**Как посмотреть открытые порты в Linux**

**Обновлено:** 01 мая 2020 **Опубликовано:** 2 августа, 2015 от [admin](https://losst.pro/author/admin) , 4 комменариев, время чтения: 6 минут

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

Сетевые порты - это механизм, с помощью которого операционная система определяет какой именно программе необходимо передать сетевой пакет. Здесь можно привести пример с домом. Например, почтальону необходимо доставить посылку. Он доставляет посылку к дому, это IP адрес компьютера. А дальше в самом доме уже должны разобраться в какую квартиру направить эту посылку. Номер квартиры - это уже порт.

Если порт открыт это означает, что какая либо программа, обычно сервис, использует его для связи с другой программой через интернет или в локальной системе. Чтобы посмотреть какие порты открыты в вашей системе Linux можно использовать множество различных утилит. В этой статье мы рассмотрим самые популярные способы посмотреть открытые порты Linux.

Содержание статьи

* [Как посмотреть открытые порты linux](https://losst.pro/kak-posmotret-otkrytye-porty-v-linux#kak-posmotret-otkrytye-porty-linux)
  + [1. netstat](https://losst.pro/kak-posmotret-otkrytye-porty-v-linux#toc-1-netstat)
  + [2. ss](https://losst.pro/kak-posmotret-otkrytye-porty-v-linux#toc-2-ss)
* [3. lsof](https://losst.pro/kak-posmotret-otkrytye-porty-v-linux#toc-3-lsof)
  + [4. Nmap](https://losst.pro/kak-posmotret-otkrytye-porty-v-linux#toc-4-nmap)
  + [5. Zenmap](https://losst.pro/kak-posmotret-otkrytye-porty-v-linux#toc-5-zenmap)
* [Выводы](https://losst.pro/kak-posmotret-otkrytye-porty-v-linux#vyvody)

**Как посмотреть открытые порты linux**

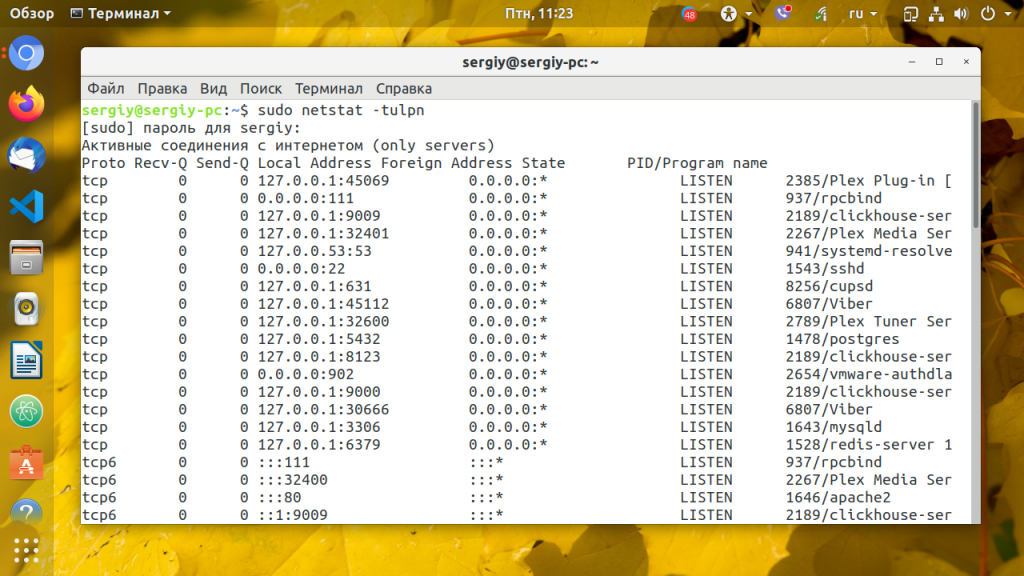
**1. netstat**

Утилита netstat позволяет увидеть открытые в системе порты, а также открытые на данный момент сетевые соединения. Для отображения максимально подробной информации надо использовать опции:

* **-l** или**--listening** - посмотреть только прослушиваемые порты;
* **-p** или **--program** - показать имя программы и ее PID;
* **-t** или **--tcp -**показать tcp порты;
* **-u** или **--udp** показать udp порты;
* **-n** или **--numeric** показывать ip адреса в числовом виде.

