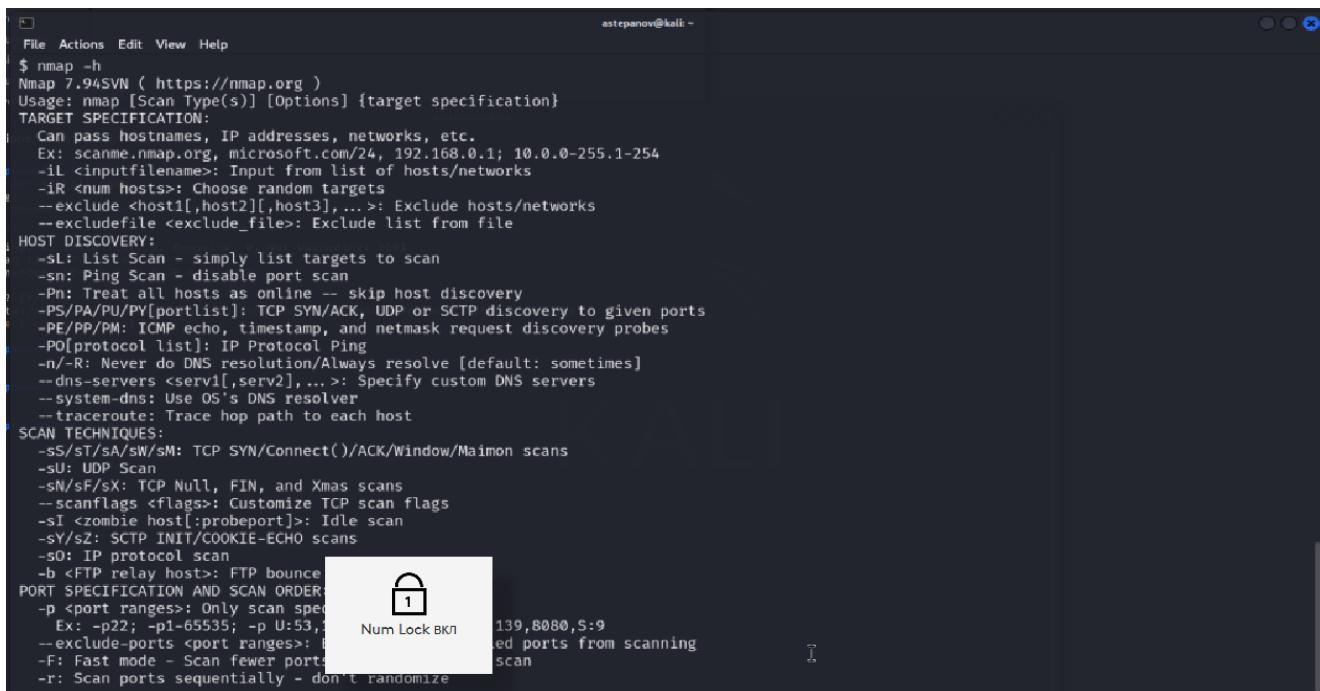


Модуль 2. Сканирование сетей (HW)

Лабораторная работа №2 (HW)

Для выполнения данной лабораторной работы пришлось устанавливать Windows на виртуальную машину

Шаг 1. Установите Nmap на Linux (на Kali nmap уже предустановлен)



The screenshot shows a terminal window with the command `$ nmap -h` entered. The output is the help documentation for Nmap 7.94sVN, which includes sections on TARGET SPECIFICATION, HOST DISCOVERY, SCAN TECHNIQUES, and PORT SPECIFICATION AND SCAN ORDER. A small window titled "Num Lock BNK" is overlaid on the terminal window, showing a lock icon and the number "1".

```
$ nmap -h
Nmap 7.94sVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
      -iL <inputfilename>: Input from list of hosts/networks
      -iR <num hosts>: Choose random targets
      --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
      --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PU/PV[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/-T/-sA/-sW/-sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/-F/-SX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/-sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,443-4567
  --exclude-ports <port ranges>: Exclude specified ports from scanning
  -F: Fast mode - Scan fewer ports
  -r: Scan ports sequentially - don't randomize
```

