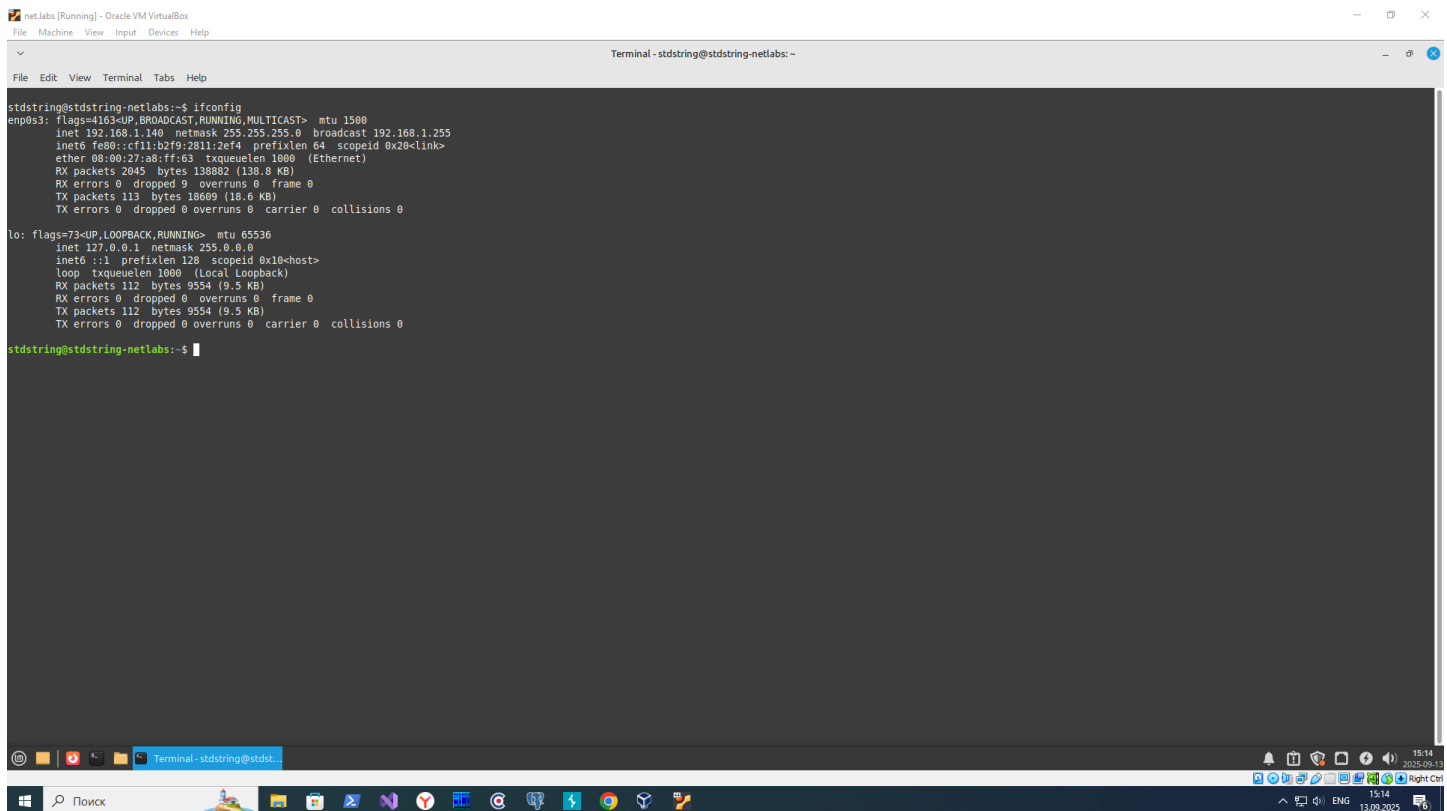


Задание:

Установите Nmap и выполните в нем следующие задачи:

1. Проведите сканирование домашней сети.
2. Обнаружьте все хосты, входящие в сеть.
3. Определите операционную систему всех устройств.
4. Постройте топологию сети.
5. Обнаружьте открытые порты.
6. Сохраните результаты сканирования.