Открытые порты Linux, которые ожидают соединений имеют тип LISTEN, а перед портом отображается IP адрес на котором сервис ожидает подключений. Это может быть определенный IP адрес или \*/0.0.0.0 что означают любой доступный адрес:

 sudo netstat -tulpn

[](https://losst.pro/wp-content/uploads/2015/08/Snimok-ekrana-ot-2020-05-01-11-23-48.png)

**2. ss**

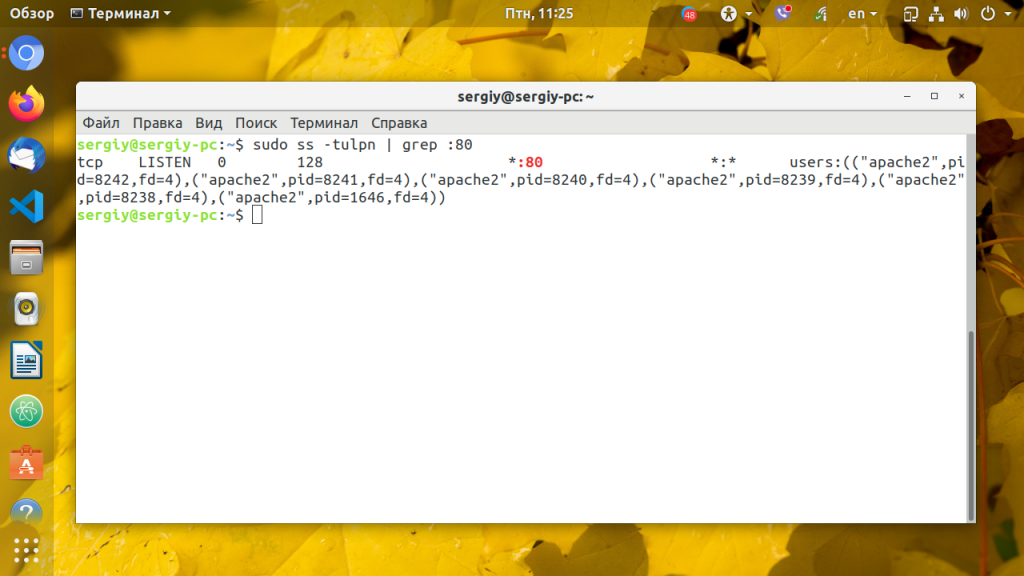
Утилита ss - это современная альтернатива для команды netstat. В отличие от netstat, которая берет информацию из каталога /proc, утилита ss напрямую связывается со специальной подсистемой ядра Linux, поэтому работает быстрее и её данные более точные, если вы хотите выполнить просмотр открытых портов это не имеет большого значения. Опции у неё такие же:

sudo ss -tulpn

[](https://losst.pro/wp-content/uploads/2015/08/Snimok-ekrana-ot-2020-05-01-11-24-32.png)

Можно вывести только процессы, работающие на 80-том порту:

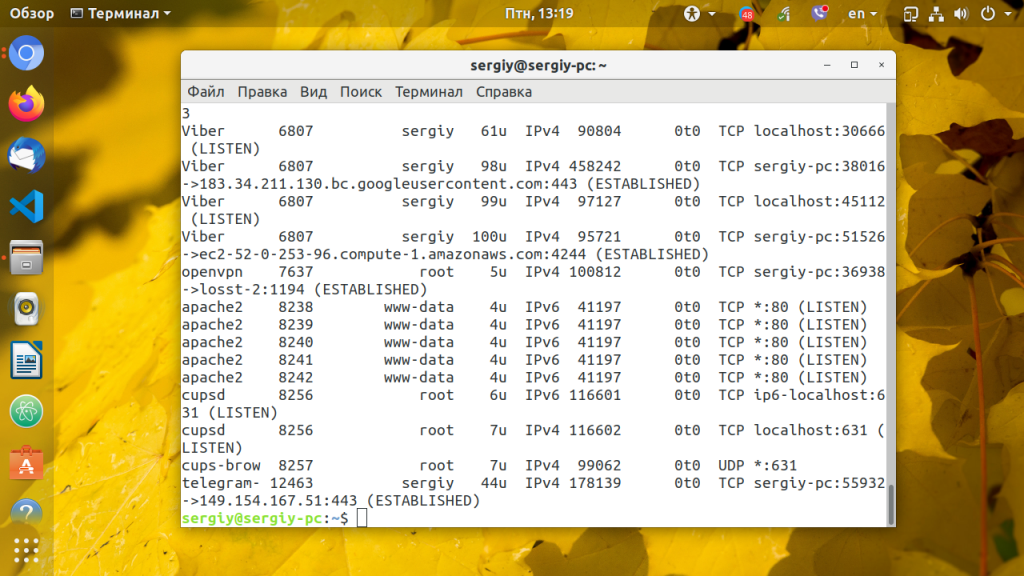
sudo ss -tulpn | grep :80

[](https://losst.pro/wp-content/uploads/2015/08/Snimok-ekrana-ot-2020-05-01-11-25-29.png)