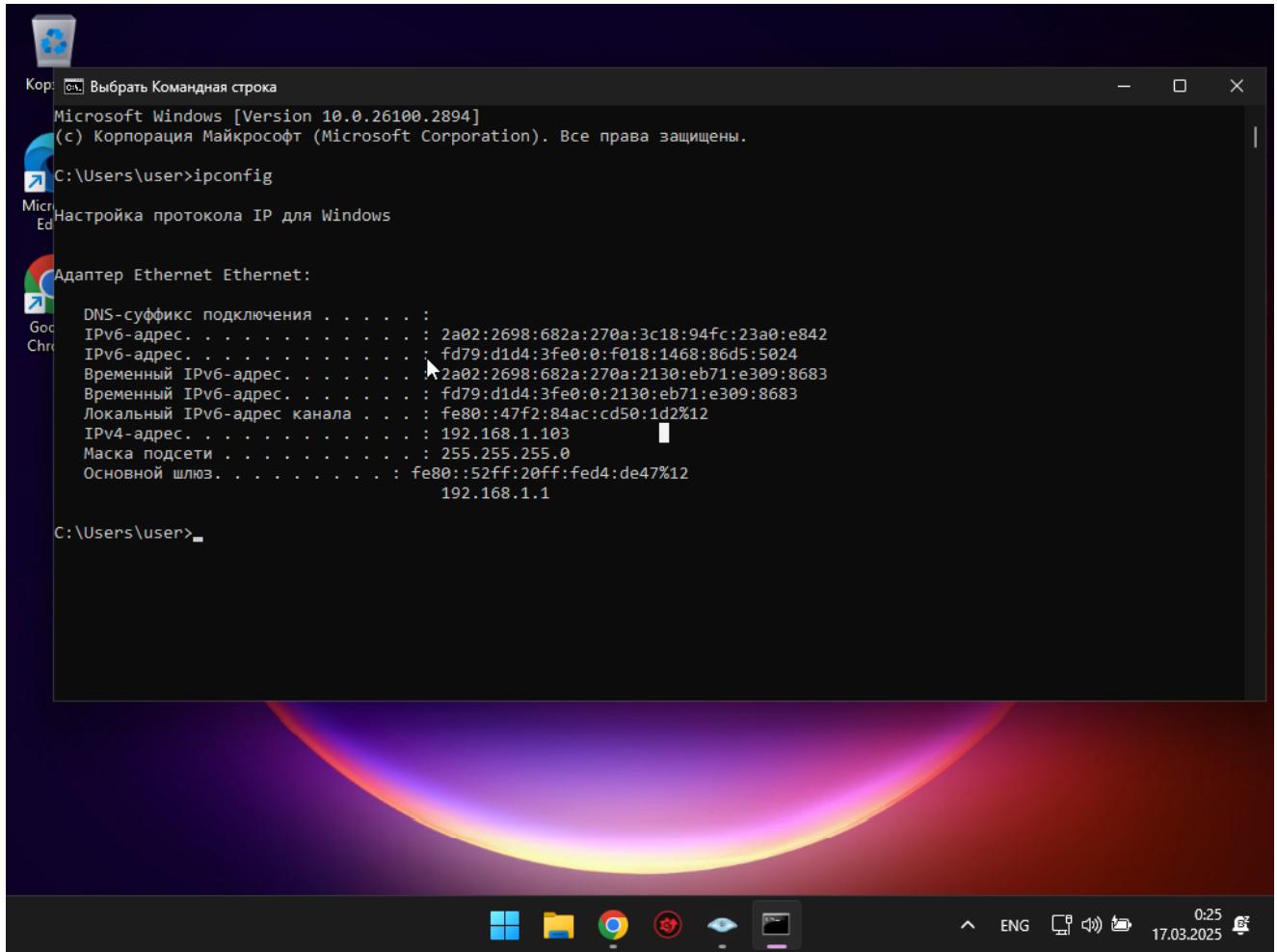
Шаг 2. Установите Nmap на Windows

Zenmap window showing the results of an Nmap scan. The target is set to 192.168.1.0/24. The command used is nmap -sn -PE -PP -PM 192.168.1.0/24. The Nmap Output tab is selected, displaying the following scan results:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-17 00:12 Азербайджанское время (зима)
Nmap scan report for 192.168.1.1
Host is up (0.0060s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.11s latency).
MAC Address: 84:25:19:34:30:6C (Samsung Electronics)
Nmap scan report for 192.168.1.43
Host is up (0.042s latency).
MAC Address: CC:4B:73:EF:E4:6A (Ampak Technology)
Nmap scan report for 192.168.1.61
Host is up (0.070s latency).
MAC Address: BE:94:CC:81:0A:D4 (Unknown)
Nmap scan report for 192.168.1.79
Host is up (0.050s latency).
MAC Address: F4:FE:FB:32:25:E6 (Samsung Electronics)
Nmap scan report for 192.168.1.78
Host is up (0.086s latency).
MAC Address: 3C:0E:30:42:18:15 (Apple)
Nmap scan report for 192.168.1.104
Host is up (0.097s latency).
MAC Address: F0:B0:40:59:A2:17 (Hunan FN-Link Technology Limited)
Nmap scan report for 192.168.1.113
Host is up (0.0020s latency).
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.130
Host is up (0.0060s latency).
MAC Address: 50:C2:E8:F5:66:21 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.103
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 15.94 seconds
```

Шаг 3. Узнайте IP-адрес на двух машинах

IP-адрес машины Windows - 192.168.1.103



```
Кор: Выбрать Командная строка
Microsoft Windows [Version 10.0.26100.2894]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\user>ipconfig

