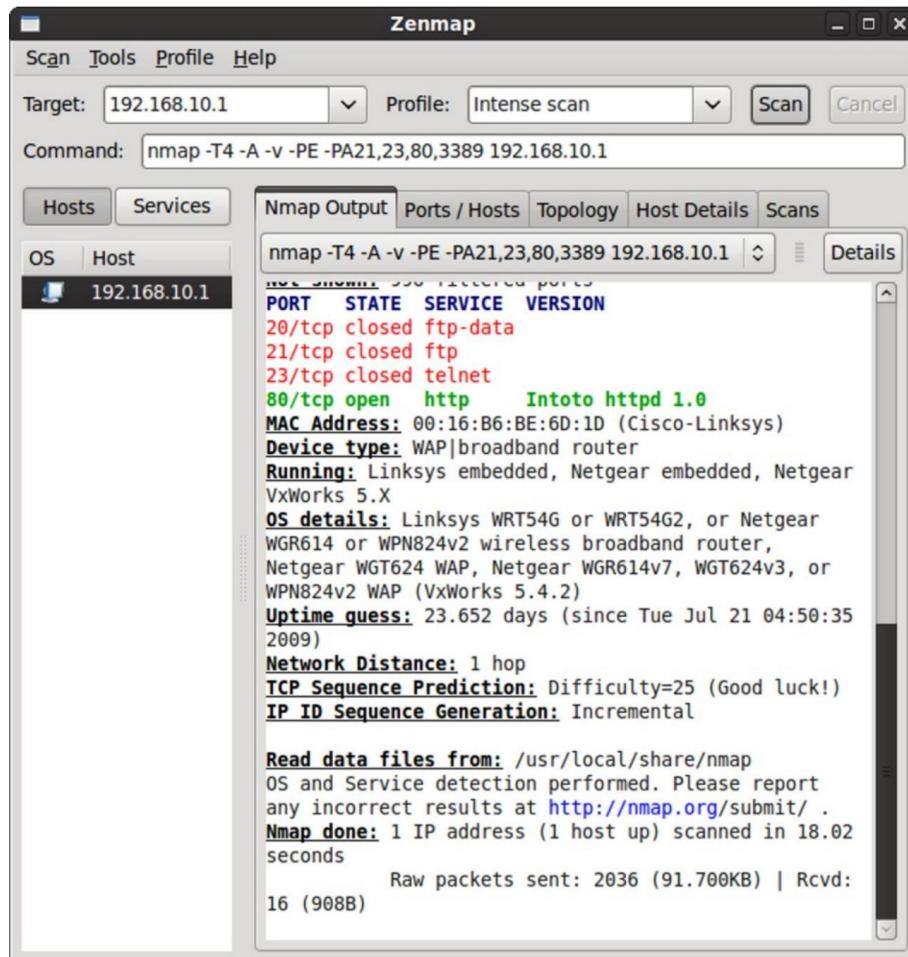


Раздел 11:

Дзенмап

## Обзор Zenmap

Zenmap — это графический интерфейс для Nmap, разработанный для облегчения работы с Nmap. Сложные функции сканирования . Zenmap GUI — это кроссплатформенная программа, которую можно использовать в системах Windows, Mac OS X и Unix/Linux.



Графический интерфейс Zenmap

## Запуск с кейм Zenmap

### Пользователи Windows

Zenmap устанавливается по умолчанию при установке Nmap в системах Windows. Начать

Zenmap: выберите «Пуск» > «Программы» > Nmap > Zenmap GUI.

### Пользователи Unix и Linux

Zenmap устанавливается автоматически при компиляции или Nmap из исходного кода. Если вы

установите Nmap через apt или yum, возможно, вам придется вручную установить пакет Zenmap.

Это можно сделать, выполнив одну из следующих команд:

Debian/Ubuntu: apt-get install zenmap

Fedora/Red Hat/CentOS: yum install zenmap

Gentoo: выйти на zenmap

После установки появится графический интерфейс Zenmap, который можно запустить, выбрав Приложения >

Интернет > Zenmap из меню GNOME.

### Пользователи Mac OS X

Zenmap для Mac OS X устанавливается в разделе «Приложения» > «Zenmap». Это включено

автоматически как часть установки Nmap по умолчанию

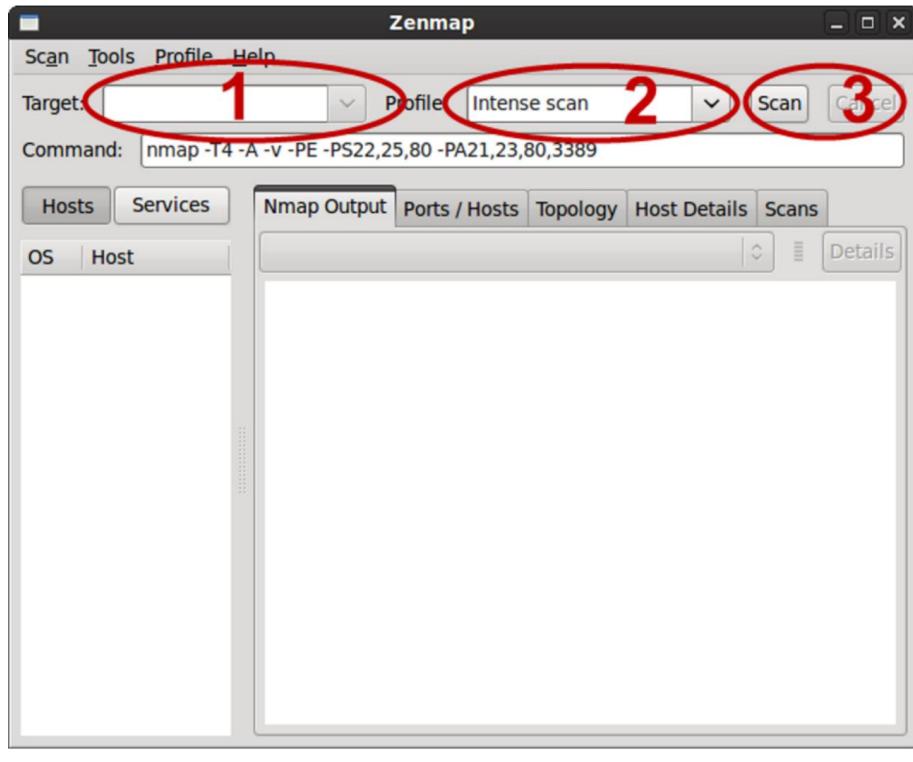
#### Примечание

Сервер X11 для Mac OS X необязателен для запуска Zenmap в системах Mac.

Это программное обеспечение можно найти на установочном DVD-диске Mac OS X.

## Основные операции Zenmap

Выполнить сканирование с помощью Zenmap также просто, как 1, 2, 3...



Шаг 1. Введите цель (или выберите недавноцель из списка).

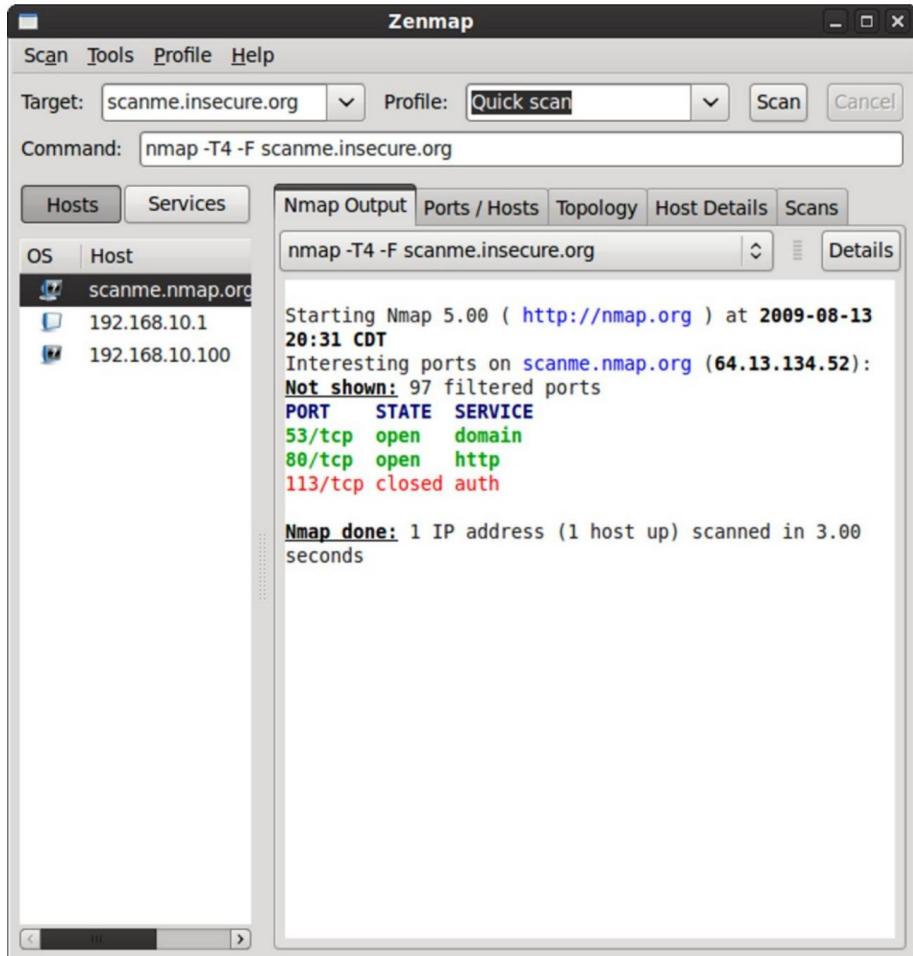
Шаг 2. Выберите профиль сканирования

Шаг 3. Нажмите кнопку сканирования .