**3. lsof**

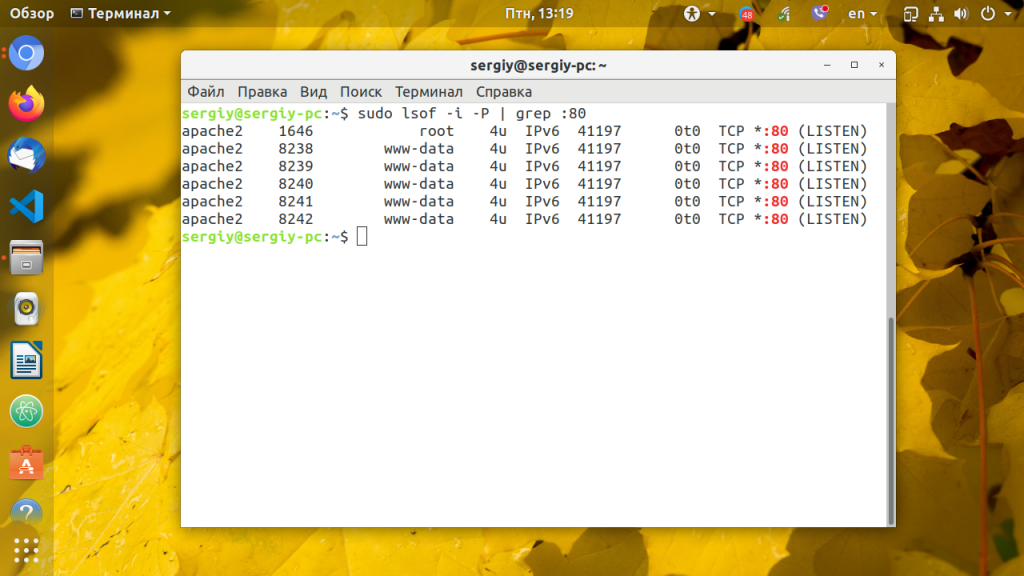
Утилита lsof позволяет посмотреть все открытые в системе соединения, в том числе и сетевые, для этого нужно использовать опцию -i, а чтобы отображались именно порты, а не названия сетевых служб следует использовать опцию -P:

 sudo lsof -i -P

[](https://losst.pro/wp-content/uploads/2015/08/Snimok-ekrana-ot-2020-05-01-13-19-00.png)

Ещё один пример, смотрим какие процессы работают с портом 80:

 sudo lsof -i -P | grep :80

[](https://losst.pro/wp-content/uploads/2015/08/Snimok-ekrana-ot-2020-05-01-13-19-15.png)