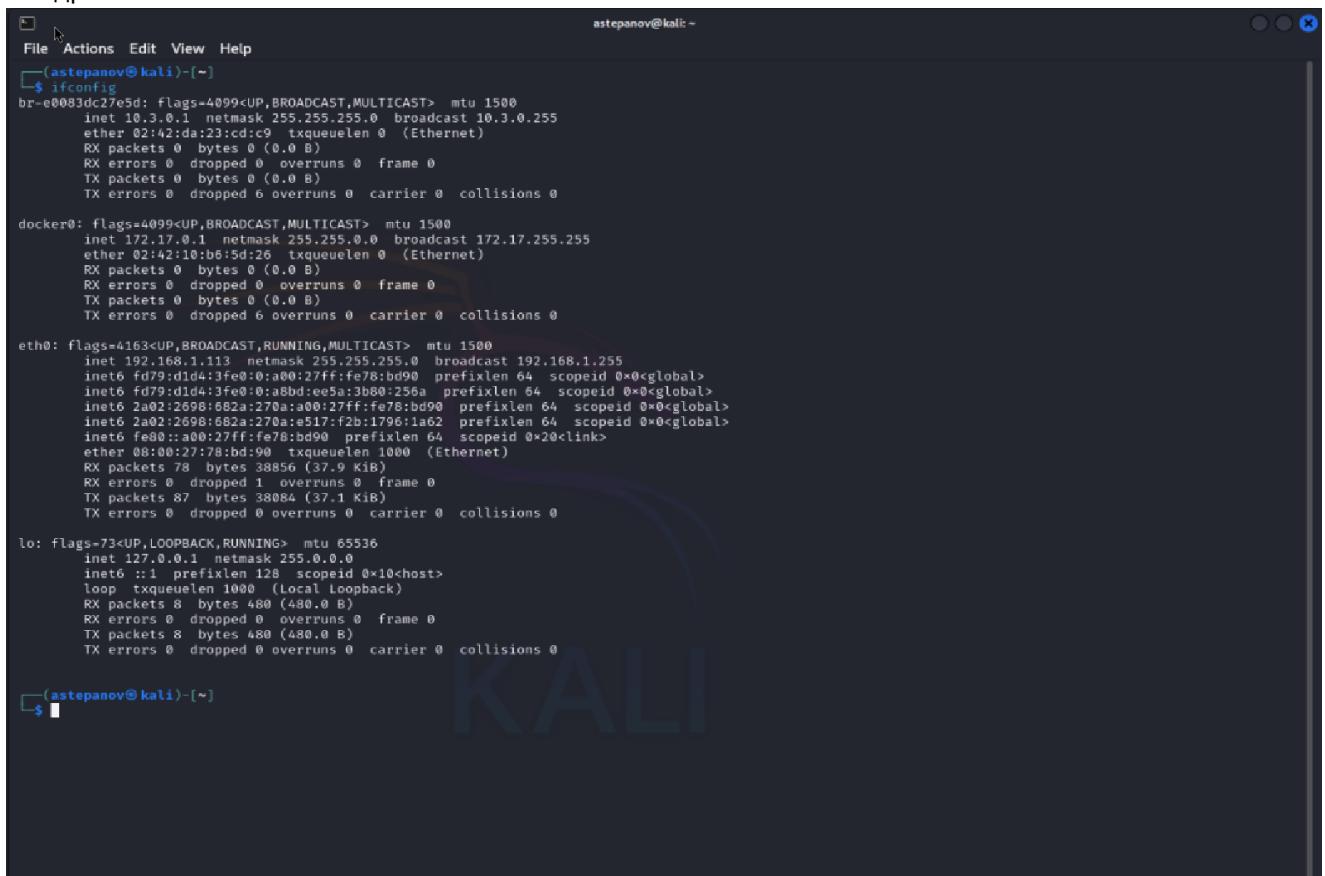
Мастер настройки протокола IP для Windows

Адаптер Ethernet Ethernet:

DNS-суффикс подключения . . . . . :
IPv6-адрес . . . . . : 2a02:2698:682a:270a:3c18:94fc:23a0:e842
IPv6-адрес . . . . . : fd79:d1d4:3fe0:0:f018:1468:86d5:5024
Временный IPv6-адрес . . . . . : 2a02:2698:682a:270a:2130:eb71:e309:8683
Временный IPv6-адрес . . . . . : fd79:d1d4:3fe0:0:2130:eb71:e309:8683
Локальный IPv6-адрес канала . . . . . : fe80::47f2:84ac:cd50:1d2%12
IPv4-адрес . . . . . : 192.168.1.103
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : fe80::52ff:20ff:fed4:de47%12
192.168.1.1

C:\Users\user>
```

IP-адрес машины Kali Linux - 192.168.1.113



```
astepanov㉿kali ~
File Actions Edit View Help
	astepanov㉿kali ~
$ ifconfig
br-e0083dc27e5d: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 10.3.0.1 netmask 255.255.255.0 broadcast 10.3.0.255
        ether 02:42:da:23:cd:c9 txqueuelen 0 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
        ether 02:42:10:b5:5d:26 txqueuelen 0 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.113 netmask 255.255.255.0 broadcast 192.168.1.255
        ether fd79:d1d4:3fe0:0:a0:27ff:fe78:bd90 txqueuelen 64 scopeid 0x0<global>
        inet6 fd79:d1d4:3fe0:0:a8bd:ee5a:3b80:256a prefixlen 64 scopeid 0x0<global>
        inet6 2a02:2698:682a:270a:a0:27ff:fe78:bd90 prefixlen 64 scopeid 0x0<global>
        inet6 2a02:2698:682a:270a:a517:f2b:1796:1a62 prefixlen 64 scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe78:bd90 prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:78:bd:90 txqueuelen 1000 (Ethernet)
        RX packets 78 bytes 38856 (37.9 KiB)
        RX errors 0 dropped 1 overruns 0 frame 0
        TX packets 87 bytes 38088 (37.1 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