## Результаты Zenmap

Результаты сканирования отображаются после завершения сканирования. Вывод Nmap

Вкладка отображает необработанные результаты сканирования в том виде, в котором они отображаются в командной строке.



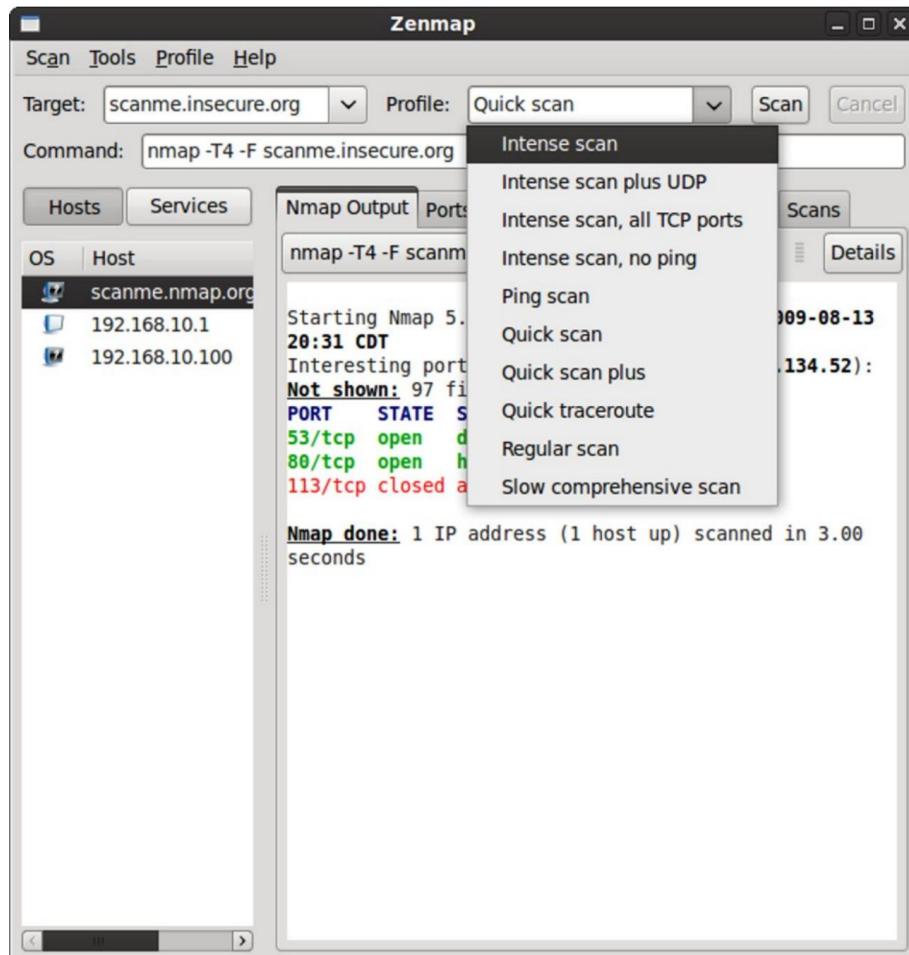
Выходные данные сканирования Zenmap

### Примечание

Фактическая выполненная строка командной строки отображается в командной строке поле выше.

## Сканирование профилей

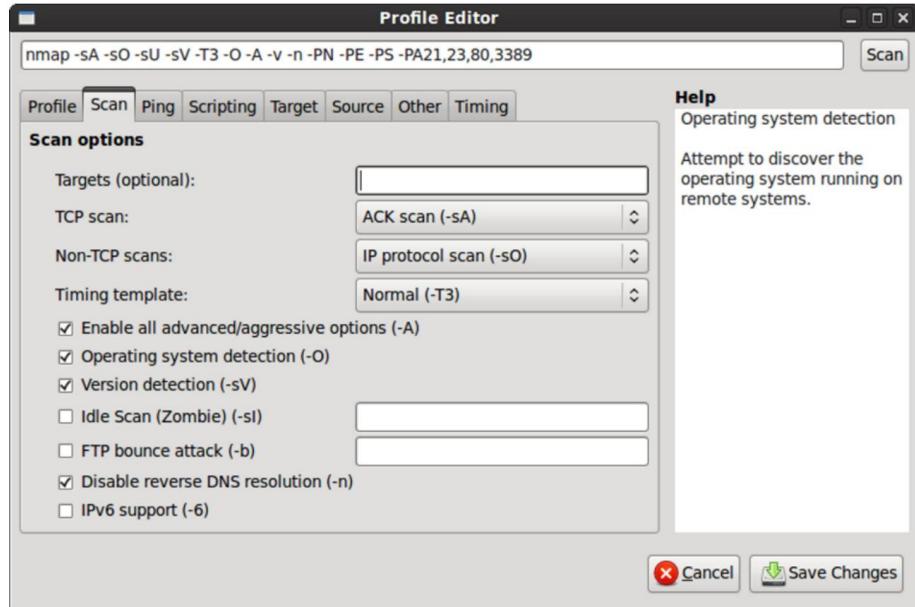
Zenmap предоставляет встроенные профили для наиболее распространенных типов сканирования. Этот упрощает процесс сканирования, устраняя необходимость вручную указывать длинный список аргументов в командной строке.



Профили сканирования Zenmap

## Редактор профиля

Если встроенные сценарии не соответствуют вашим потребностям, вы можете создать собственное сканирование профиля. Для этого просто откройте редактор профиля, выбрав «Профиль» > «Новый профиль» из меню Zenmap (или нажмите CTRL + P на клавиатуре).



Редактор профилей Zenmap

В редакторе профилей Zenmap вы можете выбрать параметры для своего пользовательского профиля.

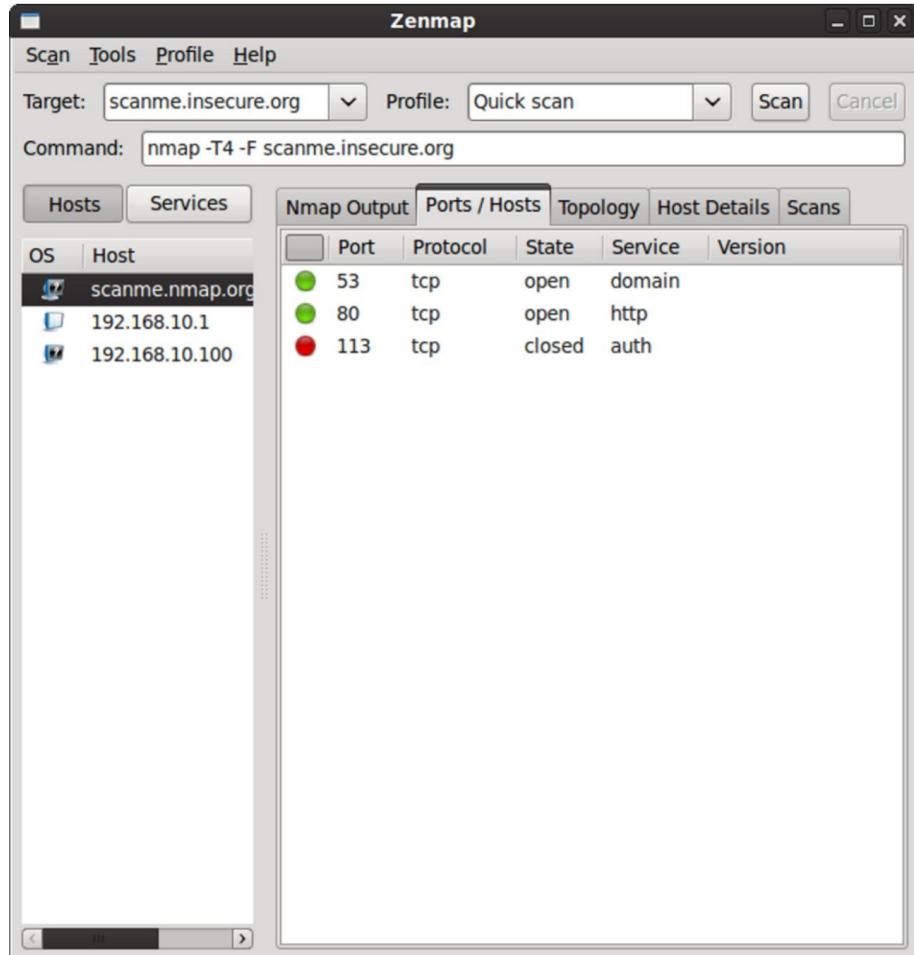
и Zenmap автоматически построит с ложные строки командной строки Nmap на основе

по вашему выбору.

После завершения просто нажмите кнопку «Сохранить изменения», и ваш индивидуальный профиль будет сохранен. Доступен для использования в меню выбора профиля.

## Просмотр открытых портов

После завершения сканирования вы можете просмотреть удобные для пользователя результаты на вкладке «Порты/Хосты». Кнопки с надписью «Хосты» и «Службы» можно использовать для переключения отображение последних сканирований.