Локальная конфигурация сетевого интерфейса

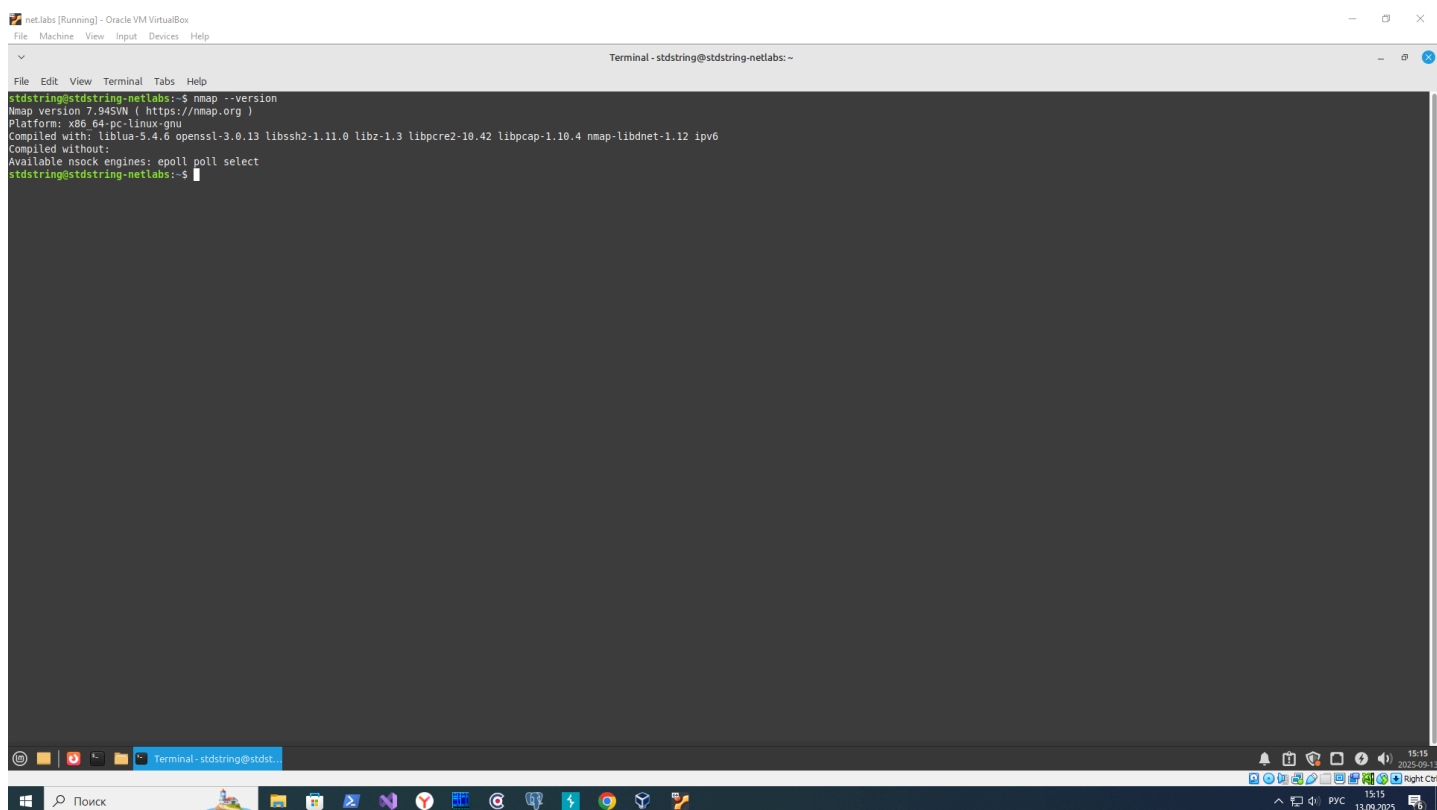


```
stdstring@stdstring-netlabs:~$ ifconfig
emp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.140 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::cf11:b2f9:2811:2ef4 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:a8:ff:63 txqueuelen 1000 (Ethernet)
    RX packets 2045 bytes 138882 (138.8 KB)
    RX errors 0 dropped 9 overruns 0 frame 0
    TX packets 113 bytes 18609 (18.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

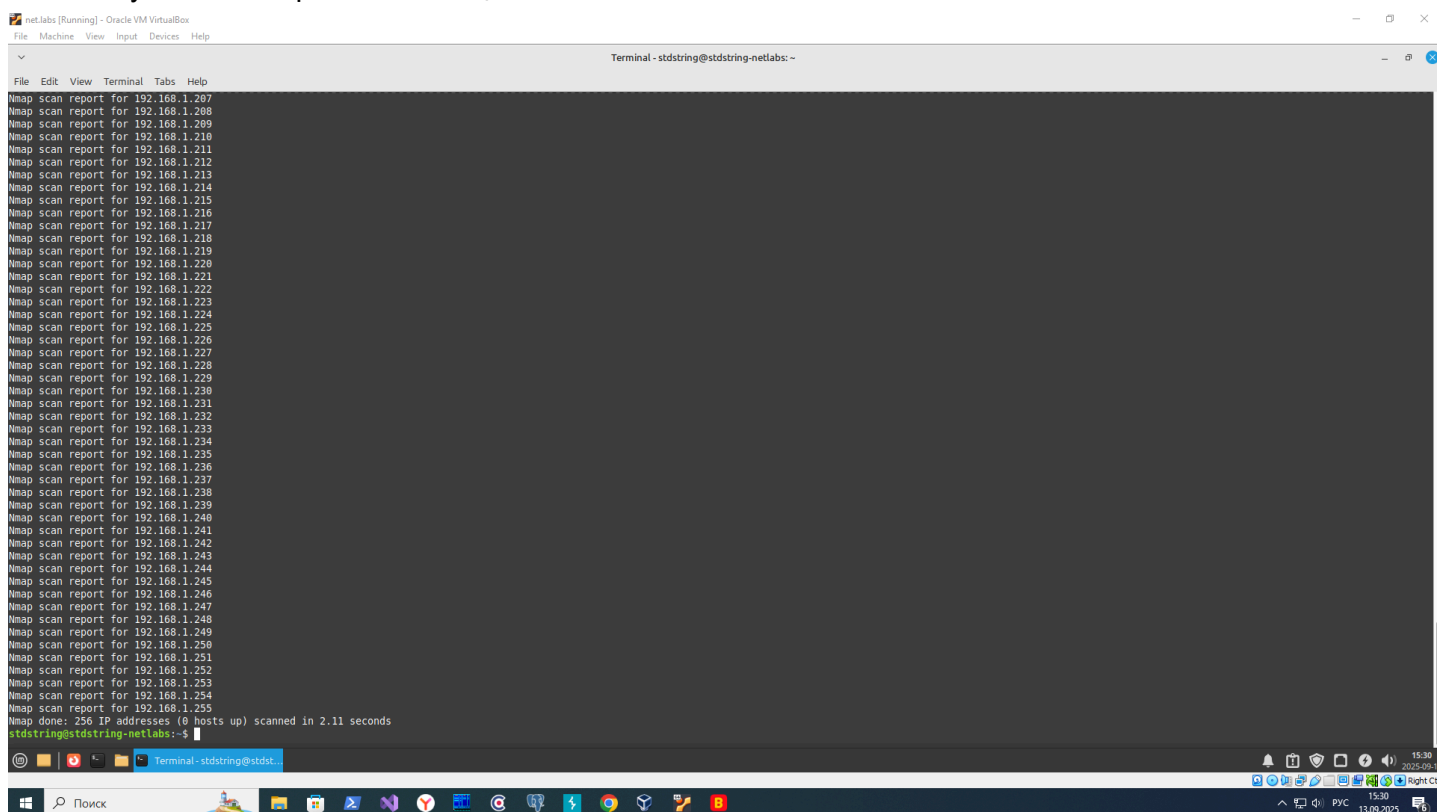
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 112 bytes 9554 (9.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 112 bytes 9554 (9.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

stdstring@stdstring-netlabs:~$
```

Проверяю версию nmap:



Запускаю сканирование с опцией sL:



Результат - ничего не обнаружено: 0 hosts up

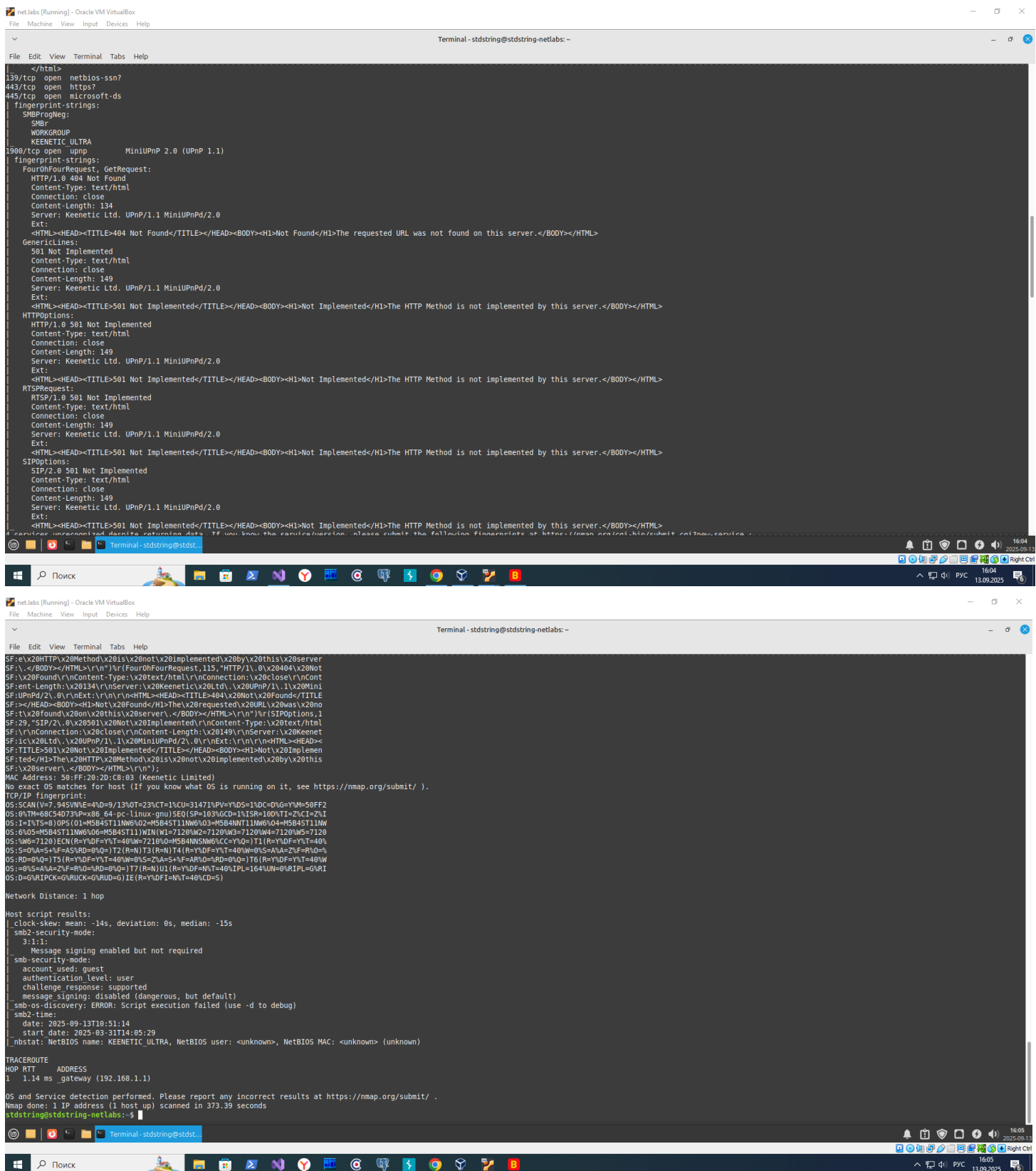
Запускаю сканирование с опцией sn:

```
stdstring@stdstring-netlabs:~$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 15:35 +05
Nmap scan report for gateway (192.168.1.1)
Host is up (0.0048s latency).
Nmap scan report for 192.168.1.2
Host is up (0.0040s latency).
Nmap scan report for 192.168.1.78
Host is up (0.044s latency).
Nmap scan report for 192.168.1.107
Host is up (0.0017s latency).
Nmap scan report for stdstring-netlabs (192.168.1.140)
Host is up (0.000027s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.52 seconds
stdstring@stdstring-netlabs:~$
```

Результат - обнаружено 5 хостов со следующими адресами: 192.168.1.1, 192.168.1.2, 192.168.1.78, 192.168.1.107, 192.168.1.140. Из них один хост с IP адресом 192.168.1.140 - исходный хост, хост с IP адресом 192.168.1.1 - маршрутизатор (gateway).

Пробую определить операционную систему на каждом хосте

1. Проверяю хост 192.168.1.1 (маршрутизатор):



Видно, что на этом хосте операционная система - это KeeneticOS (это видно по разным fingerprint). Это ожидаемо, т.к. хост 192.168.1.1 - это маршрутизатор

2. Проверяю хост 192.168.1.2:

```
stdstring@stdstring-netlabs:~$ sudo nmap -O 192.168.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 16:09 +05
Nmap scan report for 192.168.1.2
Host is up (0.00030s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2179/tcp   open  vnc
5357/tcp   open  wsdapi
5432/tcp   open  postgresql
MAC Address: 68:85:CA:AA:9B:9E (Intel Corporate)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows 10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
stdstring@stdstring-netlabs:~$
```

Видно, что на этом хосте операционная система - это Microsoft Windows 10 1709 - 1909.

3. Проверяю хост 192.168.1.78:

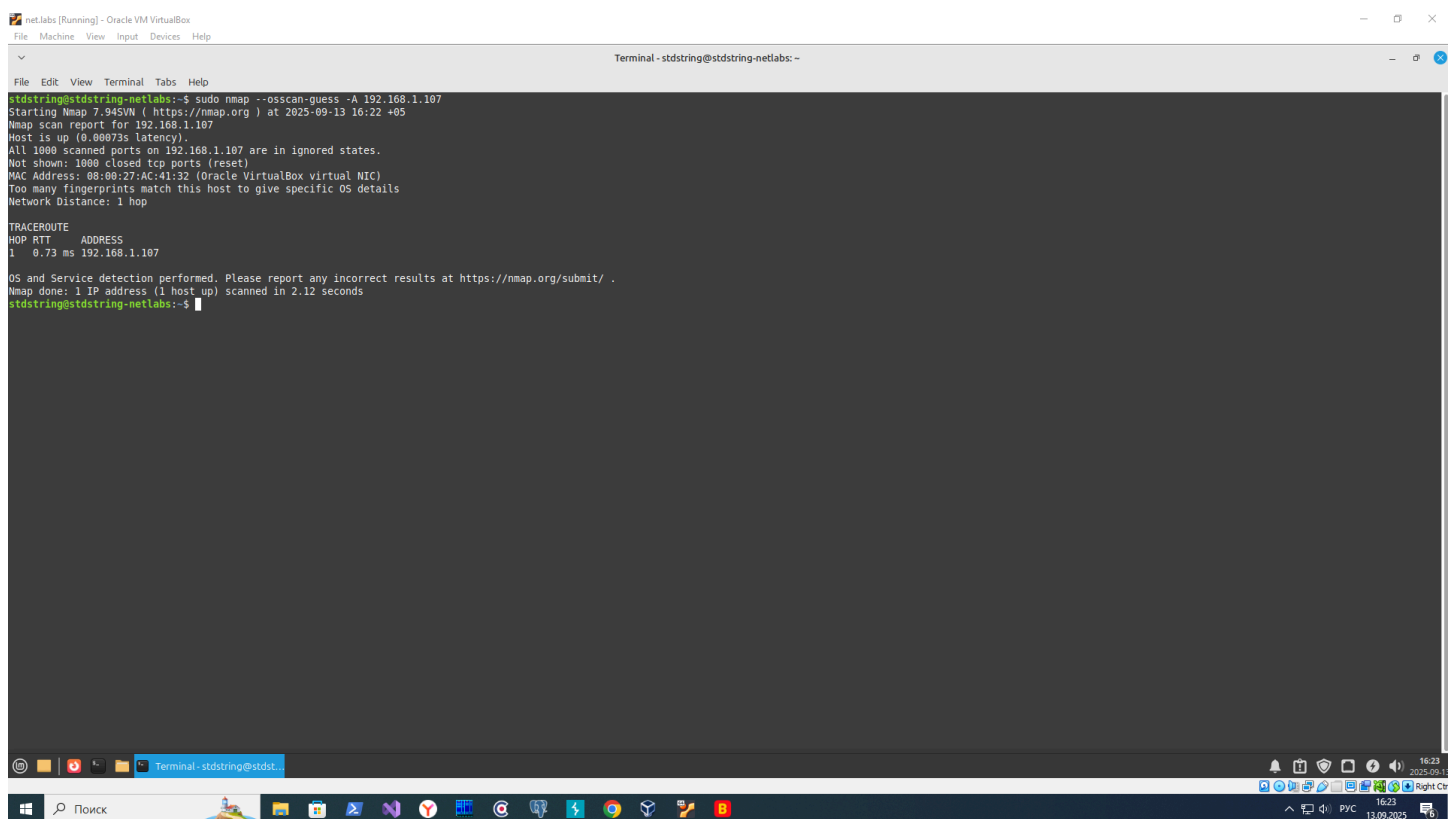
```
stdstring@stdstring-netlabs:~$ sudo nmap --osscan-guess -A 192.168.1.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 16:15 +05
Nmap scan report for 192.168.1.78
Host is up (0.0038s latency).
All 1000 scanned ports on 192.168.1.78 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: F0:B0:40:92:A7F5 (Hunan PN-Link Technology Limited)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 3.77 ms 192.168.1.78

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds
stdstring@stdstring-netlabs:~$
```

На данном хосте версию ОС определить не удалось

4. Проверяю хост 192.168.1.107:



```
netLabs [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal - stdstring@stdstring-netlabs: ~

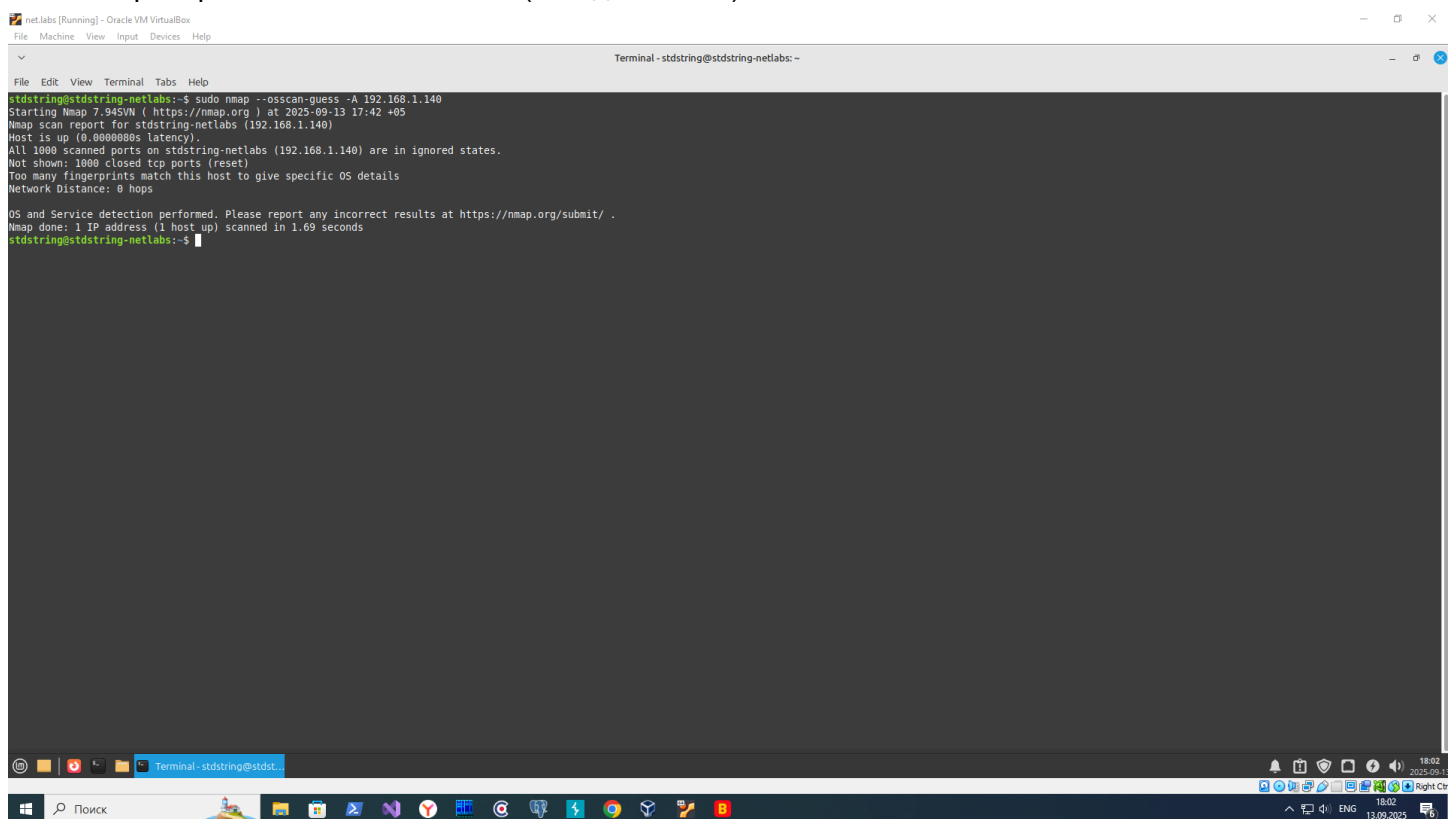
File Edit View Terminal Tabs Help

stdstring@stdstring-netlabs:~$ sudo nmap --osscan-guess -A 192.168.1.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 16:22 +05
Nmap scan report for 192.168.1.107
Host is up (0.00073s latency).
All 1000 scanned ports on 192.168.1.107 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:AC:41:32 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.73 ms 192.168.1.107

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
stdstring@stdstring-netlabs:~$
```

