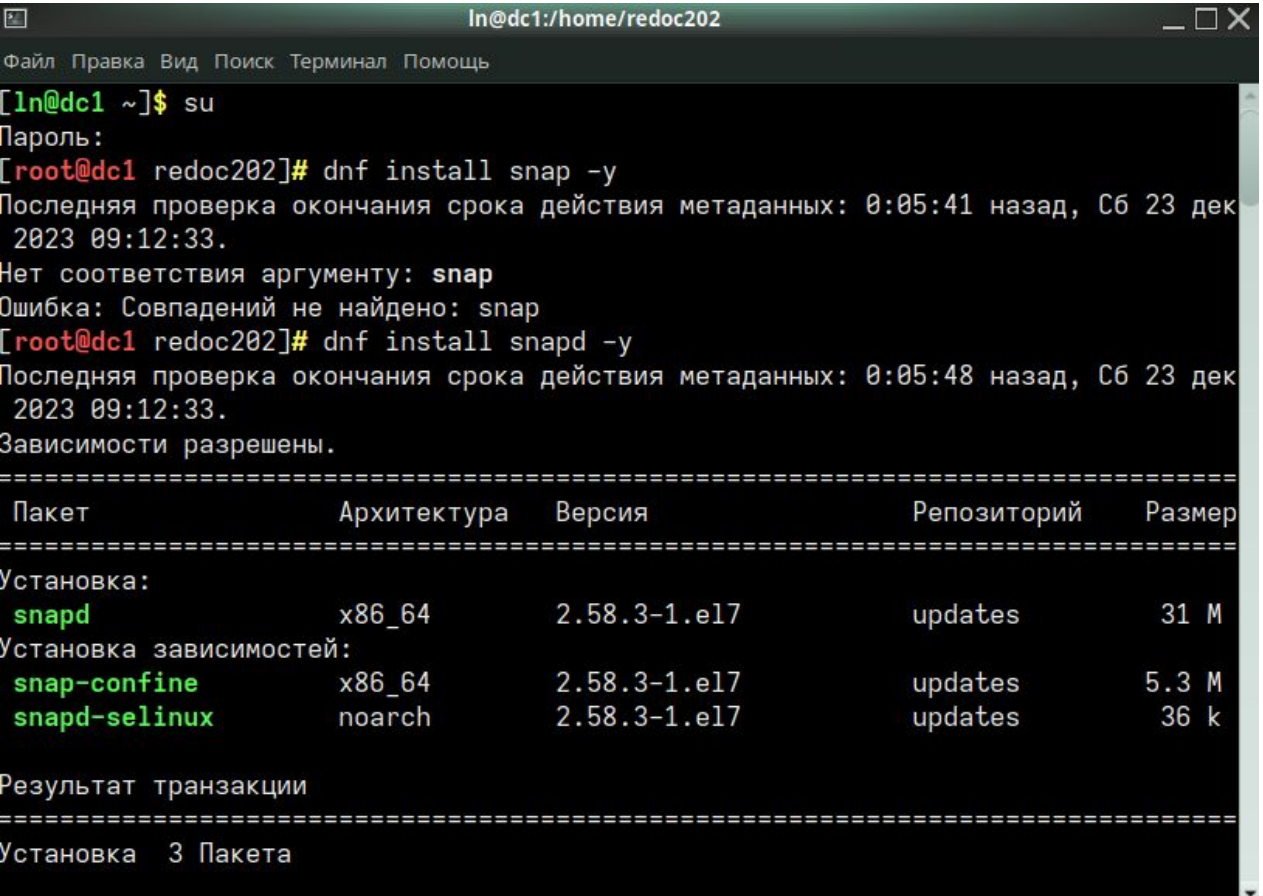