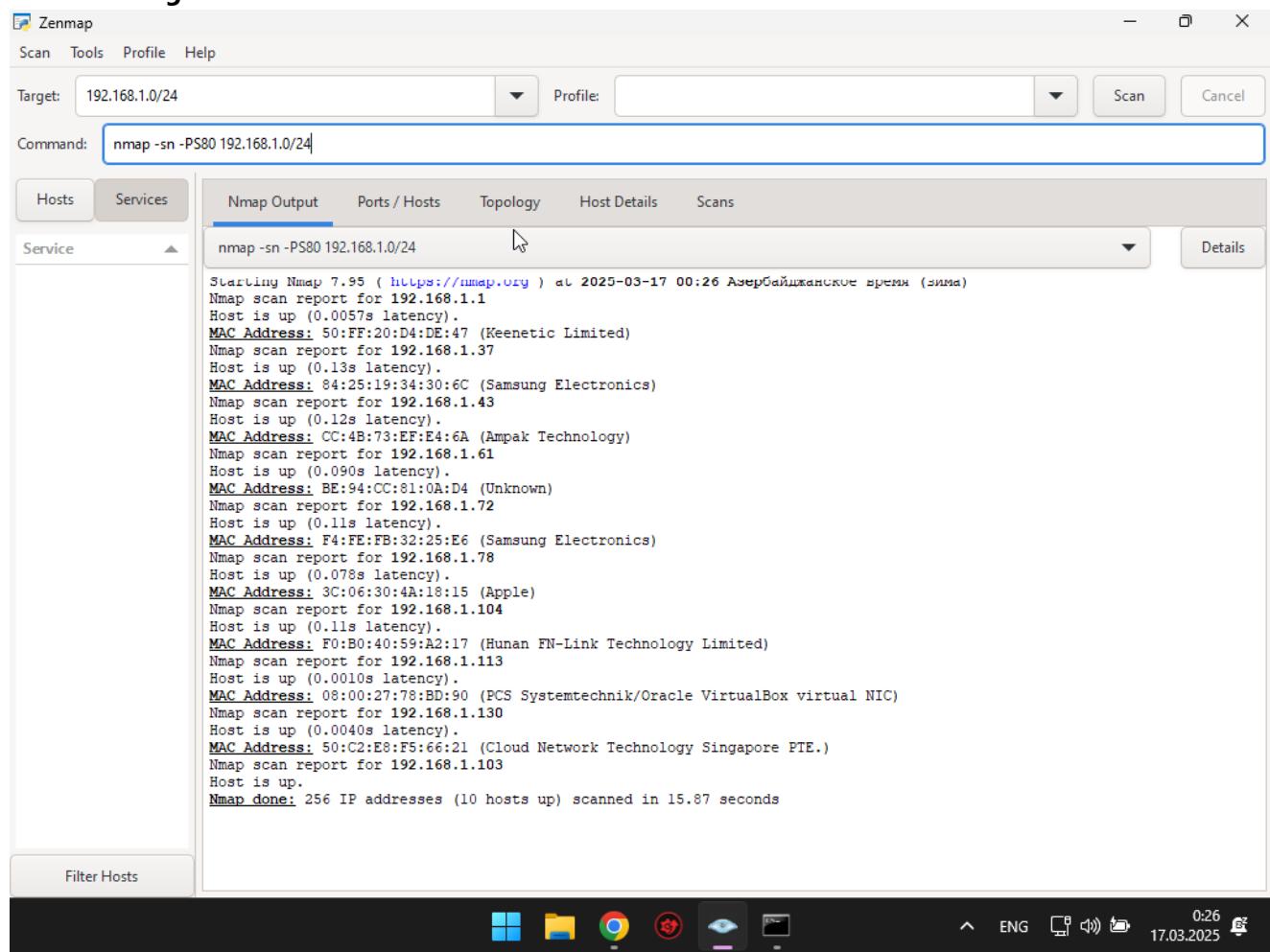
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
        RX packets 8 bytes 480 (480.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 8 bytes 480 (480.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(astepanov㉿kali)-[~]
```

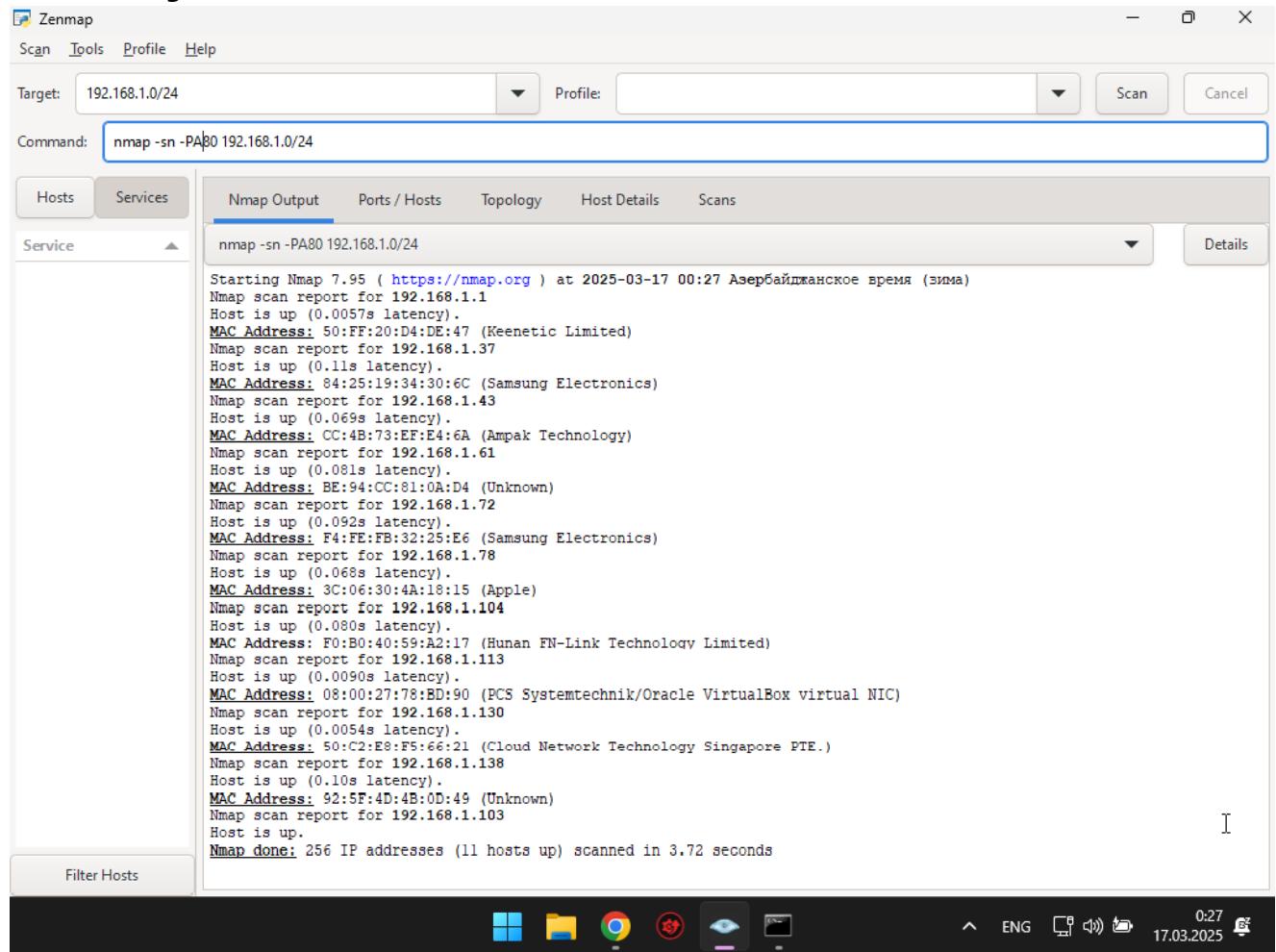
Шаг 4. Исследуем доступность сети

С машины Windows

TCP SYN Ping



TCP ACK Ping



UDP Ping

Zenmap interface showing the results of a UDP scan (nmap -sn -PU53) on the target 192.168.1.0/24. The Nmap Output tab displays the scan report, which lists 10 hosts found to be up with their MAC addresses and manufacturer information. The scan completed in 3.01 seconds.

Target: 192.168.1.0/24

Command: nmap -sn -PU53 192.168.1.0/24

Nmap Output

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-17 00:28 Азербайджанское время (зима)
Nmap scan report for 192.168.1.1
Host is up (0.0056s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.055s latency).
MAC Address: 84:25:19:34:30:6C (Samsung Electronics)
Nmap scan report for 192.168.1.43
Host is up (0.12s latency).
MAC Address: CC:4B:73:EE:E4:6A (Ampak Technology)
Nmap scan report for 192.168.1.61
Host is up (0.073s latency).
MAC Address: BE:94:CC:81:0A:D4 (Unknown)
Nmap scan report for 192.168.1.72
Host is up (0.089s latency).
MAC Address: F4:FE:FB:32:25:E6 (Samsung Electronics)
Nmap scan report for 192.168.1.78
Host is up (0.059s latency).
MAC Address: 3C:06:30:4A:18:15 (Apple)
Nmap scan report for 192.168.1.104
Host is up (0.086s latency).
MAC Address: F0:B0:40:59:A2:17 (Hunan FN-Link Technology Limited)
Nmap scan report for 192.168.1.113
Host is up (0.016s latency).
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.130
Host is up (0.0010s latency).
MAC Address: 50:C2:E5:F5:66:21 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.103
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 3.01 seconds
```