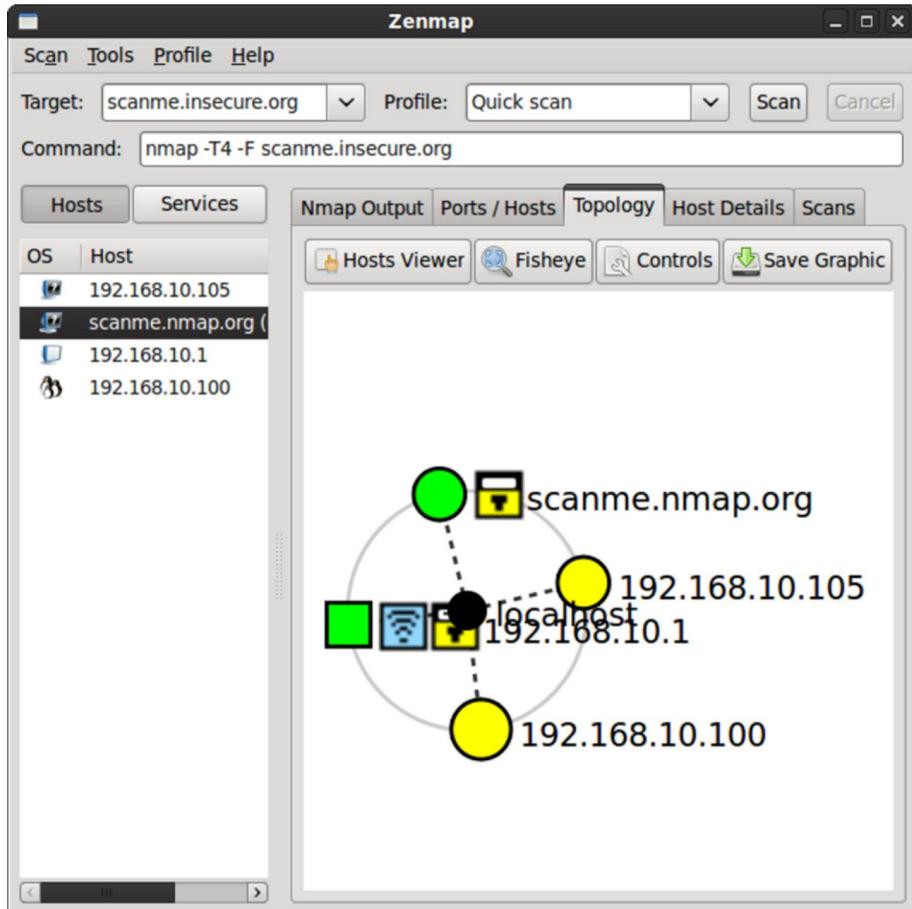


Отображение портов Zenmap

## Просмотр карты сети

[Technet24.ir](#)

После выполнения одного или нескольких сканирований вы можете просмотреть результаты на графической карте на вкладке Топология.



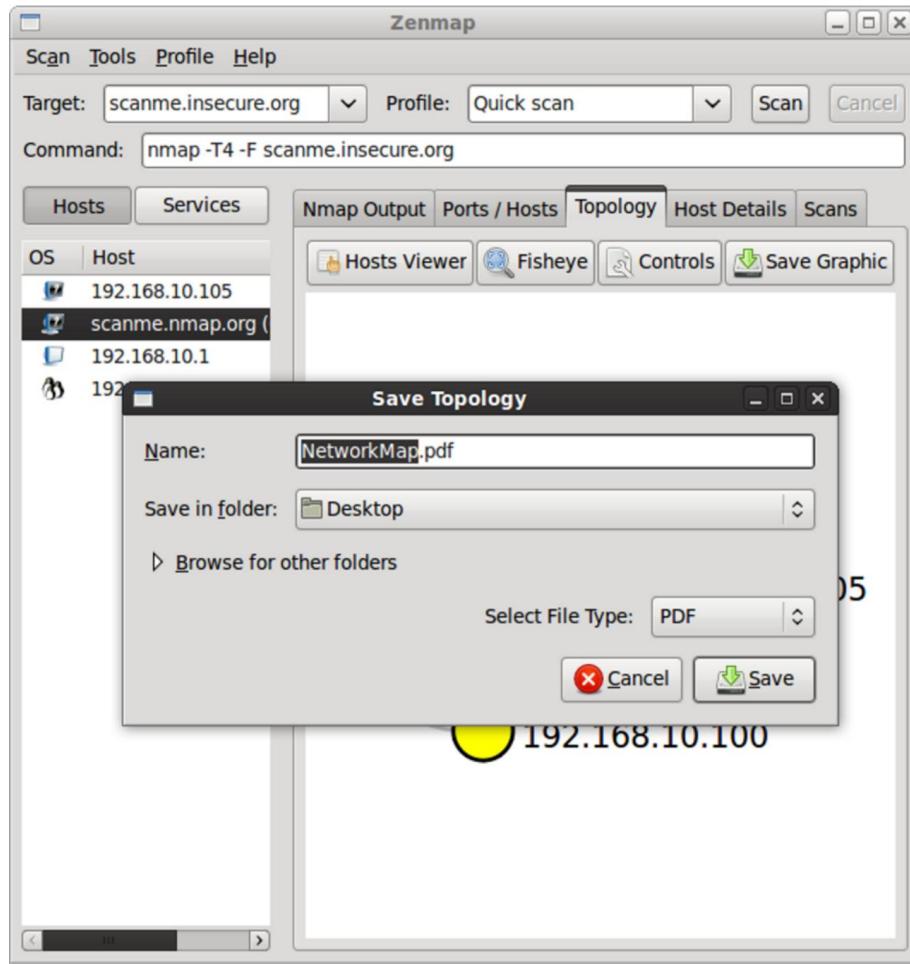
Карта топологии Zenmap

Функция топологии Zenmap предоставляет интерактивную графику, которую можно

манипулировать нажатием кнопки «Управление» для изменения различных параметров отображения.

## Сохранение карты сети

Вы также можете сохранить карту топологии Zenmap, нажав кнопку «Сохранить в графику».



Сохранение карты топологии

Zenmap поддерживает экспорт карт в несколько популярных форматов, включая PNG, PDF, SVG и Postscript крипту.

## Глоссарий сведений о хосте

Вкладка «Сведения о хосте» обеспечивает удобное отображение информации, полученной из

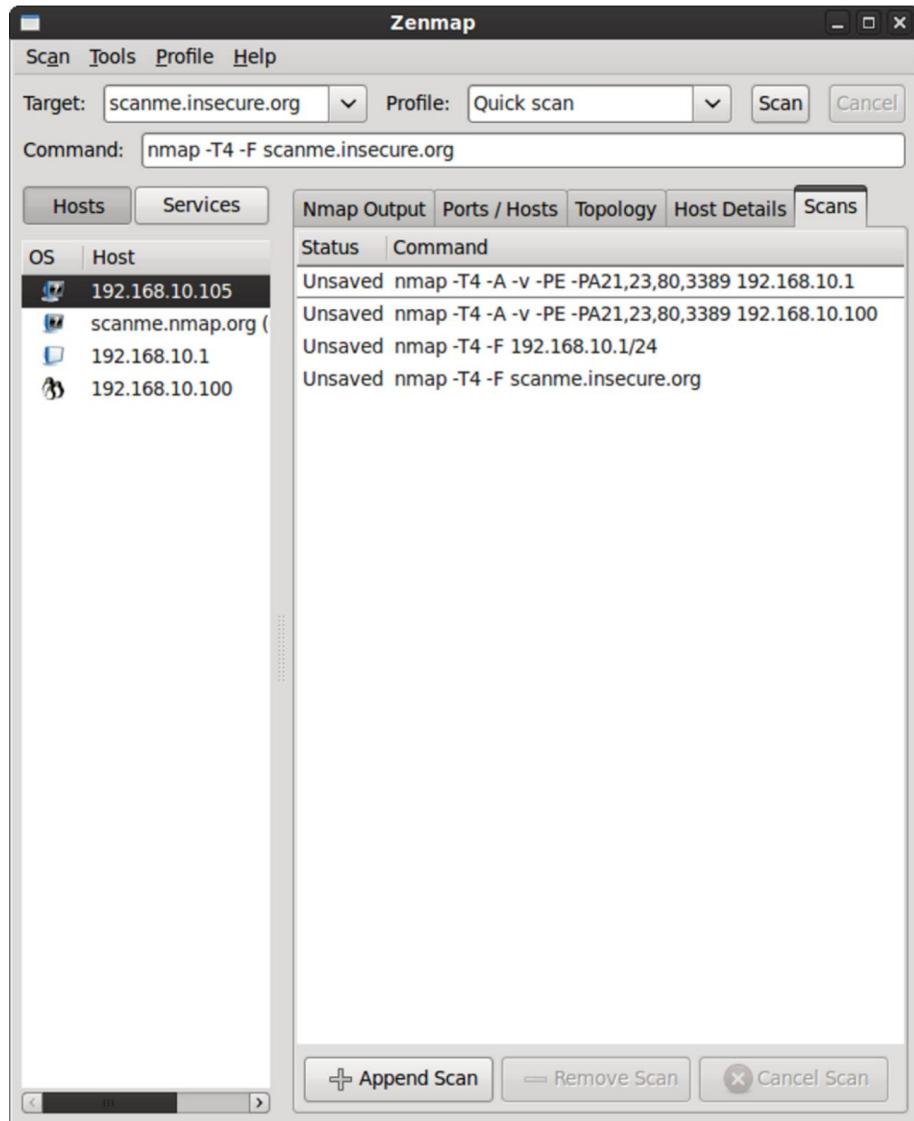
целевой системы.

The screenshot shows the Zenmap interface with the title bar "Zenmap". The menu bar includes "Scan", "Tools", "Profile", and "Help". The toolbar has fields for "Target" (set to "scanme.insecure.org") and "Profile" (set to "Quick scan"), along with "Scan" and "Cancel" buttons. The command line below the toolbar shows "nmap -T4 -F scanme.insecure.org". The main window has tabs: "Hosts" (selected), "Services", "Nmap Output", "Ports / Hosts", "Topology", "Host Details" (selected), and "Scans". The "Host Details" tab displays information for host 192.168.10.100. It includes sections for "Comments", "Host Status" (State: up, Open ports: 5, Filtered ports: 0, Closed ports: 95, Scanned ports: 100, Up time: Not available, Last boot: Not available), "Addresses" (IPv4: 192.168.10.100, IPv6: Not available, MAC: Not available), "Operating System" (Name: Linux 2.6.17 - 2.6.28, Accuracy: 100%), "Ports used", and "OS Class". There are also small icons of penguins and a yellow box next to some status lines.