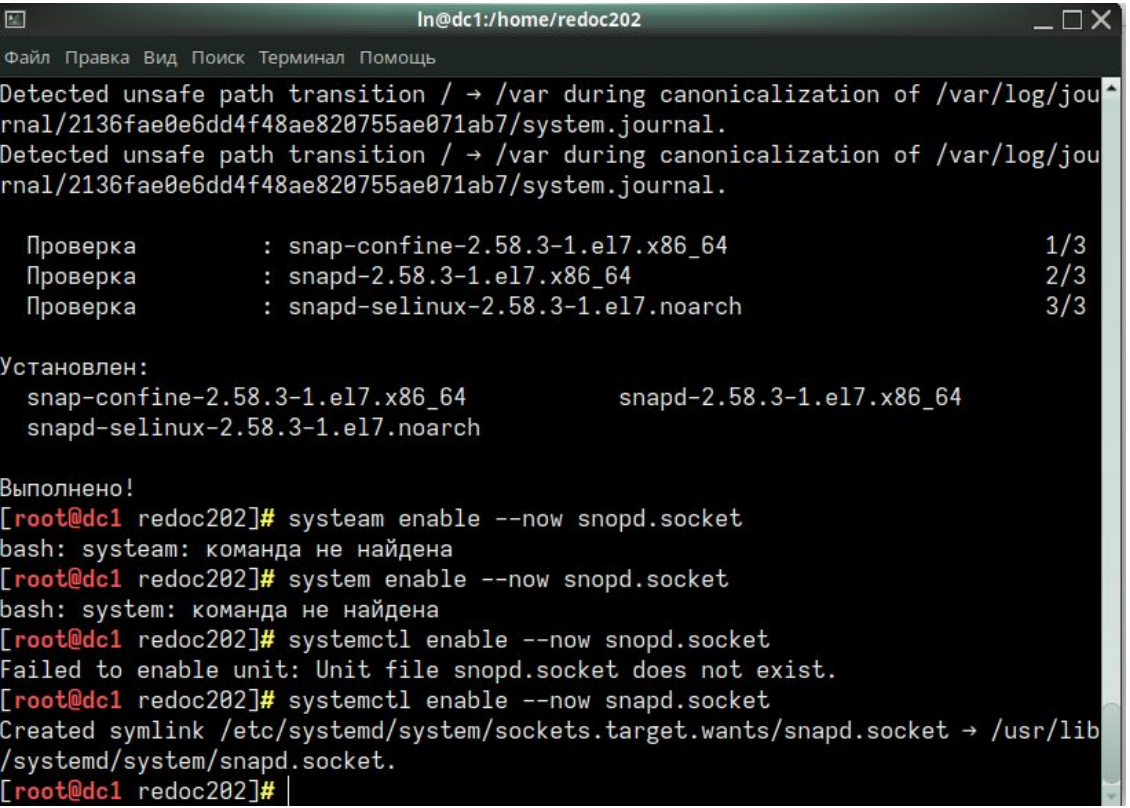
Шаг 1