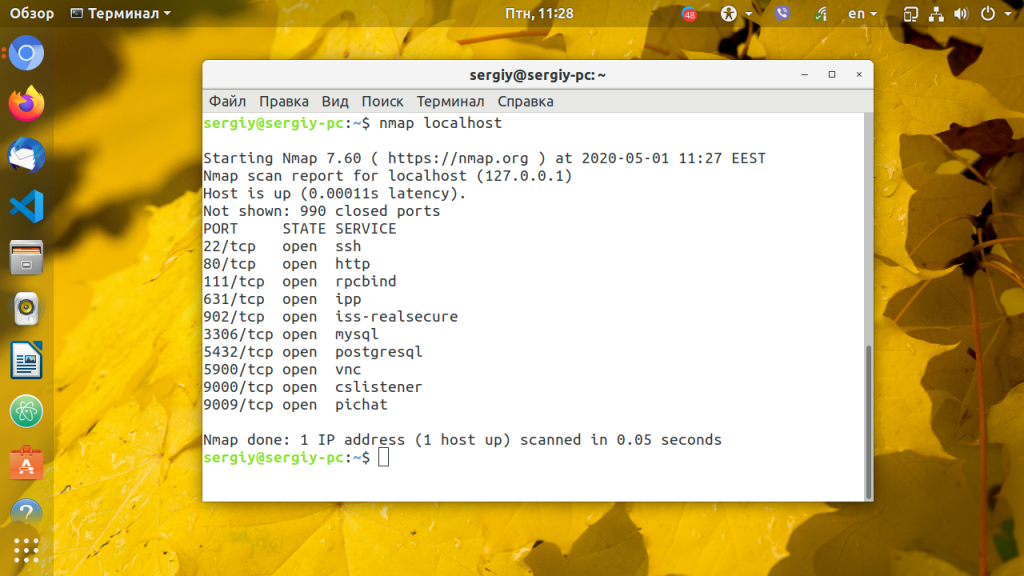
**4. Nmap**

Программа Nmap - мощный сетевой сканер, разработанный для сканирования и тестирования на проникновение удаленных узлов, но ничего не мешает направить его на локальный компьютер. Утилита позволяет не только посмотреть открытые порты, но и примерно определить какие сервисы их слушают и какие уязвимости у них есть. Программу надо установить:

sudo apt install nmap

Затем можно использовать:

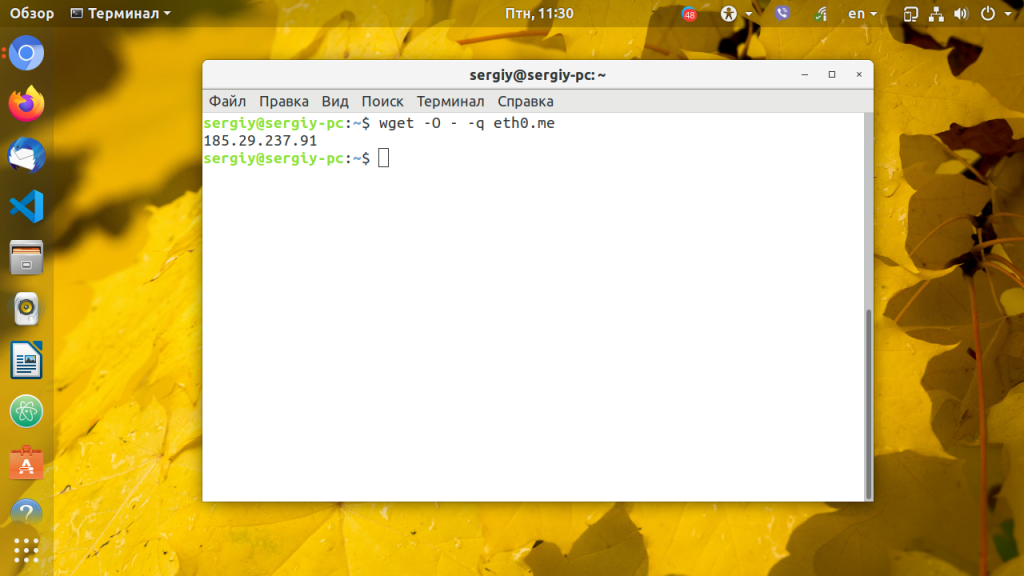
 nmap localhost

[](https://losst.pro/wp-content/uploads/2015/08/Snimok-ekrana-ot-2020-05-01-11-28-10.png)

Для простого сканирования можно запускать утилиту без опций. Детальнее о её опциях можно узнать в статье [про сканирование сети в Nmap](https://losst.pro/kak-polzovatsya-nmap-dlya-skanirovaniya-seti). Эта утилита ещё будет полезна если вы хотите посмотреть какие порты на компьютере доступны из интернета.

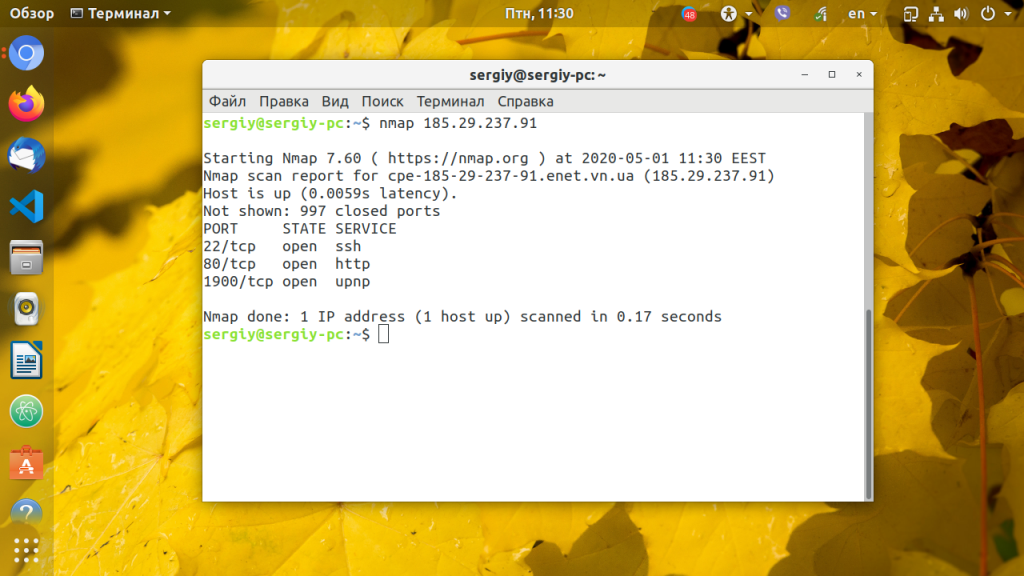
Если это публичный сервер, то результат скорее всего не будет отличатся от локального сканирования, но на домашнем компьютере все немного по другому. Первый вариант - используется роутер и в сеть будут видны только порты роутера, еще одним порогом защиты может стать NAT-сервер провайдера. Технология NAT позволяет нескольким пользователям использовать один внешний IP адрес. И так для просмотра открытых внешних портов сначала узнаем внешний ip адрес, для надежности воспользуемся онлайн сервисом:

wget -O - -q eth0.me

[](https://losst.pro/wp-content/uploads/2015/08/Snimok-ekrana-ot-2020-05-01-11-30-41.png)

Дальше запускаем сканирование:

 nmap 185.29.237.91

[](https://losst.pro/wp-content/uploads/2015/08/Snimok-ekrana-ot-2020-05-01-11-30-58.png)

В результате мы видим, что открыт порт 80 веб-сервера и 22 - порт службы ssh, я их не открывал, эти порты открыты роутером, 80 - для веб-интерфейса, а 22 для может использоваться для обновления прошивки. А еще можно вообще не получить результатов, это будет означать что все порты закрыты, или на сервере установлена система защиты от вторжений IDS. Такая проверка портов может оказаться полезной для того, чтобы понять находится ли ваш компьютер в безопасности и нет ли там лишних открытых портов, доступных всем.

**5. Zenmap**

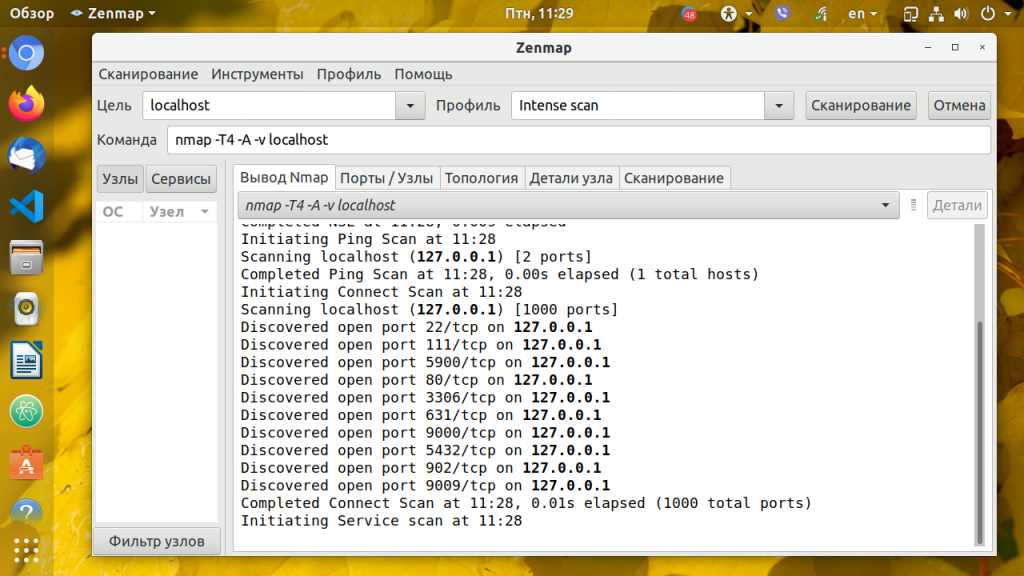
Программа Zenmap - это графический интерфейс для nmap. Она не делает ничего нового кроме того, что может делать nmap, просто предоставляет ко всему этому удобный интерфейс. Для её установки выполните:

sudo apt install zenmap

Запустить программу можно из главного меню или командой:

zenmap

Затем введите адрес **localhost** в поле **Цель**и нажмите кнопку**Сканирование**:

[](https://losst.pro/wp-content/uploads/2015/08/Snimok-ekrana-ot-2020-05-01-11-29-10.png)

После завершения сканирования утилита вывела список открытых портов Linux.