Подробности о хосте Zenmap

## Просмотр истории сканирования

На вкладке «Сканирования» отображается история сканирования для текущего сеанса.

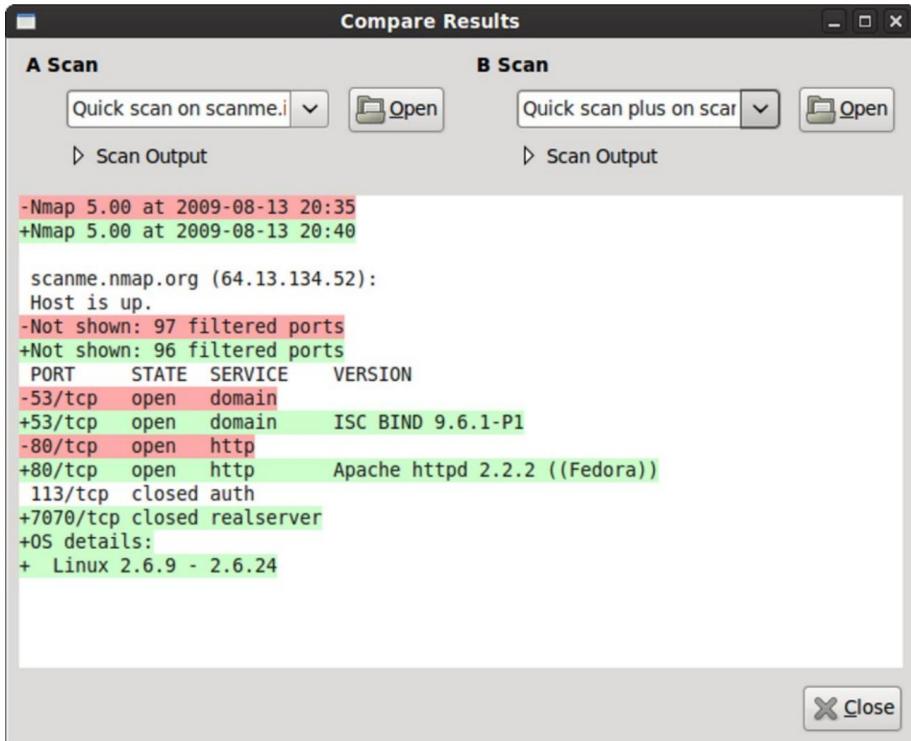


Сравнение результатов сканирования

[Technet24.ru](#)

Сканирования Nmap и Zenmap можно сравнить с помощью функции сравнения результатов.

для этого выберите «Инструменты» &gt; «Сравнить результаты» в меню Zenmap или нажмите CTRL + D.



Утилита сравнения Zenmap

Zenmap загружает последние сканы в утилиту сравнения, или вы можете импортировать

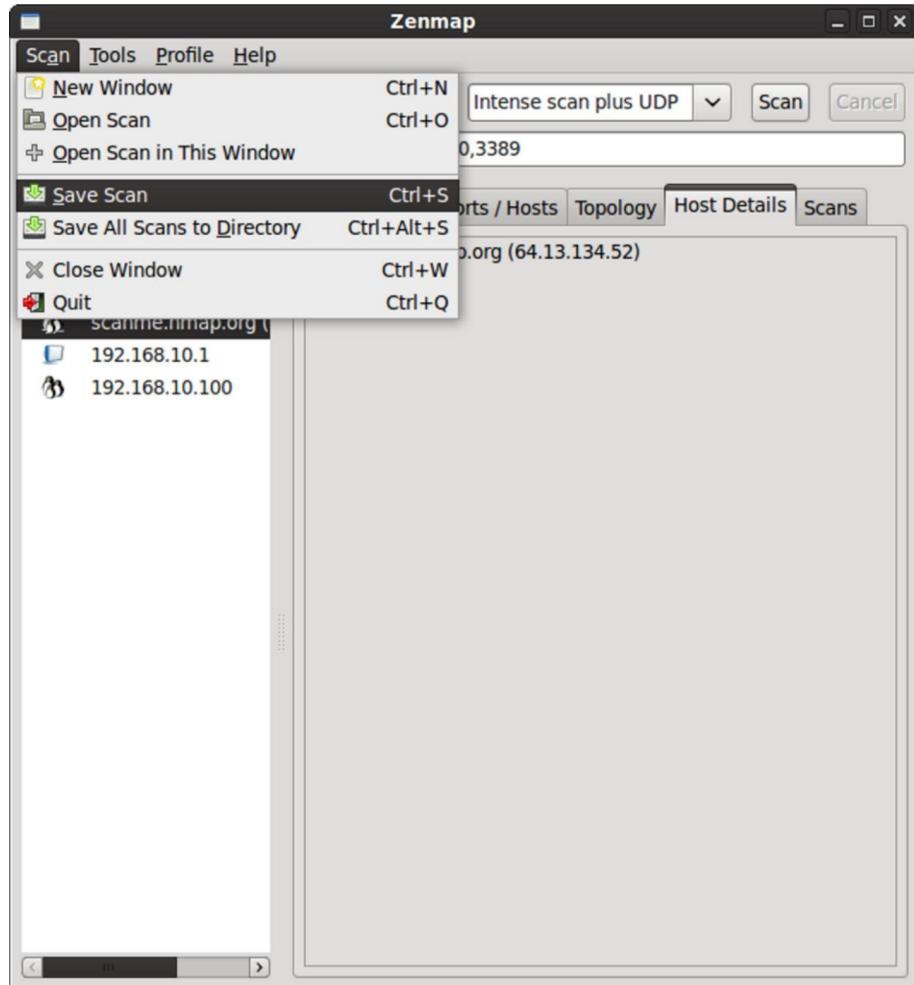
XML-файл Nmap (обсуждается на стр. 130), нажав кнопку «Открыть».

различия между двумя выбранными сканами выделены для удобства сравнения.

Сохранение скриншотов

Сканированные изображения Zenmap можно сохранить для дальнейшего использования, выбрав «Сканировать» > «Сохранить скриншоты».

Меню или нажмите CTRL + S.



Сохранение скриншотов Zenmap

Раздел 12:

Скриптовый движок Nmap (NSE)

## Обзор с криптового движка Nmap

Nmap Scripting Engine (NSE) — мощный инструмент, позволяющий пользователю разрабатывать пользовательские сценарии, которые можно использовать для использования расширенных функций сканирования Nmap. Помимо возможности писать собственные скрипты, имеется еще ряд стандартных встроенных скриптов, которые предлагают некоторые интересные функции, такие как уязвимость обнаружение и эксплуатация. В этом разделе описываются основные возможности использования этих встроенных сценариев.

**Примечание** Скрипты для NSE написаны на языке программирования Lua.

К сожалению, программирование на Lua выходит за рамки этой книги. Для

дополнительной информации Lua посетите [www.lua.org](http://www.lua.org).

**Предупреждение** NSE использует различные методы сканирования, которые (в некоторых редких случаях) могут привести к нежелательным результатам, таким как прослушивание системы и потеря данных. потерять. Кроме того, функция эксплуатации уязвимостей NSE может помочь вам у вас проблемы с законом, если у вас нет разрешения на сканирование цели системы

Краткое описание функций, описанных в этом разделе:

Особенность	Вариант
Выполнение отдельных сценариев	--script [скрипт]
Выполнить несколько сценариев	--script [скрипт1, скрипт2 и т. д.]
Выполнение сценариев по каталогу	--script [каталог]
Выполнение нескольких каталогов сценариев	--script [каталог1, каталог2]
Установление неполадок сценариев	--script-trace
Обновите базу данных скриптов	--script-updatedb

## Выполнение отдельных сценариев

Аргумент `--script` используется для выполнения сценариев NSE.

Синтаксис использования: `nmap --script [script.nse] [цель]`

```
# nmap --script whois.nse scanme.insecure.org
```

Запуск Nmap 5.00 ( <http://nmap.org> ) 13 ноя бря 2009 г., 15:27 CST.

Интересные порты на [scanme.nmap.org](http://scanme.nmap.org) (64.13.134.52):

Не показано: 996 отфильтрованных портов.

ПОРТ	ГОСУДАРСТВЕННАЯ СЛУЖБА
------	------------------------

25/TCP	закрытый smtp
--------	---------------

53/TCP	открытый домен
--------	----------------

70/TCP	закрытый сурслик
--------	------------------

80/TCP	открытый http
--------	---------------

Результаты xост-крипта:

- | whois: Запись найдена на [whois.arin.net](http://whois.arin.net).

- , с сетевой диапазон: 64.13.134.0 - 64.13.134.63

- | сетевое имя : NET-64-13-143-0-26

- | Название организаций: Titan Networks

- | орг ида INSEC

- | страна: штат США Калифорния

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 8,12 секунды.

Выполнение сценария NSE

Результаты скрипта отображаются под заголовком «Результаты xост-крипта». В примере

выше опция `--script` используется для выполнения сценария `whois.nse`. Встроенный

скрипт `whois.nse` извлекает информацию об общедоступном IP-адресе указанного

цели от ARIN (Американский реестр номеров Интернета). Это всего лишь один из

множества встроенных скриптов NSE.

Кончик Полный список встроенных скриптов для Nmap 5.00 можно найти в Интернете по адресу:

Кончик

[www.nmap.org/nsedoc/](http://www.nmap.org/nsedoc/).

## Выполнить не сколько сценариев

Скриптовый движок Nmap поддерживает возможность одновременного запуска нескольких скриптов.

Синтаксис использования : nmap --script [script1,script2 и т. д | "выражение"] [цель]

```
# nmap --script "smtp*" 10.10.1.44
```

Запуск Nmap 5.00 ( http://nmap.org ) 15 ноя бря 2009 г., 14:24 CST.