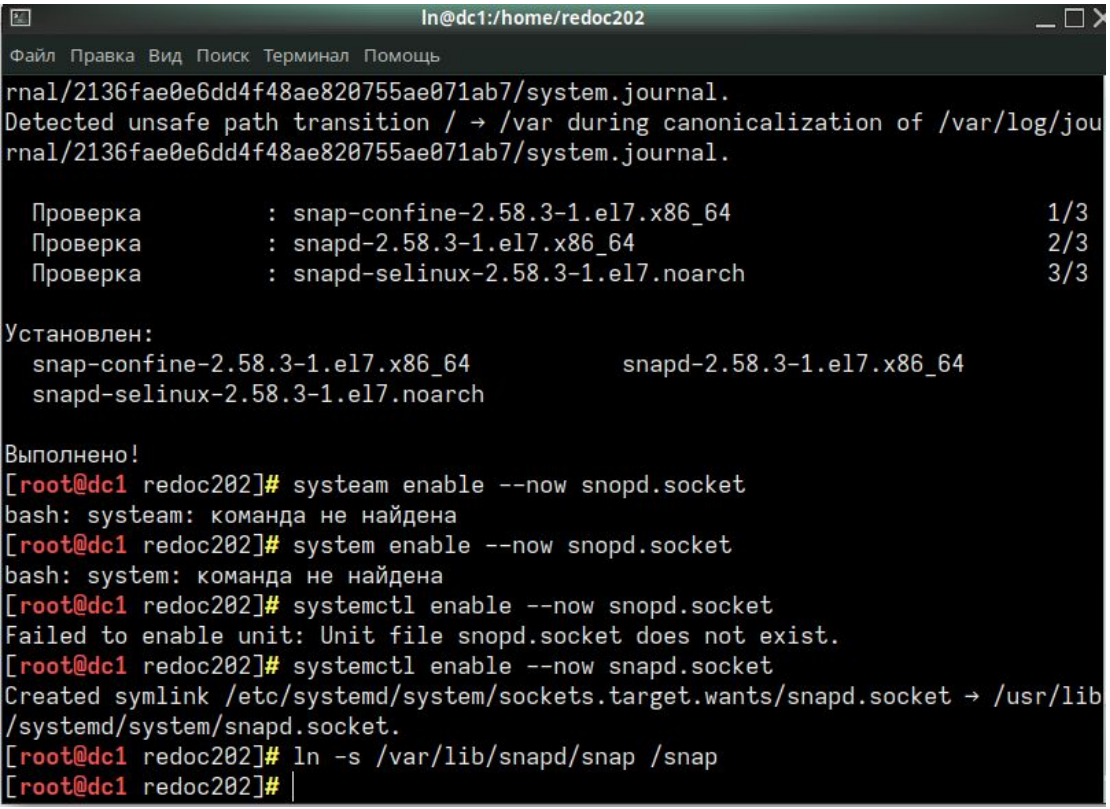
Скачиваем снап

Шаг 2



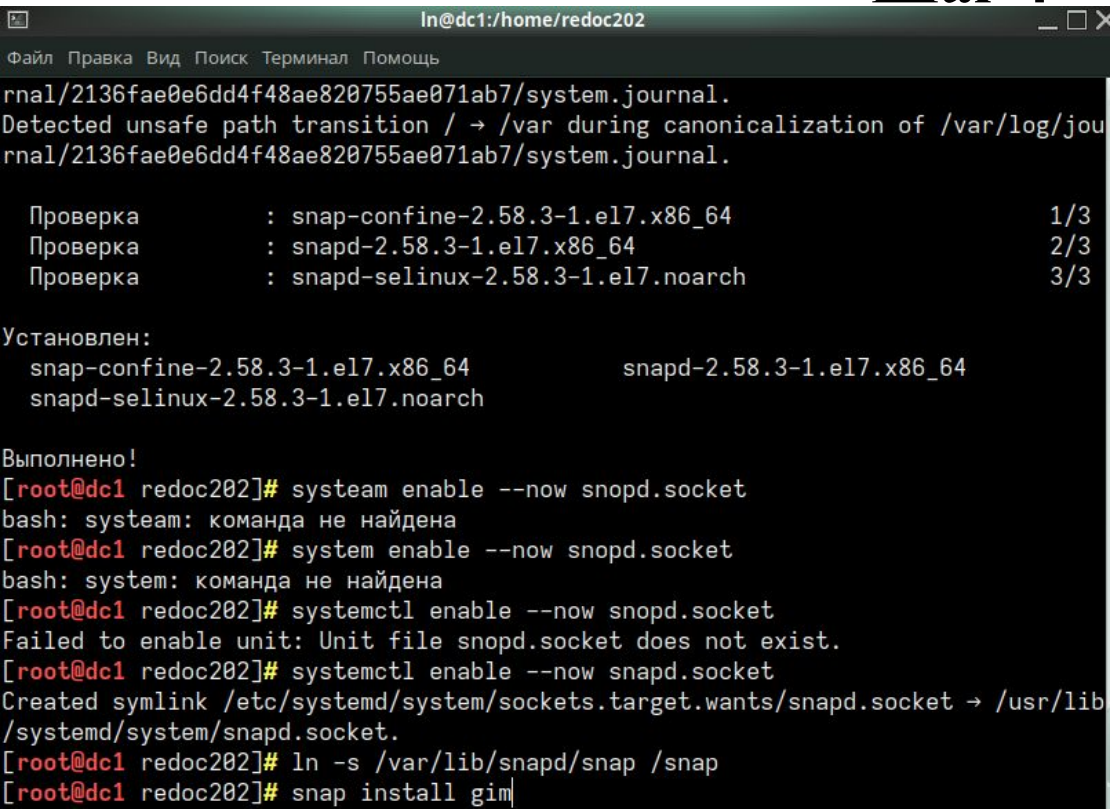