На данном хосте версию ОС определить не удалось
5. Проверяю хост 192.168.1.140 (исходный хост):



```
netLabs [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal - stdstring@stdstring-netlabs: ~

File Edit View Terminal Tabs Help

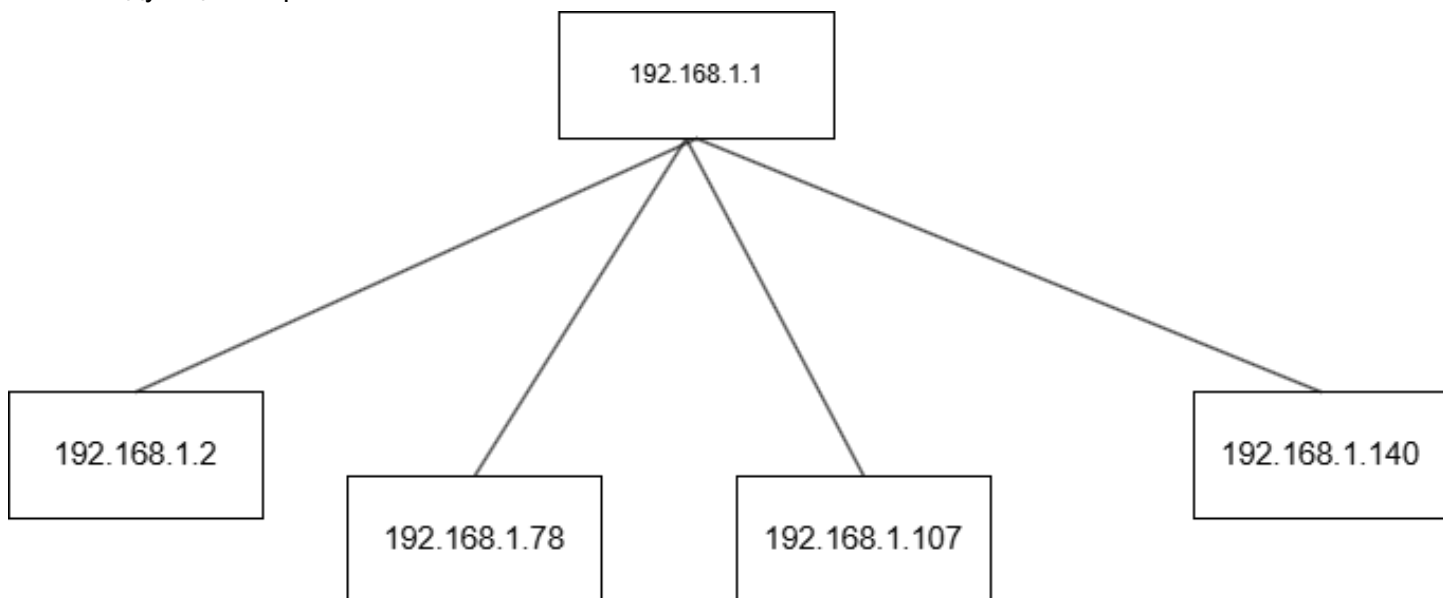
stdstring@stdstring-netlabs:~$ sudo nmap --osscan-guess -A 192.168.1.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 17:42 +05
Nmap scan report for stdstring-netlabs (192.168.1.140)
Host is up (0.0000000s latency).
All 1000 scanned ports on stdstring-netlabs (192.168.1.140) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
stdstring@stdstring-netlabs:~$
```

На данном хосте версию ОС определить не удалось
Строю топологию сети. В сети присутствуют:
1. Маршрутизатор с IP адресом 192.168.1.1.

2. Компьютер с ОС Microsoft Windows 10 с IP адресом 192.168.1.2.
3. Компьютер (устройство) с неопределенной ОС с IP адресом 192.168.1.78
4. Компьютер (устройство) с неопределенной ОС с IP адресом 192.168.1.107 (на самом деле там Astra Linux)
5. Компьютер (устройство) с неопределенной ОС с IP адресом 192.168.1.140 (на самом деле там Mint 22.1)

Все эти устройства подключены к центральному узлу (маршрутизатору) - поэтому топология сети в данном случае звезда. Если ее нарисовать, то выглядеть она будет следующим образом:



Пробую определить открытые порты:

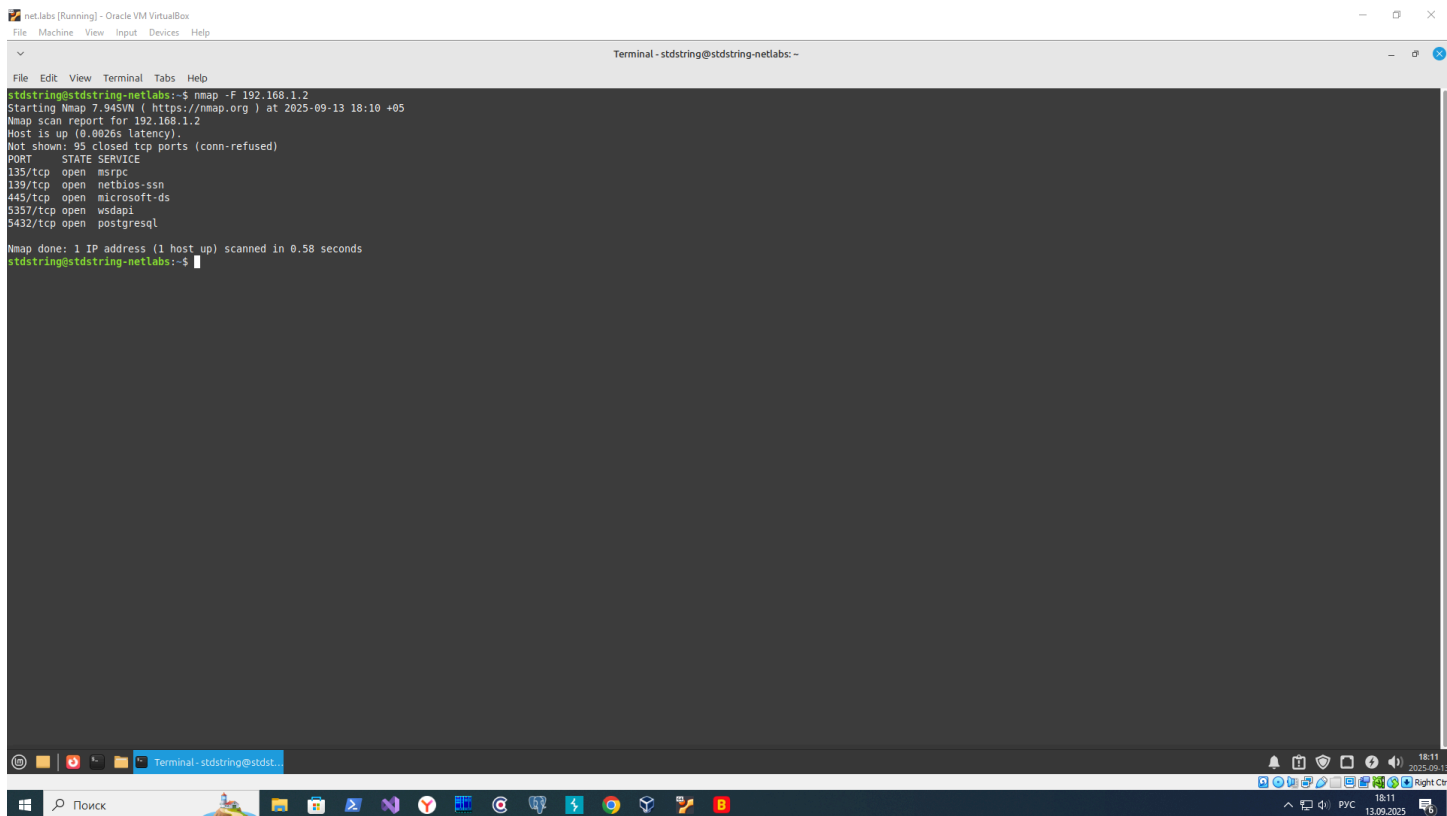
1. Проверяю хост 192.168.1.1 (маршрутизатор):

```
stdstring@stdstring-netlabs:~$ nmap -F 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 18:09 +05
Nmap scan report for gateway (192.168.1.1)
Host is up (0.0030s latency).
Not shown: 93 closed tcp ports (conn-refused)
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1900/tcp  open  upnp
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
stdstring@stdstring-netlabs:~$
```

The screenshot shows a terminal window with the output of an Nmap scan. The scan was performed on the host 192.168.1.1, which is identified as 'gateway'. The results show that the host is up and several ports are open: 23/tcp (telnet), 53/tcp (domain), 80/tcp (http), 139/tcp (netbios-ssn), 443/tcp (https), 445/tcp (microsoft-ds), and 1900/tcp (upnp). The terminal window is titled 'Terminal - stdstring@stdstring-netlabs: ~' and is running on a Windows 10 desktop environment.

Нахожу 7 открытых портов

2. Проверяю хост 192.168.1.2:



```
net.labs [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

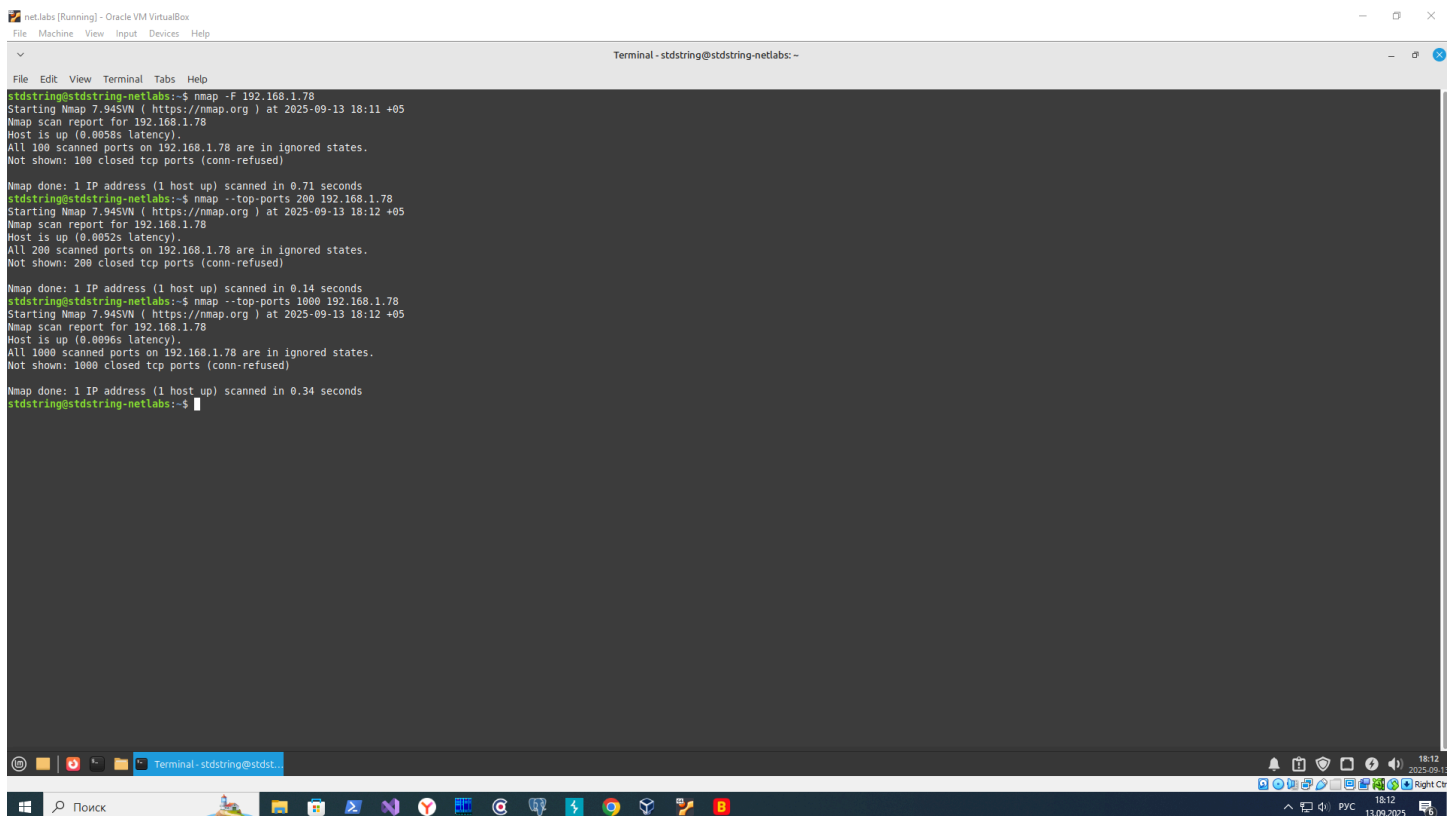
Terminal - stdstring@stdstring-netlabs: ~

stdstring@stdstring-netlabs:~$ nmap -F 192.168.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 18:10 +05
Nmap scan report for 192.168.1.2
Host is up (0.8826s latency).
Not shown: 95 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
5432/tcp   open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
stdstring@stdstring-netlabs:~$
```