Интересные порты на 10.10.1.44:

...

```
| smtp-команды: EHLO Exchange-01.dontfearthecommandline.com Здравствуйте
[10.10.1.173], TURN, SIZE, ETRN, КОНВЕЙЕРНАЯ ОБОРУДОВАНИЕ, DSN, РАСПРОШИТЕЛЬНЫЕ СТАТУСЫ КОДЫ,
8bitmime, BINARYMIME, CHUNKING, VRFY, X-EXPS GSSAPI NTLM ВХОД X-
EXPS=ВХОД АУТИЗАЦИЯ GSSAPI NTLM ВХОД AUTH=ВХОД X-LINK2STATE, XEXCH50
| HELP Этот сервер поддерживает следующие команды: HELO EHLO
STARTTLS RCPT ДАННЫЕ RSET MAIL QUIT HELP AUTH TURN ETRN BDAT VRFY
| smtp-open-relay: обнаружено ОТКРЫТОЕ РЕЛЕ.
...
```

Выполнение всех SMTP-скриптов

В этом примере подстановочный знак звездочки используется для выполнения всех сценариев, которые начните с smtp. Вы также можете предоставить список отдельных сценариев, разделенных запятыми, для запустите, используя следующий синтаксис : nmap --script script1,script2,script3 и т. д.

### Примечание

При использовании подстановочных знаков выражение должно быть заключено в кавычки, например «smtp\*» или «ftp\*».

### Кончик

Некоторые скрипты Nmap принимают аргументы с помощью опции --script-args . Этот позволяет указывать определенные параметры для сценария . Полный список аргументов для каждого сценария можно найти на сайте [www.nmap.org/nsedoc/](http://www.nmap.org/nsedoc/).

## Категории скриптов

Вы можете использовать опцию `-script` для выполнения сценариев NSE в зависимости от категории. Стол

ниже описаны доступные категории:

Категория	Цель
все	Запускает все доступные сценарии NSE.
авторизаций	Скрипты, связанные с аутентификацией
получение	Запускает базовый набор сценариев по умолчанию
открытие	Попытки получить подробную информацию о цели
внешний	Скрипты, которые вызываются с внешними источниками (например, с базой данных <code>whois</code> ).
навязчивый	Скрипты, которые целевая система может считать навязчивыми.
вредоносное ПО	Скрипты, проверяющие наличие открытых бэкдоров и вредоносного ПО
безопасный	Базовые скрипты, которые не навязчивы
уязвимость	Проверяет цель на наличие часто используемых уязвимостей

Категории сценариев NSE

Использование категорий скриптов — это самый простой способ запуска встроенных скриптов NSE.

Знать конкретный сценарий, который вы хотите запустить. Однако выполнение сценариев по категориям

выполнение может занять больше времени, поскольку каждая категория содержит множество сценариев.

Кончик	Полный список сценариев NSE в каждой категории можно найти в Интернете по адресу: <a href="http://www.nmap.org/nsedoc/">www.nmap.org/nsedoc/</a> .
--------	---

## Выполнение сценариев по категориям

Опция `--script` можно использовать для выполнения нескольких сценариев в зависимости от их категории.

Синтаксис использования: `nmap --script [категория] [цель]`

```
# nmap --script по умолчанию 10.10.1.70
```

Запуск Nmap 5.00 ( <http://nmap.org> ) 13 маября 2009 г., 15:09 CST.

Интересные порты на 10.10.1.70:

Не показано: 997 отфильтрованных портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

139/tcp открыть netbios-ssn

445/TCP открыть Microsoft-DS

5900/TCP открыть VNC

MAC-адрес: 00:0C:F1:A6:1F:16 (Intel)

Результаты хост-крипта:

|\_ nbstat: Имя NetBIOS: AXIS-01, Пользователь NetBIOS: <неизвестно>, NetBIOS

МАК: 00:0C:F1:A6:1F:16

| smb-os-discovery: Windows XP

| Диспетчер локальной сети: Диспетчер локальной сети Windows 2000.

| Имя : РАБОЧАЯ ГРУППА AXIS-01

| Системное время : 2009-11-13 15:09:12 UTC-6

Nmap выполнено: 1 IP-адрес (1 хост работает) сканируется за 52,40 секунды.

Выполнение всех сценариев в категории по умолчанию

Указав категорию (см. стр. 165) с опцией `--script`, Nmap выполнит

каждый сценарий в этой категории. В приведенном выше примере результаты сценариев в

Категории по умолчанию отображаются под заголовком «Результаты хост-крипта».

Кончик

Опция `-sC` — это сокращение для `--script default`, который будет выполнять все сценарии NSE в категории по умолчанию

## Выполнение нескольких категорий сценариев

Несколько категорий сценариев могут выполняться одновременно, используя один из следующих вариантов:

синтаксические структуры:

nmap --script категория 1, категория 2 и т. д.

Если указать несколько категорий сценариев в виде списка разделенных запятыми, будут выполнены все скрипты в определенных категориях. Например, выполнив nmap --script вредоносное ПО, vuln запустит все сценарии вредоносного ПО и уязвимостей категории.

категории.

nmap --script "категория 1 и категория 2"

Сценарии NSE могут принадлежать более чем к одной категории. Использование этого синтаксиса приведет к выполнению всех, что относятся к обеим указанным категориям. Например, nmap --script «по умолчанию безопасно» будет выполнять только сценарии, принадлежащие как категории по умолчанию безопасные категории.

nmap --script "категория 1 или категория 2"

Оператор или можно использовать для запуска сценариев, принадлежащих любому из указанных категорий. Например, nmap --script «по умолчанию или безопасно» будет выполнить все сценарии, принадлежащие к категории по умолчанию или безопасным.

nmap --script "не категория"

Оператор not используется для исключения скриптов, принадлежащих к указанной категории. Для примера, выполнение nmap --script «не навязчиво» запустит все скрипты, которые не относятся к категории интрузивных.

Устранение неполадок сценариев

Опция `--script-trace` ис пользуется для отслеживания сценариев NSE.

Синтаксис использования : `nmap --script [крипт(ы)] --script-trace [цель]`

```
# nmap --script default --script-trace 10.10.1.70
Запуск Nmap 5.00 (http://nmap.org) в 2009-11-14, 13:51 CST.

NSEOCK (5.1060с) nsock_loop() запущен (время ожидания = 50 мс). 0 событий в ожидании
NSEOCK (5.1060с) UDP-соединение запрошено на 10.10.1.70:137 (IOD #1) EID 8
NSEOCK (5.1070с) TCP-соединение запрошено на 10.10.1.70:5900 (IOD #2) EID 16
NSEOCK (5.1070с) UDP-соединение запрошено на 10.10.1.70:137 (IOD #3) EID 24
NSEOCK (5.1080с) nsock_loop() запущен (тайм-аут = 50 мс). 3 события ожидаются
Обратный вызов NSEOCK (5.1080с): CONNECT SUCCESS для EID 8 [10.10.1.70:137]
NSE: UDP 10.10.1.73:56824 > 10.10.1.70:137 | СОЕДИНИТЬ
Обратный вызов NSEOCK (5.1080с): CONNECT SUCCESS для EID 16 [10.10.1.70:5900]
NSE: TCP 10.10.1.73:49401 > 10.10.1.70:5900 | СОЕДИНИТЬ
Обратный вызов NSEOCK (5.1080с): CONNECT SUCCESS для EID 24 [10.10.1.70:137]
...
...
```

Выход трафика NSE

Опция `--script-trace` отображает все пакеты, отправленные и полученные сценарием NSE, и полезен для устранения проблем, связанных с сценариями.

Некоторые сценарии могут генерировать тысячи строк вывода при использовании трафика сценария.

вариант. В большинстве случаев лучше перенаправить вывод в файл для последующего просмотра.

Пример ниже показывает, как это сделать.

```
# nmap --script default 10.10.1.70 --script-trace > трафик.txt
```

Перенаправление вывода трафика NSE

Результатирующий файл трафик.txt будет содержать все данные трафика, и его можно будет просмотреть в стандартный текстовый редактор.

## Обновите базу данных с скриптов

Опция `--script-updatedb` используется для обновления базы данных скриптов.

Синтаксис использования: `nmap --script-updatedb`

```
# nmap --script-updatedb
```

Запуск Nmap 5.00 (<http://nmap.org>) в 2009-11-14, 13:42 CST.

NSE: Обновление базы данных правил.

База данных сценариев NSE успешно обновлена.

Nmap выполнено: 0 IP-адресов (0 открытых портов) сканируется за 0,38 секунды.

Обновление базы данных сценариев в NSE

Nmap поддерживает базу данных скриптов, которая используется для облегчения возможности выполнение нескольких сценариев по категориям (обсуждается на странице 164). Самый Unix-подобный системы раньше тесно связаны в каталоге `/usr/share/nmap/scripts/`. системы Windows сохранили эти файлы в `C:\Program Files\Nmap\scripts`. Если вы добавляете или удаляете сценарии из каталога сценариев вы должны запустить `nmap --script-updatedb`, чтобы применить изменения в базе данных скриптов.



Раздел 13:

Разница

## Обзор Ndiff

Ndiff — это инструмент в составе пакета Nmap, который позволяет сравнивать два сканирования и помечать любые изменения между ними. Он принимает два разных XML-файла Nmap (обсуждается на стр. 130) и выделяет различия между каждым файлом для удобства сравнения. Ndiff можно использовать в командной строке или в форме графического интерфейса в Zenmap. приложение (см. стр. 159).

Краткое описание функций, описанных в этом разделе:

Особенность	Вариант
Сравнение с использованием Ndiff	-равница
Подробный режим Ndiff	-B
Режим вывода XML	--xml

## Сравнение сканов с ис использованием Ndiff

Утилита ndiff ис используется для сравнения двух сканирований Nmap.