Проверка сокета snap

Шаг 3



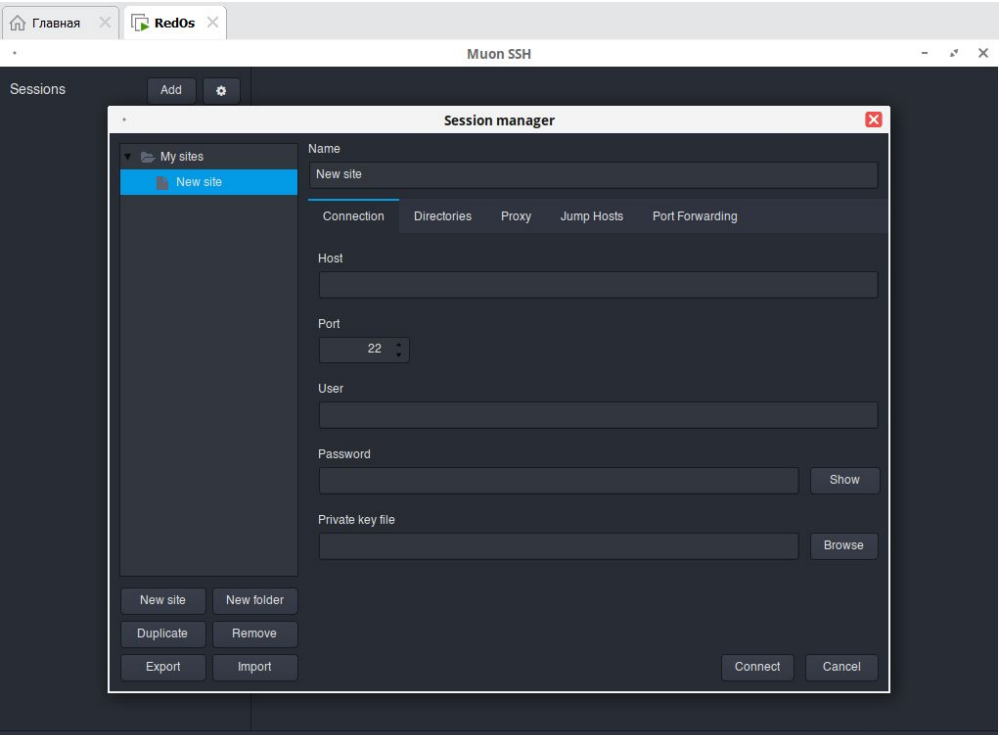
Включаем поддержку классической привязки