Filter Hosts

Scan Details

0:28 17.03.2025

ICMP Ping Types

Zenmap interface showing the results of an ICMP ping scan (nmap -sn -PE -PM -PP) of the subnet 192.168.1.0/24. The results are displayed in the Nmap Output tab.

Scan Command: nmap -sn -PE -PM -PP 192.168.1.0/24

Scanned Ports:

- 192.168.1.1 (Keenetic Limited)
- 192.168.1.37 (Samsung Electronics)
- 192.168.1.43 (Ampak Technology)
- 192.168.1.61 (Unknown)
- 192.168.1.72 (Apple)
- 192.168.1.78 (Samsung Electronics)
- 192.168.1.113 (Hunan FN-Link Technology Limited)
- 192.168.1.130 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
- 192.168.1.103 (Cloud Network Technology Singapore PTE.)

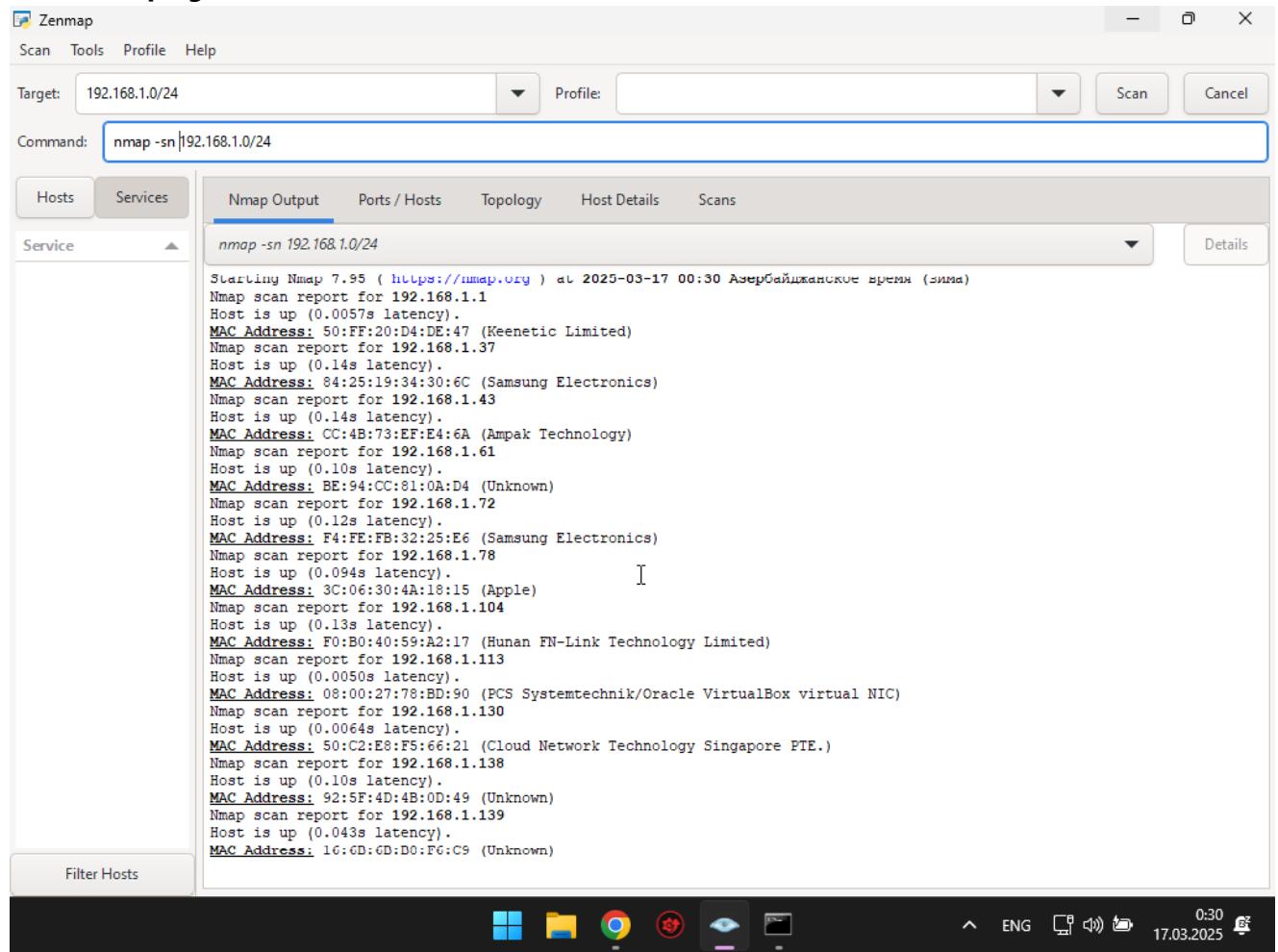
Summary: Starting Nmap 7.95 (https://nmap.org) at 2025-03-17 00:29 Азербайджанское время (Энгл.)
Nmap scan report for 192.168.1.1
Host is up (0.0070s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.051s latency).
MAC Address: 84:25:19:34:30:6C (Samsung Electronics)
Nmap scan report for 192.168.1.43
Host is up (0.040s latency).
MAC Address: CC:4B:73:EF:E4:6A (Ampak Technology)
Nmap scan report for 192.168.1.61
Host is up (0.073s latency).
MAC Address: BE:94:CC:81:0A:D4 (Unknown)
Nmap scan report for 192.168.1.72
Host is up (0.060s latency).
MAC Address: F4:FE:FB:32:25:E6 (Samsung Electronics)
Nmap scan report for 192.168.1.78
Host is up (0.12s latency).
MAC Address: 3C:06:30:4A:18:15 (Apple)
Nmap scan report for 192.168.1.104
Host is up (0.10s latency).
MAC Address: F0:B0:40:59:A2:17 (Hunan FN-Link Technology Limited)
Nmap scan report for 192.168.1.113
Host is up (0.0090s latency).
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.130
Host is up (0.0089s latency).
MAC Address: 50:C2:E5:F5:66:21 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.103
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 2.56 seconds

IP Protocol Ping

Zenmap interface showing the results of an Nmap scan. The target is set to 192.168.1.0/24. The command entered is nmap -sn -PO 192.168.1.0/24. The Nmap Output tab is selected, displaying the scan report. The report shows 10 hosts up from 256 scanned, with various MAC addresses and manufacturer information. The scan completed in 3.12 seconds.

Starting Nmap 7.95 (https://nmap.org) at 2025-03-17 00:29 Азербайджанское время (Baku)
Nmap scan report for 192.168.1.1
Host is up (0.0070s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.099s latency).
MAC Address: 84:25:19:34:30:6C (Samsung Electronics)
Nmap scan report for 192.168.1.43
Host is up (0.084s latency).
MAC Address: CC:4B:73:EF:E4:6A (Ampak Technology)
Nmap scan report for 192.168.1.61
Host is up (0.047s latency).
MAC Address: BE:94:CC:81:0A:D4 (Unknown)
Nmap scan report for 192.168.1.72
Host is up (0.14s latency).
MAC Address: F4:FE:FB:32:25:E6 (Samsung Electronics)
Nmap scan report for 192.168.1.78
Host is up (0.096s latency).
MAC Address: 3C:06:30:42:18:15 (Apple)
Nmap scan report for 192.168.1.104
Host is up (0.15s latency).
MAC Address: F0:B0:40:59:A2:17 (Hunan FN-Link Technology Limited)
Nmap scan report for 192.168.1.113
Host is up (0.0030s latency).
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.130
Host is up (0.0020s latency).
MAC Address: 50:C2:E8:F5:66:21 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.103
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 3.12 seconds

Обычный ping-скан



С машины Kali Linux

TCP SYN Ping

```
(astepanov㉿kali)-[~]
$ nmap -sn -PS80 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 16:31 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0038s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.13s latency).
MAC Address: 84:25:19:34:30:6C (Samsung Electronics)
Nmap scan report for 192.168.1.43
Host is up (0.15s latency).
MAC Address: CC:4B:73:EF:E4:6A (Ampak Technology)
Nmap scan report for 192.168.1.61
Host is up (0.10s latency).
MAC Address: BE:94:CC:81:0A:D4 (Unknown)
Nmap scan report for 192.168.1.72
Host is up (0.13s latency).
MAC Address: F4:FE:FB:32:25:E6 (Samsung Electronics)
Nmap scan report for 192.168.1.78
Host is up (0.095s latency).
MAC Address: 3C:06:30:4A:18:15 (Apple)
Nmap scan report for 192.168.1.103
Host is up (0.00055s latency).
MAC Address: 08:00:27:16:2A:56 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.104
Host is up (0.14s latency).
MAC Address: F0:B0:40:59:A2:17 (Hunan FN-Link Technology Limited)
Nmap scan report for 192.168.1.130
Host is up (0.00026s latency).
MAC Address: 50:C2:E8:F5:66:21 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.113
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 3.25 seconds

(astepanov㉿kali)-[~]
$
```