Синтаксис ис использования : ndiff [файл1.xml файл2.xml]

```
# ndiff scan1.xml scan2.xml
-Nmap 5.00 в 2009-12-17 09:18
+Nmap 5.00 в 2009-12-18 12:44

10.10.1.48, 00:0C:29:D5:38:F4:
-Не показано: 994 закрытых порта.
+Не показано: 995 закрытых портов.

ВЕРСИЯ ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПОРТА

-80/tcp открыть http
```

Сравнение двух сканирований Nmap

Основное ис использование утилиты Ndiff заключается в сравнении двух разных XML-файлов Nmap.

(обсуждается на стр. 130). Различия между двумя файлами выделены значком

Знак минус указывает на информацию первом файле, а знак плюс указывает на информацию первом файле.

изменения во втором файле. В приведенном выше примере мы видим, что порт 80 на

второе сканирование изменило состояние с открытое на закрытое.

## Подробный режим Ndiff

Опция `-v` используется для отображения подробного вывода с помощью Ndiff.

Синтаксис использования : `nmap -v [файл1.xml файл2.xml]`

```
# nmap -v scan1.xml scan2.xml
-Nmap 5.00 в 2009-12-17 09:18
+Nmap 5.00 в 2009-12-18 12:44

10.10.1.48, 00:0C:29:D5:38:F4:
Хост вставлен.
-Не показано: 994 закрытых порта.
+Не показано: 995 закрытых портов.

ПОРТ      ГОСУДАРСТВЕННАЯ ВЕРСИЯ
21/TCP открытый FTP
22/TCP открыть SSH
25/TCP открыть SMTP
-80/tcp открыть http
111/tcp открыть rpcbind
2049/tcp открыть nfs
```

Выход сканирования Ndiff в подробном режиме

Подробный вывод отображает все строки обоих XML-файлов и выделяет различия .  
с знаком минус , обозначающим информацию первом файле , и знаком плюс .  
указывая изменения во втором файле . Это отличие от стандартного Ndiff.  
поведение (описанное на стр. 173) , которое отображает только различия между  
два файла . Подробный вывод часто более полезен , чем вывод по умолчанию поскольку он отображает  
все информацию из оригинального сканирования .

## Режим вывода XML

Опция `-xml` используется для генерации вывода XML с помощью Ndiff.

Синтаксис использования : `ndiff --xml [файл1.xml] [файл2.xml]`

```
# ndiff --xml scan1.xml scan2.xml
<?xml версия ="1.0" кодировка="UTF-8"?>
<nmapdiff версия ="1">
<скандинифф>
<x ос тдифф>
<x ос т>
<адрес адрес ="10.10.1.48" addrtype="ipv4"/>
<адрес адрес ="00:0C:29:D5:38:F4" addrtype="mac"/>
<порты>
<a>
<extraports count="994" state="closed"/>
</a>
<b>
<extraports count="995" state="closed"/>
</b>
<портдинифф>
<a>
<port portid="80" протокол="tcp">
<state state="open"/>
<имя службы="http"/>
...
...
```

XML-вывод Ndiff

Вывод XML — отличный инструмент для передачи информации из Ndiff в третью сторону.

Программа, использующая широкоподдерживаемый формат.

Кончик

Выход по умолчанию `-xml` отображает XML-код на экране. Чтобы сократить это информационный файл, введите `ndiff --xml scan1.xml scan2.xml >ndiff.xml`, который перенаправит выходные данные в файл с именем `ndiff.xml`.



Раздел 14:

Секреты и уловки

## Обзор с оветов и рекомендац ий

В этом разделе представлено не сколько полезных с оветов и рекомендац ий, которые помогут получить макс имальную отдачу от Nmap. Он также включает ис пользование сторонних прог рамм, к оторые работают с овместно с Nmap, чтобы помочь вам проанализировать вашу сеть.

Краткое изложение тем, обс уждаемых в этом разделе:

Тема	Страница
Объедините не сколько вариантов	179
Сканирование в интерактивном режиме	180
Взаимодействие во время выполнения	181
Удаленное сканирование вашей сети	182
Вайршарк	183
Scanme.Insecure.org Онлайн-ресурсы Nmap	184
	185

## Объедините несолько вариантов

Если вы еще не заметили, Nmap позволяет комбинировать несолько опций для создания индивидуального сканирования, уникальное для ваших нужд.

Синтаксис использования : nmap [опции] [цель]

```
# nmap -reason -F --open -T3 -O scanme.insecure.org
```

Запуск Nmap 5.00 (<http://nmap.org>) 17 декабря 2009 г., 16:01 CST.

Интересные порты на [scanme.nmap.org](http://scanme.nmap.org) (64.13.134.52):

Не показано: 95 фильтруемых портов, 3 закрытых порта.

Причина: 95 откасов и 3 сбросов

ГОСУДАРСТВЕННАЯ ПОРТОВАЯ СЛУЖБА ПРИЧИНА

Синхронизация открытого домена 53/tcp

80/tcp открыть http зрелице-о

Тип устройств общего назначения |WAP|брандмауэр|маршрутизатор

Работает (ПРОСТОУГАДАЮ: Linux 2.6.X|2.4.X (95%), Linksys Linux 2.4.X

...

Объединение несолько опций Nmap

В приведенном выше примере множество различных вариантов комбинируются для получения желаемого результата.

Результаты. Как видите, возможности практически безграничны. Вы должны заметить,

однако не все варианты совместимы друг с другом, как показано в

следующий пример.

```
# nmap -PN -sP 10.10.1.*
```

-PN (пропустить пинг) несовместим с -sP (сканирование ping). Если ты только х отите перечислить хосты, попробуйте сканирование списка (-sL)

Предупреждение Nmap при объединении несовместимых опций

В этом примере очевидно, что опция -PN (не пинговать) и опция -sP (только пинг).

не совместимы друг с другом. К счастью Nmap предоставляет дружественный и

информационное сообщение об ошибке и, таким образом, никакого вреда не будет.

## Сканирование в интерактивном режиме

Опция `--interactive` включает интерактивную оболочку Nmap.

Синтаксис использования : nmap --interactive

```
$ nmap --interactive
```

Запуск Nmap версии 5.00 (<http://nmap.org>)

Добро пожаловать в интерактивный режим! Нажмите `h <enter>` для получения помощи.

Nmap>

Оболочка интерактивного режима Nmap

В интерактивном режиме вы можете запустить сканирование, просто набрав букву `n`

затем нажмите `c` для ввода адреса и любые стандартные параметры Nmap. Пример ниже

демонстрирует использование интерактивного режима для выполнения простого сканирования `-F`.

Синтаксис использования : n [опции] [цель]

```
nmap> n -F 10.10.1.1
```

Интересные порты на 10.10.1.1:

Не показано 98 закрытых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

80/tcp открыть http

443/TCP открыть https

Nmap выполнено: 1 IP-адрес (1 x сканируется) за 0,19 секунды.

Пример сканирования с использованием Nmap в интерактивном режиме

Когда вы закончите сканирование, просто введите `x`, чтобы выйти из интерактивной оболочки.

Кончик

Нажатие клавиши `h` в интерактивном режиме отображает меню правки, которое описывает доступные варианты.

Взаимодействие во время выполнения

[Technet24.ir](#)

Nmap предлагает несолько нажатий клавиш во время выполнения, которые могут изменить текущий процесс.

Сканирование. В таблице ниже перечислены клавиши взаимодействия Nmap во время выполнения.

Ключ	Функция
в	Нажатие строчной буквы v во время сканирования повысит уровень детализации.
В	Нажатие заглавной буквы V во время сканирования повысит уровень детализации.
д	Нажатие строчной буквы d во время сканирования увеличит время отладки.
Д	Нажатие заглавной буквы D во время сканирования повысит уровень отладки.
п	Нажатие строчной буквы p во время сканирования активирует отслеживание пакетов.
П	Нажатие заглавной буквы P во время сканирования отключит отслеживание пакетов.
?	Нажимаем ? во время сканирования будет отображаться справка о взаимодействии во время выполнения.
Любой другой клавиша, нет в списке выше	Нажатие во время сканирования клавиши, отличной от указанных выше, приведет к печати сообщения о состоянии, указывающим о ходе сканирования и оставшееся время.

Ключи взаимодействия во время выполнения Nmap

Взаимодействие во время выполнения очень полезно для получения обновлений статуса при выполнении сканирования.

Большое количество состояний. В приведенном ниже примере показано состояние текущего сканирования.

При нажатии пробела.

```
# nmap -T2 10.10.1.*  
[Космос]  
Статистика: Прошло 0:06:45; Завершено 18 хостов (30 больше), 30 проходов SYN  
Скрытое сканирование  
Время скрытого сканирования SYN: выполнено около 38,44%; Ит. д.: 16:56 (0:10:26  
оставшийся)  
...
```

Использование клавиш взаимодействия во время выполнения для отображения статуса сканирования

Помимо возможности отображать обновления статуса, клавиши взаимодействия во время выполнения также могут настроить параметры подробностей, трафик и отладки, не прерывая сканирование в процессе.

## Удаленное сканирование вашей сети

Nmap Online — это веб-сайт, предоставляющий (бесплатные) функции сканирования Nmap через Интернет. Браузер. Это может быть полезно для удаленного сканирования вашей сети или устранения неполадок. проблемы с подключением от внешнего источника. Просмотрите [www.nmap-online.com](http://www.nmap-online.com). и введите свой IP-адрес или адрес целевой системы, которую вы хотите сканировать.