Шаг 4



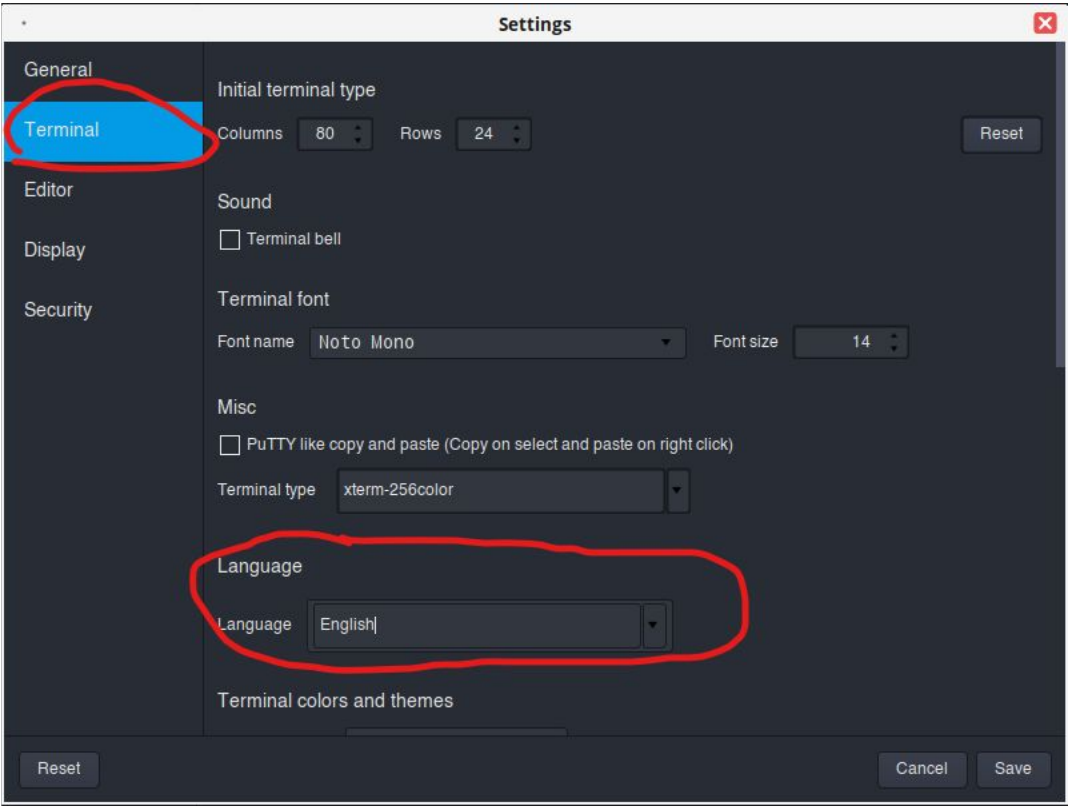
Устанавливаем графический редоктор гим

Шаг 5



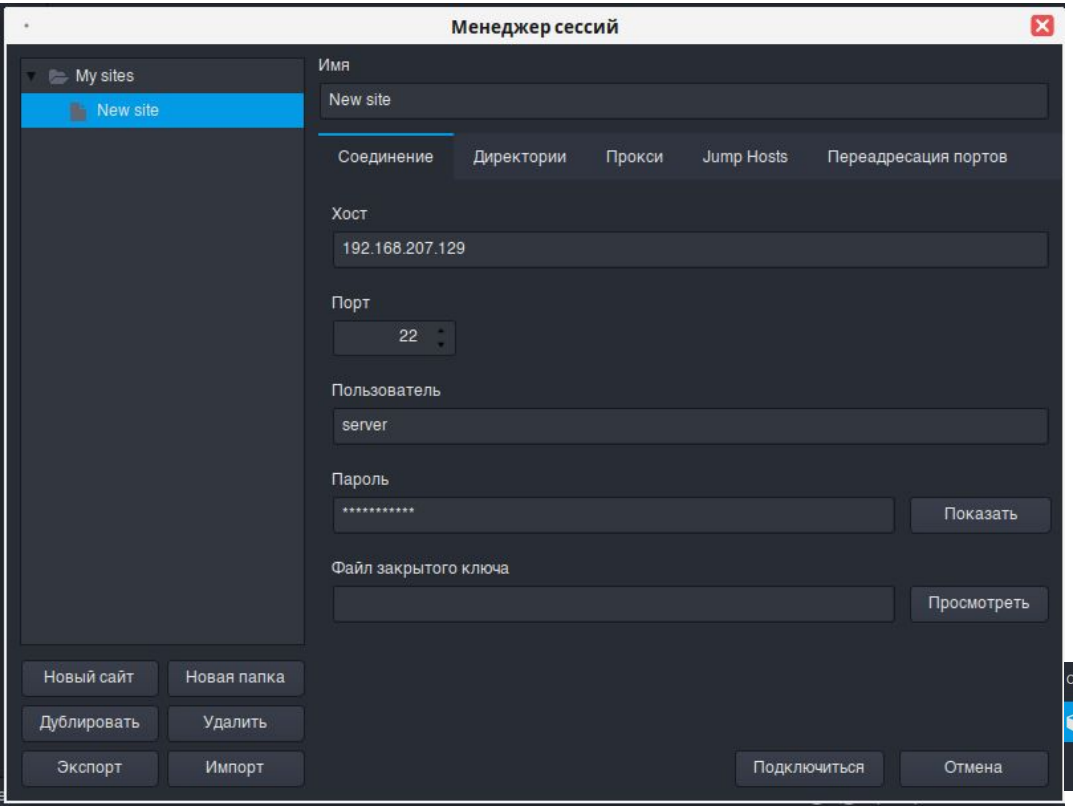
скачиваем muon

Шаг 6

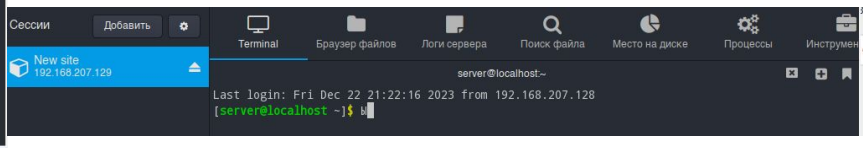


Ставим английский язык

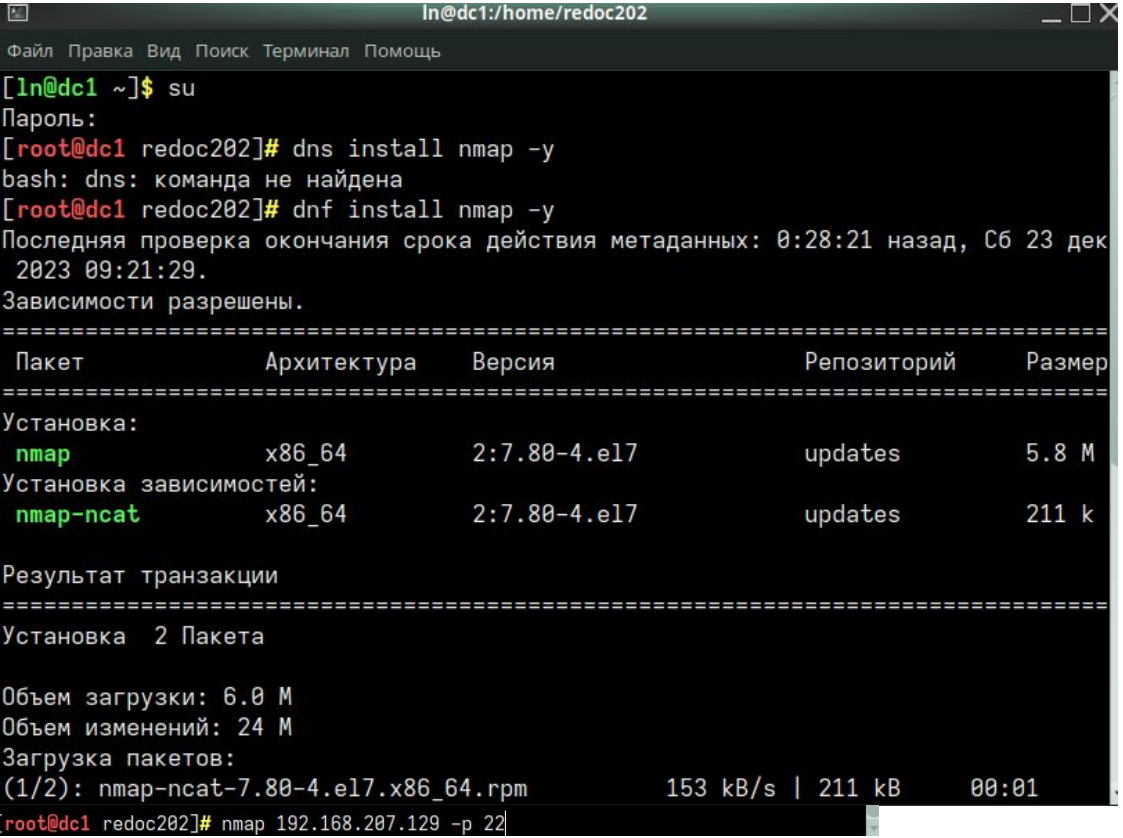
Шаг 7



В поле Хост укажите IP-адрес сервера или имя хоста.
В поле Порт укажите нормер порта для подключения (по умолчанию используется порт 22).
В поле Пользователь укажите имя пользователя, к учетной записи которого необходимо подключиться.
В поле Пароль укажите пароль от учетной записи указанного выше пользвоателя.(на redos обязательно должен стоять пароль,чтобы подключиться к терминалу)
В поле Файл закрытого ключа загрузите файл из каталога, в котором хранится закрытый ключ.



