Сети

Networking

- Кто слушает порт в Linux

Кто слушает порт в Linux

Открытый доступ к порту хоть и является угрозой безопасности системы, но по сути ничего плохого не представляет до тех пор, пока его не начинает использовать программа. А чтобы выяснить какая программа слушает какой порт можно использовать утилиты "netstat" (или "ss") и "lsof".

Чтобы узнать информацию о программе, которая прослушивает определённый порт, можно воспользоваться командой "lsof" со следующими ключами:

```
sudo lsof -i :номер_порта
```

Здесь "номер_порта" - это цифра.

Пример результата выполнения команды с 53 портом:

```
$: sudo lsof -i :53
COMMAND   PID            USER   TYPE NODE NAME
systemd-r 818 systemd-resolve   IPv4  UDP localhost:domain
systemd-r 818 systemd-resolve   IPv4  TCP localhost:domain (LISTEN)
```

Но рекомендуем чаще запускать команду для получения списка программ, которые используют какие-либо tcp/udp порты. В этом помогает "netstat" или "ss":

```
sudo netstat -lntup
```

Опишем все ключи, которые используются в команде

- -l показать только прослушиваемые "LISTEN" порты.
- -n показывать адреса как ip, а не пытаться определять домены.
- -t показывать TCP порты.
- -u показывать UDP порты.
- -p показать название программы, которая слушает порт.

Если запустить эту команду на веб сервере, то команда распечатает в терминале такую информацию (некоторые столбцы скрыты):

```
$: sudo netstat -lntup
Prt  Local Addr     State   PID/Program
tcp  0.0.0.0:443    LISTEN  204/nginx
tcp  0.0.0.0:80     LISTEN  202/nginx
tcp  0.0.0.0:22     LISTEN  174/sshd
udp  127.0.0.1:323          233/chronyd
```

По результату можно заметить какая программа прослушивает какой порт. Если ip в секции "Local Address" равен "127.0.0.1", то это локальное обращение. Такой порт можно не

закрывать фаерволом - он и так не будет доступен извне. Но ip с нулями "0.0.0.0" говорят о том, что программа слушает все адреса. То есть она примет любой запрос, в том числе внешний.