The screenshot shows the Nmap Online interface in Mozilla Firefox. At the top, there's a banner for "Nmap Free Security Scanner" with the tagline "Network-wide ping sweep, portscan, OS Detection Audit your network security before the bad guys do". A placeholder "Your IP: [REDACTED]" is shown. The main area has two main sections:

- New Scan:** A form where users can choose a scan type. The "Quick Scan" option is selected, with the command "-r -T5 -sS [REDACTED]". Other options include "Full Nmap Scan" (-r 1 -F -T4 -sS [REDACTED]) and "Custom scan". It also includes a text input for "Nmap options" with "-F -T5 -sS [REDACTED]", a checkbox for "I agree with Terms of Service", and a "Scan Now!" button.
- My Scan Results:** A section for viewing previous scan results. It includes fields for "Email" and "Password", a "Remember on this computer" checkbox, and a "View My Scan Results" button. To the right is a "Donate" section with logos for "monerobooters.com" and "PayPal".

At the bottom, there's a note about contacting support and a footer stating "Nmap Online • a project of Different Internet Experience Ltd. • administered by [www.matousec.com](http://www.matousec.com) • Terms of Service".

Done

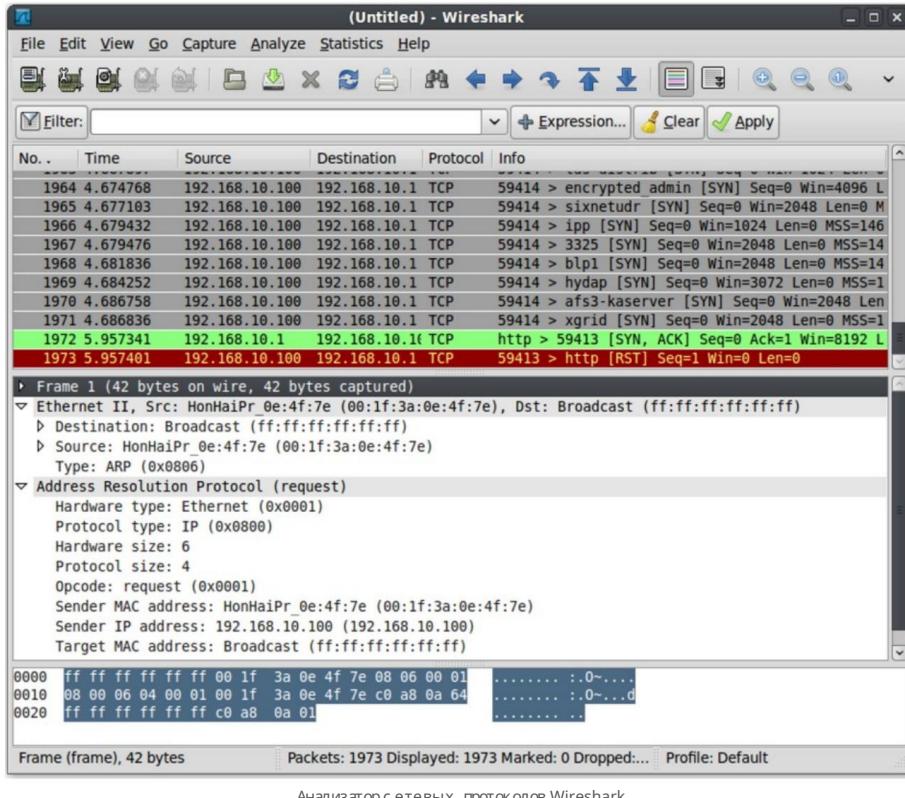
Домашняя страница Nmap онлайн

Чтобы предотвратить злоупотребления, Nmap Online разрешает максимум 5 запросов на сканирование с одного IP-адреса каждые 24 часа и максимум 20 сканирований каждые 7 дней. Прежде чем вы сможете выполнить сканирование.

**Примечание:**

## Вайршарк

Wireshark — отличное дополнение к набору инструментов любого системного администратора. Это сложный (но простой в использовании) анализатор сетевых протоколов. Вы можете использовать Wireshark для захватывать и анализировать сетевой трафик и работать вместе с Nmap, позволяя смотреть каждый отправленный и полученный пакет во время сканирования.



Wireshark доступен для Windows, Linux и Mac OS X и его можно загрузить.

бесплатно на сайте [www.wireshark.org](http://www.wireshark.org).

## Scanme.Insecure.org

Сервер scanme.insecure.org является распространенным примером цели, ис пользуемой в этом документе. Гид. Эта система размещена в проекте Nmap и может свободно сканироваться пользователем Nmap.

```
# nmap -F scanme.insecure.org
```

Запуск Nmap 5.00 ( http://nmap.org ) 18 декабря 2009 г., 16:52 CST.

Интересные порты на scanme.nmap.org (64.13.134.52):

Не показано: 95 фильтруемых портов.

ПОРТ ГОСУДАРСТВЕННАЯ СЛУЖБА

25/TCP закрыт SMTP

53/TCP открытый домен

80/tcp открыть http

110/tcp закрыт, порт

113/tcp закрытая авторизация

Nmap выполнено: 1 IP-адрес (1 x остается) сканируется за 2,63 секунды.

Пример сканирования с использованием scanme.insecure.org в качестве цели

### Примечание

Добрые люди из проекта Nmap предоставляют эту ценную слугу в качестве инструмента для обучения и устранения неполадок и просим вас быть вежливыми и не агрессивно сканируя его один раз в день или с помощью других инструментов, не связанных с Nmap.

## Онлайн-ресурсы Nmap

Книга Федора Nmap

[www.nmap.org/book/man.html](http://www.nmap.org/book/man.html)

Руководство по

установке Nmap [www.nmap.org/book/install.html](http://www.nmap.org/book/install.html)

Документация по криптовому движку Nmap

[www.nmap.org/nsedoc/](http://www.nmap.org/nsedoc/)

Справочное руководство

Zenmap [www.nmap.org/book/zenmap.html](http://www.nmap.org/book/zenmap.html)

Журнал изменений

Nmap [www.nmap.org/changelog.html](http://www.nmap.org/changelog.html)

Списки рассылок

Nmap [www.seclists.org](http://www.seclists.org)

Онлайн-сканирование

Nmap [www.nmap-online.com](http://www.nmap-online.com)

Инструменты

безопасности [www.sectools.org](http://www.sectools.org)

Списки рассылок

Nmap [www.seclists.org](http://www.seclists.org)

Nmap Facebook

[www.nmap.org/fb](http://www.nmap.org/fb)

Nmap Twitter

[www.twitter.com/nmap](http://www.twitter.com/nmap)

Поваренная книга

Nmap [www.nmapcookbook.com](http://www.nmapcookbook.com)



## Приложение А – Шпарг алка по Nmap

Загрузите и распечатайте эту шпарг алку на сайте [www.NmapCookbook.com](http://www.NmapCookbook.com).

Основные методы сканирования	
Сканировать одну цель	nmap [цель]
Сканировать несколько целей	nmap [цель1, цель2 и т. д.]
Сканирование списка целей	nmap -iL [список.txt]
Сканировать диапазон хостов	nmap [диапазон IP-адресов]
Сканировать все порты есть	nmap [ip-адрес /dir]
Сканировать случайные хосты	nmap -iR [число]
Исключение целей из сканирования	nmap [цель] --exclude [цель]
Исключение целей с помощью списка	nmap [цель] --excludefile [list.txt]
Выполните адресацию с канирование	nmap -A [цель]
Сканировать цель IPv6	nmap -6 [цель]
Параметры обнаружения	
Выполните сканирование только с помощью ping	nmap -sP [цель]
Не пинговать	nmap -PN [цель]
TCP SYN-пинг	nmap -PS [цель]
TCP ACK-пинг	nmap -PA [цель]
UDP-пинг	nmap -PU [цель]
SCTP-инициализирующий пинг	nmap -PY [цель]
ICMP-эхопинг	nmap -PE [цель]
Проверка метки времени ICMP	nmap -PP [цель]
Пинг маски адреса ICMP	nmap -PM [цель]
Пинг IP-протокола	nmap -PO [цель]
ARP-пинг	nmap -PR [цель]
Трассировка	nmap --traceroute [цель]
Принудительное обратное разрешение DNS	nmap -R [цель]
Отключить обратное разрешение DNS	nmap -n [цель]
Альтернативный поиск к DNS	nmap --system-dns [цель]
Укажите DNS-серверы вручную	nmap --dns-servers [серверы] [цель]
Создать список хостов	nmap -sL [цель]
Расширенные функции сканирования	
TCP SYN-сканирование	nmap -sS [цель]
Сканирование TCP-соединения	nmap -sT [цель]
UDP-сканирование	nmap -sU [цель]
TCP NULL-сканирование	nmap -sN [цель]
TCP FIN-сканирование	nmap -sF [цель]
Родительское сканирование	nmap -sX [цель]
TCP ACK-сканирование	nmap -sA [цель]
Пользоваться TCP-сканирование	nmap --scanflags [флаги] [цель]
Сканирование IP-протокола	nmap -sO [цель]
Отправка необработанных пакетов Ethernet	nmap --send-eth [цель]
Отправлять IP-пакеты	nmap --send-ip [цель]