TCP ACK Ping

```
(astepanov㉿kali)-[~]
$ nmap -sn -PA80 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 16:33 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0036s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.15s latency).
MAC Address: 84:25:19:34:30:6C (Samsung Electronics)
Nmap scan report for 192.168.1.43
Host is up (0.13s latency).
MAC Address: CC:4B:73:EF:E4:6A (Ampak Technology)
Nmap scan report for 192.168.1.61
Host is up (0.11s latency).
MAC Address: BE:94:CC:81:0A:D4 (Unknown)
Nmap scan report for 192.168.1.78
Host is up (0.14s latency).
MAC Address: 3C:06:30:4A:18:15 (Apple)
Nmap scan report for 192.168.1.103
Host is up (0.00086s latency).
MAC Address: 08:00:27:16:2A:56 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.104
Host is up (0.094s latency).
MAC Address: F0:B0:40:59:A2:17 (Hunan FN-Link Technology Limited)
Nmap scan report for 192.168.1.130
Host is up (0.00022s latency).
MAC Address: 50:C2:E8:F5:66:21 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.138
Host is up (0.13s latency).
MAC Address: 92:5F:4D:4B:0D:49 (Unknown)
Nmap scan report for 192.168.1.113
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 18.71 seconds
```

UDP Ping

```
[astepanov㉿kali)-[~]
$ nmap -sn -PU53 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 16:34 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0038s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.12s latency).
MAC Address: 84:25:19:34:30:6C (Samsung Electronics)
Nmap scan report for 192.168.1.43
Host is up (0.17s latency).
MAC Address: CC:4B:73:EF:E4:6A (Ampak Technology)
Nmap scan report for 192.168.1.61
Host is up (0.11s latency).
MAC Address: BE:94:CC:81:0A:D4 (Unknown)
Nmap scan report for 192.168.1.72
Host is up (0.13s latency).
MAC Address: F4:FE:FB:32:25:E6 (Samsung Electronics)
Nmap scan report for 192.168.1.103
Host is up (0.00060s latency).
MAC Address: 08:00:27:16:2A:56 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.104
Host is up (0.11s latency).
MAC Address: F0:B0:40:59:A2:17 (Hunan FN-Link Technology Limited)
Nmap scan report for 192.168.1.130
Host is up (0.00019s latency).
MAC Address: 50:C2:E8:F5:66:21 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.113
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in 3.61 seconds
```

ICMP Ping Types

```
[astepanov㉿kali)-[~]
$ nmap -sn -PE -PP -PM 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 16:34 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0036s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.12s latency).
MAC Address: 84:25:19:34:30:6C (Samsung Electronics)
Nmap scan report for 192.168.1.43
Host is up (0.11s latency).
MAC Address: CC:4B:73:EF:E4:6A (Ampak Technology)
Nmap scan report for 192.168.1.61
Host is up (0.067s latency).
MAC Address: BE:94:CC:81:0A:D4 (Unknown)
Nmap scan report for 192.168.1.72
Host is up (0.15s latency).
MAC Address: F4:FE:FB:32:25:E6 (Samsung Electronics)
Nmap scan report for 192.168.1.178
Host is up (0.062s latency).
MAC Address: 3C:06:30:4A:18:15 (Apple)
Nmap scan report for 192.168.1.103
Host is up (0.0011s latency).
MAC Address: 08:00:27:16:2A:56 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.104
Host is up (0.087s latency).
MAC Address: F0:B0:40:59:A2:17 (Hunan FN-Link Technology Limited)
Nmap scan report for 192.168.1.130
Host is up (0.00028s latency).
MAC Address: 50:C2:E8:F5:66:21 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.139
Host is up (0.13s latency).
MAC Address: 16:6B:6B:B8:F6:C9 (Unknown)
Nmap scan report for 192.168.1.113
Host is up.
Nmap done: 256 IP addresses (11 hosts up) scanned in 4.88 seconds
```

IP Protocol Ping

```
[astepanov@kali)-[~]
$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 16:35 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0036s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.13s latency).
MAC Address: 84:25:19:34:30:6C (Samsung Electronics)
Nmap scan report for 192.168.1.43
Host is up (0.12s latency).
MAC Address: CC:4B:73:EF:E4:6A (Ampak Technology)
Nmap scan report for 192.168.1.61
Host is up (0.12s latency).
MAC Address: BE:94:CC:81:0A:D4 (Unknown)
Nmap scan report for 192.168.1.103
Host is up (0.00059s latency).
MAC Address: 08:00:27:16:2A:56 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.104
Host is up (0.10s latency).
MAC Address: F0:B0:40:59:A2:17 (Hunan FN-Link Technology Limited)
Nmap scan report for 192.168.1.130
Host is up (0.00014s latency).
MAC Address: 50:C2:E8:F5:66:21 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.113
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 18.03 seconds
```