Шаг 8



Устанавливаем nmap и подключаемся к локальному серверу

Шаг 9

```
[root@localhost server]# nmap -sV 192.168.207.129 -p 1-65535 | grep open
22/tcp  open  ssh     OpenSSH 8.9 (protocol 2.0)
111/tcp open  rpcbind 2-4 (RPC #100000)
[root@localhost server]# S
```

Данный код,демонстрирует нам, все открытые порты на сетевом узле

```
[root@localhost server]# nmap --open 192.168.207.129
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:32 MSK
Nmap scan report for 192.168.207.129
Host is up (0.0000090s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
[root@localhost server]#
```

Возможен вариант с указанием параметра --open

Шаг 10

```
[root@localhost server]#  nmap -sn 192.168.207.129/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:37 MSK
Nmap scan report for 192.168.207.1
Host is up (0.00018s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.207.2
Host is up (0.000095s latency).
MAC Address: 00:50:56:ED:76:BF (VMware)
Nmap scan report for 192.168.207.128
Host is up (0.00058s latency).
MAC Address: 00:0C:29:44:92:B4 (VMware)
Nmap scan report for 192.168.207.254
Host is up (0.000080s latency).
MAC Address: 00:50:56:EC:35:2A (VMware)
Nmap scan report for 192.168.207.129
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.00 seconds
[root@localhost server]#
```

Сканировать сеть методом ping для обнаружения активных узлов.При этом в выводе команды будут отображаться IP и MAC-адреса.

Шаг 11

```
[root@localhost server]# nmap -sV 192.168.207.129
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:39 MSK
Nmap scan report for 192.168.207.129
Host is up (0.0000090s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.9 (protocol 2.0)
111/tcp open  rpcbind 2-4 (RPC #100000)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.47 seconds
[root@localhost server]#
```

Информация о сетевом узле

```
[root@localhost server]# nmap -sV -p 22,53 8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:43 MSK
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0035s latency).

PORT   STATE    SERVICE    VERSION
22/tcp filtered ssh
53/tcp open     tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.76 seconds
[root@localhost server]#
```

Сканирование определенных портов, в примере указаны 22 (ssh) и 53 (dns):

Шаг 12

```
[root@localhost server]#  nmap 192.168.207.129/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:47 MSK
Nmap scan report for 192.168.207.1
Host is up (0.00026s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
7070/tcp open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.207.2
Host is up (0.00063s latency).
Not shown: 999 closed ports
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:ED:76:BF (VMware)

Nmap scan report for 192.168.207.128
Host is up (0.0033s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 00:0C:29:44:92:B4 (VMware)

Nmap scan report for 192.168.207.254
Host is up (0.00014s latency).
All 1000 scanned ports on 192.168.207.254 are filtered
MAC Address: 00:50:56:EC:35:2A (VMware)

Nmap scan report for 192.168.207.129
Host is up (0.000010s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
```