Опции сканирования портов	
Выполните быстрое сканирование	nmap -F [цель]
Сканировать определенные порты	nmap -p [порт(ы)] [цель]
Сканировать порты по имени	nmap -p [имя порта] [цель]
Сканировать порты по протоколу	nmap -sU -sT -p U:[порты],T:[порты] [цель]
Сканировать все порты	nmap -p "*" [цель]
Сканировать все новые порты	nmap --top-ports [число] [цель]
Выполните последовательное сканирование портов	nmap -r [цель]
Определение версии	
Обнаружение операционной системы	nmap -O [цель]
Отправка отпечатков TCP/IP	www.nmap.org/submit/
Попытка угадать неизвестное	nmap -O --osscan-guess [цель]
Определение версии служб	nmap -sV [цель]
Установление неподдерживаемых версий	nmap -sV --version-trace [цель]
Выполните сканирование RPC	nmap -sR [цель]
Параметры времени	
Шаблоны времени	nmap -T[0-5] [цель]
Установите TTL пакета	nmap --ttl [время] [цель]
Минимальное количество параллельных операций	nmap --min-parallelism [число] [цель]
Максимальное количество параллельных операций	nmap --max-parallelism [число] [цель]
Минимальный размер группы источников	nmap --min-hostgroup [число] [цель]
Максимальный размер группы источников	nmap --max-hostgroup [число] [цель]
Максимальное время ожидания RTT	nmap --initial-rtt-timeout [время] [цель]
Начальный таймаут RTT	nmap --max-rtt-timeout [TTL] [цель]
Максимальное количество повторов	nmap --max-retries [число] [цель]
Таймаут хоста	nmap --host-timeout [время] [цель]
Минимальная задержка сканирования	nmap --scan-delay [время] [цель]
Максимальная задержка сканирования	nmap --max-scan-delay [время] [цель]
Минимальная скорость передачи пакетов	nmap --min-rate [число] [цель]
Максимальная скорость передачи пакетов	nmap --max-rate [число] [цель]
Победить сброс ограничений скорости	nmap --defeat-rst-ratelimit [цель]
Методы обхода брандмауэра	
Фрагментированные пакеты	nmap -f [цель]
Укажите конкретный MTU	nmap --person [ЧЕЛОВЕК] [цель]
Используйте прямиком	nmap -D RND:[число] [цель]
Сканирование зон в режиме ожидания	nmap -S [зомби] [цель]
Вручнуюкажите исходный порт	nmap --source-port [порт] [цель]
Добавить случайные данные	nmap --data-length [размер] [цель]
Случайный порт для сканирования цели	nmap --randomize-hosts [цель]
Подделать MAC-адрес	nmap --spoof-mac [MAC-адрес] [цель]
Отправить неверные контрольные суммы	nmap --badsum [цель]

Опции вывода	
Сохранить вывод в текстовый файл	nmap -oN [scan.txt] [цель]
Сохранить вывод в файл XML	nmap -oX [scan.xml] [цель]
Графический вывод	nmap -oG [scan.txt] [цель]
Выход всех поддерживаемых типов файлов	nmap -OA [путь/имя файла] [цель]
Периодически отображать статистику	nmap --stats-every [время] [цель]
133т Выход	nmap -oS [scan.txt] [цель]
Устранение неполадок и отладка	
Получать помощь	nmap -ч
Показать версию nmap	nmap -V
Подробный вывод	nmap -v [цель]
Отладка	nmap -d [цель]
Ображение причины состояния порта	nmap --причина [цель]
Ображать только открытые порты	nmap --open [цель]
Трассировка пакетов	nmap --packet-trace [цель]
Ображение сетей хост	nmap -iflist
Укажите сетевой интерфейс	nmap -e [интерфейс] [цель]
Скриптовый движок Nmap	
Выполнение отдельных сценариев	nmap --script [script.nse] [цель]
Выполнить несколько сценариев	nmap --script [выражение] [цель]
Категории скриптов	все, аутентификация, по умолчанию обнаружение, внешний, интрузивный, вредоносный, безопасный, уязвимость
Выполнение сценариев в категории	nmap --script [категория] [цель]
Выполнение нескольких категорий сценариев	nmap --script [category1,category2 и т. д.]
Устранение неполадок с сценариями	nmap --script [скрипт] --script-trace [цель]
Обновите базу данных скриптов	nmap --script-updatedb
Разница	
Сравнение с использованием Ndiff	ndiff [scan1.xml] [scan2.xml]
Подробный режим Ndiff	ndiff -v [канал1.xml] [канал2.xml]
Режим вывода XML	ndiff --xml [scan1.xml] [scan2.xml]



## Приложение В – Состояния портов Nmap

открыть

Открытый порт — это порт, который активно отвечает на входящее соединение.

закрыто

Закрытый порт — это порт на целевом объекте, который активно реагирует на зондирование, но не

на порту работает какая-либо служба. Закрытые порты обычно встречаются в системах,

где нет брандмауэра для фильтрации входящих соединений.

фильтрованный

Фильтруемые порты — это порты, которые обычно защищены каким-либо брандмауэром, который

не позволяет Nmap определить, открыт или закрыт порт.

нефильтрованный

Нефильтрованный порт — это порт, к которому Nmap имеет доступ, но не может его определить.

независимо от того, открыт он или закрыт.

открытый | фильтруемый

Открытый | фильтруемый порт — это порт, который Nmap считает открытым или фильтруемым, но

не может определить, в каком именно состоянии на самом деле находится порт.

закрыто | отфильтровано

Закрытый | фильтруемый порт — это порт, который Nmap считает закрытым или фильтруемым, но

не может определить, в каком состоянии на самом деле находится порт.



## Приложение С. Переярестная с ылка CIDR

[Technet24.ir](#)

Маска подсети	ЦИДР
000.000.000.000	/0
128.000.000.000	/1
192.000.000.000	/2
224.000.000.000	/3
240.000.000.000	/4
248.000.000.000	/5
252.000.000.000	/6
254.000.000.000	/7
255.000.000.000	/8
255.128.000.000	/9
255.192.000.000	/10
255.224.000.000	/11
255.240.000.000	/12
255.248.000.000	/13
255.252.000.000	/14
255.254.000.000	/15
255.255.000.000	/16
255.255.128.000	/17
255.255.192.000	/18
255.255.224.000	/19
255.255.240.000	/20
255.255.248.000	/21
255.255.252.000	/22
255.255.254.000	/23
255.255.255.000	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32



## Приложение D. Общие порты TCP/IP

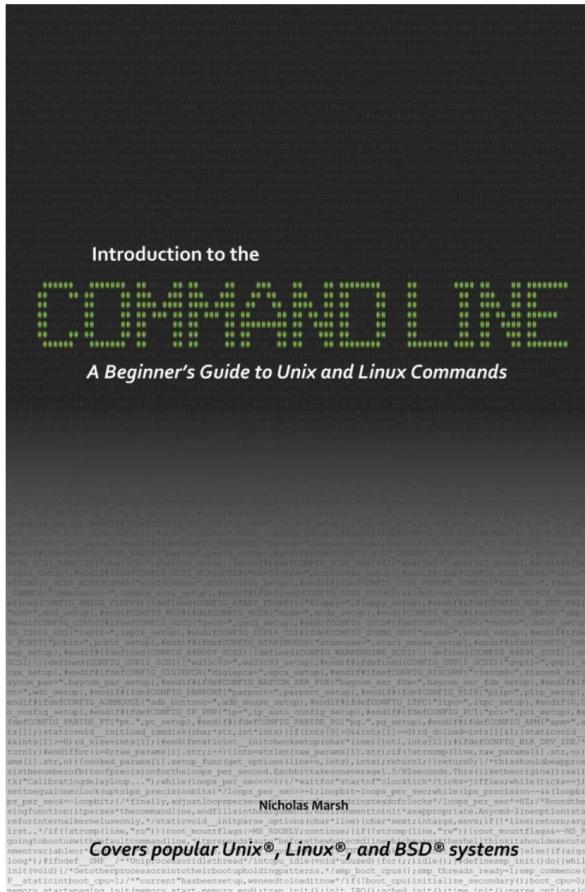
[Technet24.ir](#)

Порт	Тип	Применение
20	TCP	FTP-данные
21	TCP	FTP-управление
22	TCP   UDP Secure Shell (SSH)	
23	TCP	Телнет
25	TCP	Почтовый протокол передачи почты (SMTP)
42	TCP   UDP Служба имен Интернета Windows (WINS)	
53	TCP   UDP Система доменных имен (DNS)	
67	UDP	DHCP-сервер
68	UDP	DHCP-клиент
69	UDP	Тривиальный протокол передачи файлов (TFTP)
80	TCP   UDP Протокол передачи гипертекста (HTTP)	
110	TCP	Протокол почтового отделения 3 (POP3)
119	TCP	Протокол передачи сетевых новостей (NNTP)
123	UDP	Протокол сетевого времени (NTP)
135	TCP   UDP Microsoft RPC	
137	TCP   UDP Служба имен NetBIOS	
138	TCP   UDP Службадатагчылар TCP   UDP NetBIOS	
139	TCP   UDP Службасеансов TCP   UDP NetBIOS	
143	TCP   UDP Протокол доставки сообщений в Интернете (IMAP)	
161	TCP   UDP Протокол сетевого управления (SNMP)	
162	TCP   UDP Ловушка протокола сетевого управления (SNMP)	
389	TCP   UDP Облегченный протокол доставки каталогов (LDAP)	
443	TCP   UDP Протокол передачи гипертекста через TLS/SSL (HTTPS)	
445	TCP	Блок с сообщениями сервера (SMB)
636	TCP   UDP Облегченный протокол доставки каталогов через TLS/SSL (LDAPS)	
873	TCP	Протокол удаленной синхронизации файлов (rsync)
993	TCP	Протокол доставки интернет-сообщений через SSL (IMAPS)
995	TCP	Протокол почтового отделения 3 через TLS/SSL (POP3S)
1433	TCP	Базы данных Microsoft SQL-сервера
3306	TCP	Базы данных MySQL
3389	TCP	Сервер терминалов Microsoft/протокол удаленного рабочего стола (RDP)
5800	TCP	Веб-интерфейс виртуальных сетевых вычислений (VNC)
5900	TCP	Удаленный рабочий стол виртуальных сетевых вычислений (VNC)*



# Готовы изучить командную строку?

Ознакомьтесь с нашей последней игрой...



«Введение в командную строку» — это практическое руководство, которое учит наиболее

важные команды оболочки Unix и Linux простым понятием с пособием.

Все расматриваемые программы командной строки представлены с наглядными примерами, помогающими освоить их.

Процесс обучения поможет вам быстро и легко освоить командную строку.

[www.DontFearTheCommandLine.com](http://www.DontFearTheCommandLine.com)