Нахожу 5 открытых портов

3. Проверяю хост 192.168.1.78:



```
net.labs [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal - stdstring@stdstring-netlabs: ~

stdstring@stdstring-netlabs:~$ nmap -F 192.168.1.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 18:11 +05
Nmap scan report for 192.168.1.78
Host is up (0.8058s latency).
All 100 scanned ports on 192.168.1.78 are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

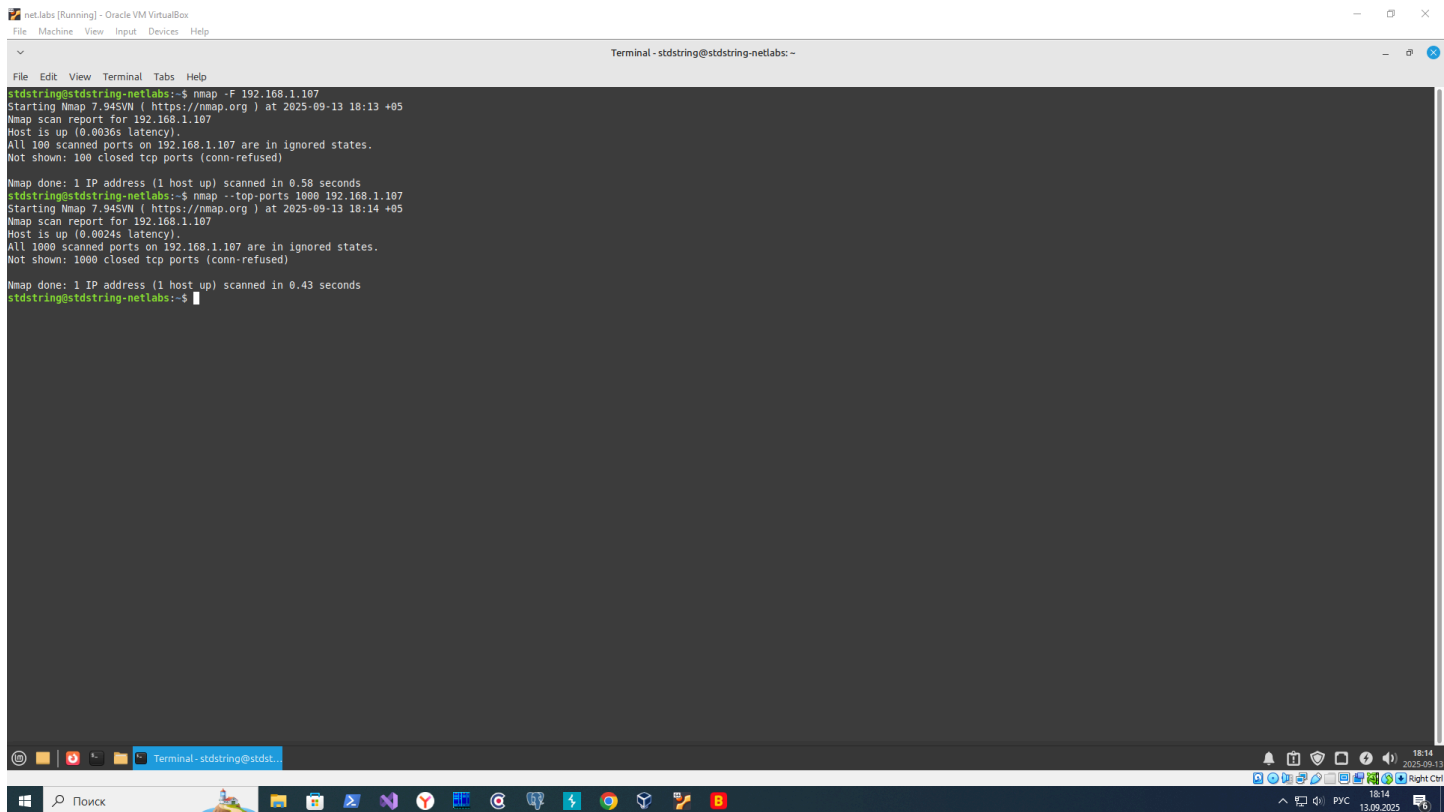
Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
stdstring@stdstring-netlabs:~$ nmap --top-ports 200 192.168.1.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 18:12 +05
Nmap scan report for 192.168.1.78
Host is up (0.8052s latency).
All 200 scanned ports on 192.168.1.78 are in ignored states.
Not shown: 200 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
stdstring@stdstring-netlabs:~$ nmap --top-ports 1000 192.168.1.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 18:12 +05
Nmap scan report for 192.168.1.78
Host is up (0.8098s latency).
All 1000 scanned ports on 192.168.1.78 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
stdstring@stdstring-netlabs:~$
```

Открытых портов не обнаружено (все порты в ignored состоянии).