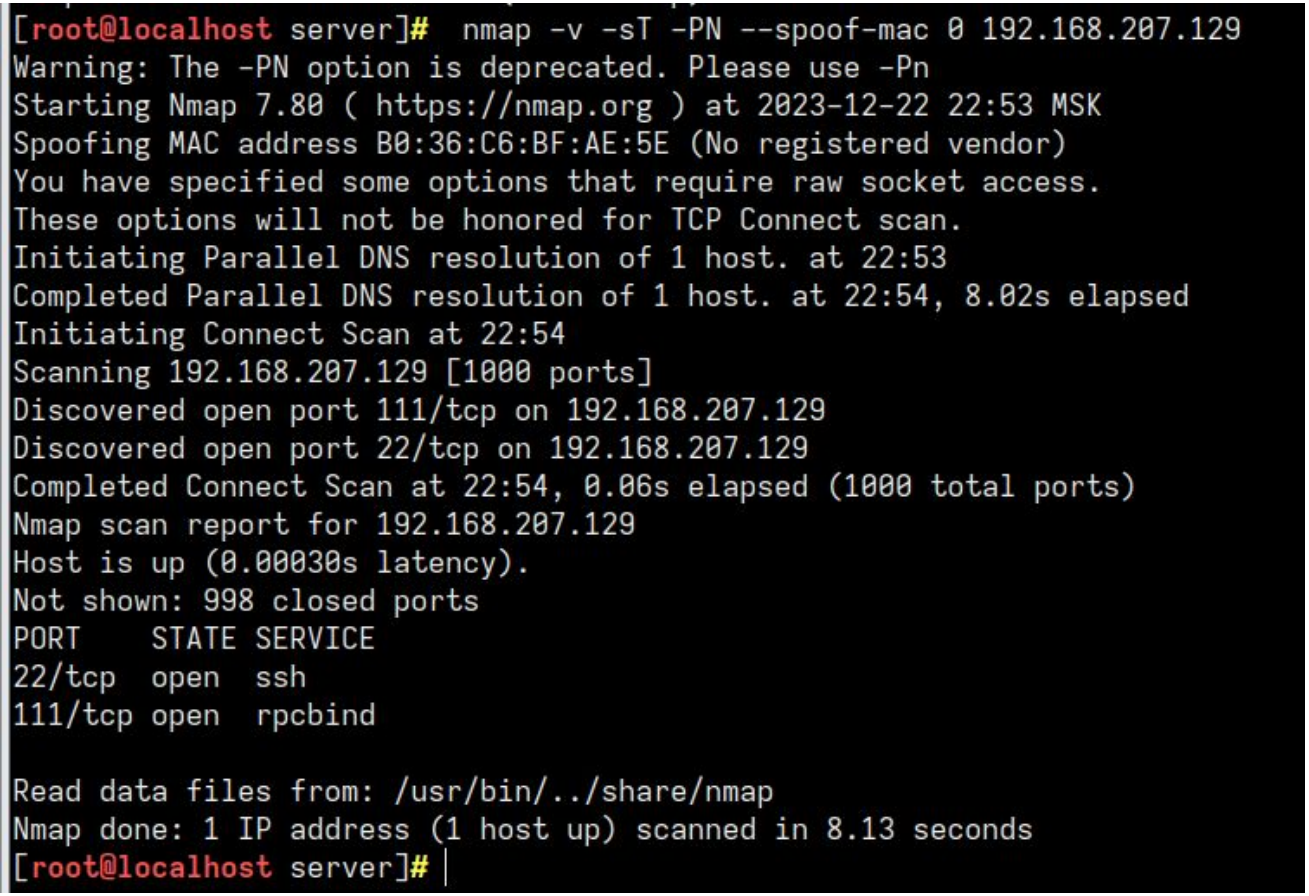
Сканирование всей подсети

Шаг 13

```
[root@localhost server]# nmap -T5 192.168.207.129/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:52 MSK
Nmap scan report for 192.168.207.1
Host is up (0.00019s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
7070/tcp open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.207.2
Host is up (0.0012s latency).
Not shown: 999 closed ports
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:ED:76:BF (VMware)

Nmap scan report for 192.168.207.128
Host is up (0.0029s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 00:0C:29:44:92:B4 (VMware)

Nmap scan report for 192.168.207.254
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.207.254 are filtered
MAC Address: 00:50:56:EC:35:2A (VMware)

Nmap scan report for 192.168.207.129
Host is up (0.000010s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
```

Быстрое сканирование открытых портов на всех хостах подсети:

Шаг 14



Сканирование с использованием подмены MAC-адреса, в данном случае одно устройство/приложение маскируется под другое, указывая его MAC-адрес. В данном примере «0» означает, что nmap выберет случайный MAC-адрес.