4. Проверяю хост 192.168.1.107:



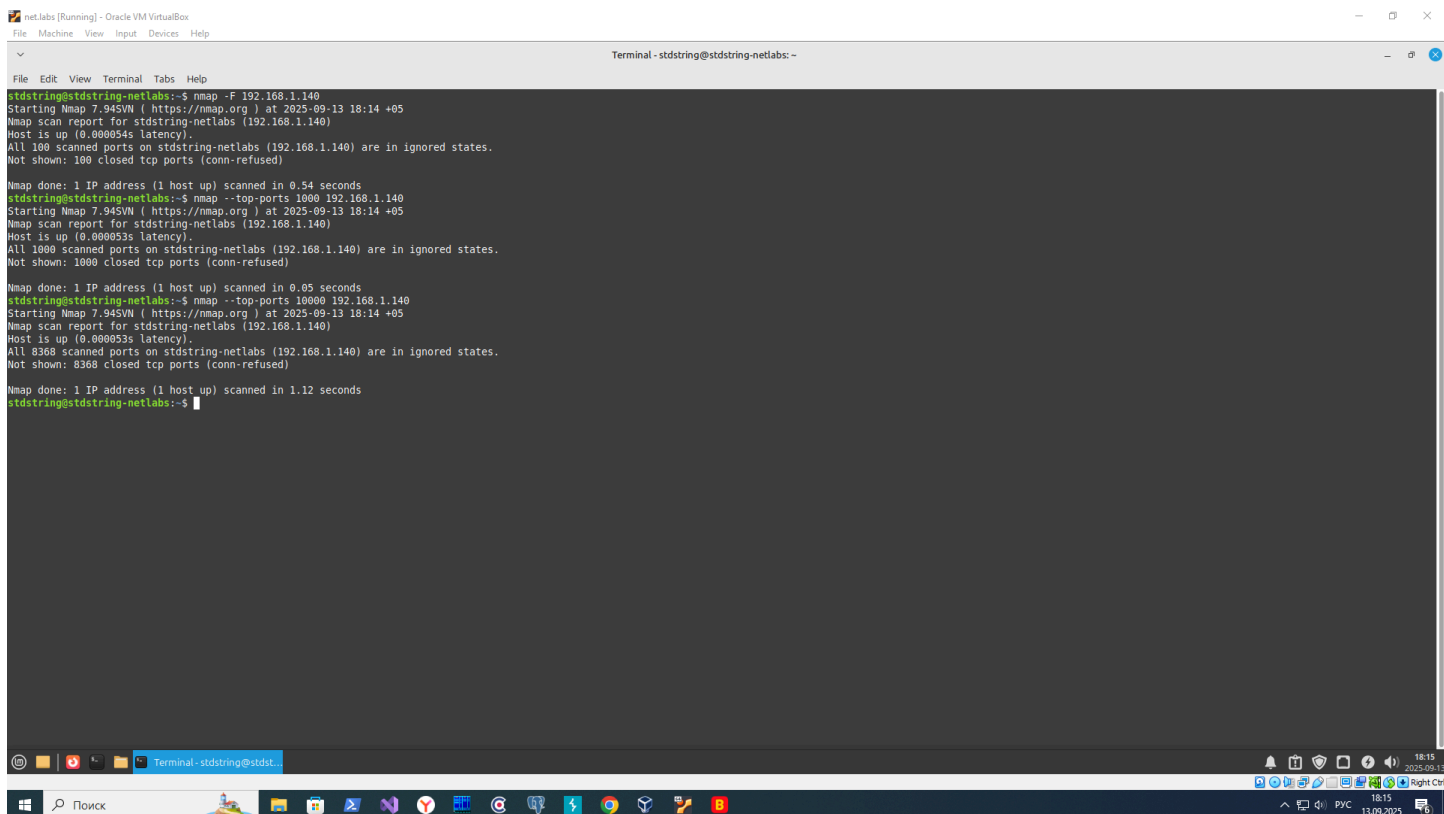
```
stdstring@stdstring-netlabs:~$ nmap -F 192.168.1.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 18:13 +05
Nmap scan report for 192.168.1.107
Host is up (0.0036s latency).
All 100 scanned ports on 192.168.1.107 are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
stdstring@stdstring-netlabs:~$ nmap --top-ports 1000 192.168.1.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 18:14 +05
Nmap scan report for 192.168.1.107
Host is up (0.0024s latency).
All 1000 scanned ports on 192.168.1.107 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
stdstring@stdstring-netlabs:~$
```

Открытых портов не обнаружено (все порты в ignored состоянии).

5. Проверяю хост 192.168.1.140 (исходный хост):



```
stdstring@stdstring-netlabs:~$ nmap -F 192.168.1.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 18:14 +05
Nmap scan report for stdstring-netlabs (192.168.1.140)
Host is up (0.000054s latency).
All 100 scanned ports on stdstring-netlabs (192.168.1.140) are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
stdstring@stdstring-netlabs:~$ nmap --top-ports 1000 192.168.1.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 18:14 +05
Nmap scan report for stdstring-netlabs (192.168.1.140)
Host is up (0.000033s latency).
All 1000 scanned ports on stdstring-netlabs (192.168.1.140) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
stdstring@stdstring-netlabs:~$ nmap --top-ports 8368 192.168.1.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 18:14 +05
Nmap scan report for stdstring-netlabs (192.168.1.140)
Host is up (0.000053s latency).
All 8368 scanned ports on stdstring-netlabs (192.168.1.140) are in ignored states.
Not shown: 8368 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds
stdstring@stdstring-netlabs:~$
```

Открытых портов не обнаружено (все порты в ignored состоянии).

Можно еще определить версии служб на хостах, на которых есть открытые порты:

1. Проверяю хост 192.168.1.1 (маршрутизатор):

The image shows a Windows 10 desktop environment. In the foreground, a terminal window titled "Terminal - stdstring@stdstring-netlabs:~" is open, displaying the output of an Nmap scan. The scan target is 192.168.1.1. The output shows that the host is up with a latency of 0.0032s. It lists several open ports: 22/tcp (SSH), 53/tcp (domain), 80/tcp (http), 139/tcp (netbios-ssn), 443/tcp (https), and 1900/tcp (upnp). The scan also identifies services like OpenSSH, Web server, and MiniUPnP. The terminal window is part of a larger application window titled "netlabs (Running) - Oracle VM VirtualBox". The desktop background is a Windows 10 wallpaper, and the taskbar at the bottom shows various icons including the Start button, search bar, and several pinned applications like File Explorer, Edge, and the terminal itself. The system tray in the bottom right corner shows the date and time as 18:19 on 2025-09-11.

2. Проверяю хост 192.168.1.2:

The image shows a Windows 10 desktop environment. At the top, a taskbar contains the Start button, a search bar with the text "Поиск", and several pinned application icons including File Explorer, Microsoft Edge, and various utility tools. The main area of the screen is occupied by a terminal window titled "Terminal - stdstring@stdstring-netlabs:". The terminal displays the output of an Nmap scan command:

```
stdstring@stdstring-netlabs:~$ nmap -sV 192.168.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-13 18:20 +05
Nmap scan report for 192.168.1.2
Host is up (0.0022s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
2179/tcp  open  vnc?
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5432/tcp  open  postgresql   PostgreSQL DB 9.6.0 or later
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.11 seconds
stdstring@stdstring-netlabs:~$
```

 The terminal window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The bottom of the screen shows the Windows taskbar with the system clock indicating 18:21 on 2025-09-13.