Обычный ping-скан

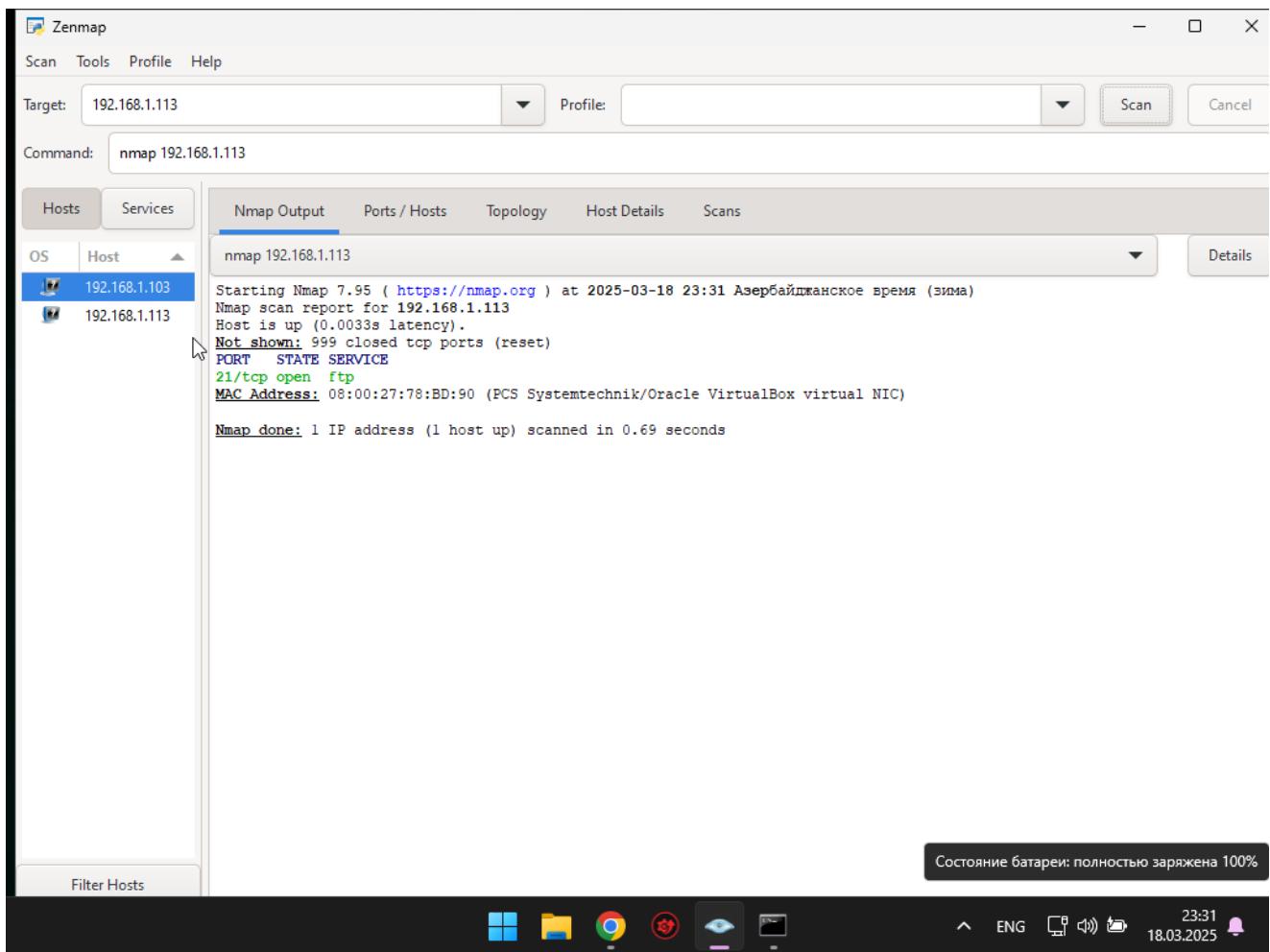
```
[astepanov@kali)-[~]
$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 16:39 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0035s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.16s latency).
MAC Address: 84:25:19:34:30:6C (Samsung Electronics)
Nmap scan report for 192.168.1.43
Host is up (0.15s latency).
MAC Address: CC:4B:73:EF:E4:6A (Ampak Technology)
Nmap scan report for 192.168.1.61
Host is up (0.11s latency).
MAC Address: BE:94:CC:81:0A:D4 (Unknown)
Nmap scan report for 192.168.1.72
Host is up (0.14s latency).
MAC Address: F4:FE:FB:32:25:E6 (Samsung Electronics)
Nmap scan report for 192.168.1.78
Host is up (0.11s latency).
MAC Address: 3C:06:30:4A:18:15 (Apple)
Nmap scan report for 192.168.1.103
Host is up (0.00062s latency).
MAC Address: 08:00:27:16:2A:56 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.104
Host is up (0.13s latency).
MAC Address: F0:B0:40:59:A2:17 (Hunan FN-Link Technology Limited)
Nmap scan report for 192.168.1.130
Host is up (0.00031s latency).
MAC Address: 50:C2:E8:F5:66:21 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.113
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 11.55 seconds
```

Таблица сравнения результатов

Вид сканирования	Описание	Найденные хосты (пример)	Оценка скорости работы
TCP SYN Ping	Отправляет SYN на порт (обычно 80), ждет SYN/ACK	Определяет хосты с открытым портом 80	Средняя скорость, зависит от количества открытых портов
TCP ACK Ping	Отправляет ACK, ждет RST	Полезно для обхода фильтров, определяет активные хосты за брандмауэрами	Средняя, но может быть быстрее, чем SYN Ping, в некоторых случаях
UDP Ping	Отправляет UDP-пакет (обычно 53), ждет ICMP Port Unreachable	Хорошо работает, если ICMP не фильтруется	Медленнее, чем TCP, из-за необходимости ожидания ICMP
ICMP Ping Types	Использует ICMP Echo Request (-PE), Timestamp Request (-PP), Address Mask Request (-PM)	Выявляет большинство активных хостов	Быстрое выполнение, так как работает с базовыми ICMP-запросами
IP Protocol Ping	Использует нестандартные IP-протоколы (GRE, ESP, AH)	Полезно против фильтрации ICMP и TCP	Медленное выполнение, так как использует нестандартные протоколы
Обычный -sn	Минимальное обнаружение хостов без сканирования портов	Зависит от политики сети	Очень быстрое, так как не включает портовое сканирование

Шаг 5. Просканируйте каждую машину с другой с помощью команды

Сканирование с Windows



Видим, что на хосте Kali открыт 21-ый порт, порт управляющего соединения FTP, который был открыт в рамках предудыщей ЛР

Сканирование с Kali Linux

На Windows-хосте, согласно сканирования с Kali-хоста, открытые порты отсутствуют

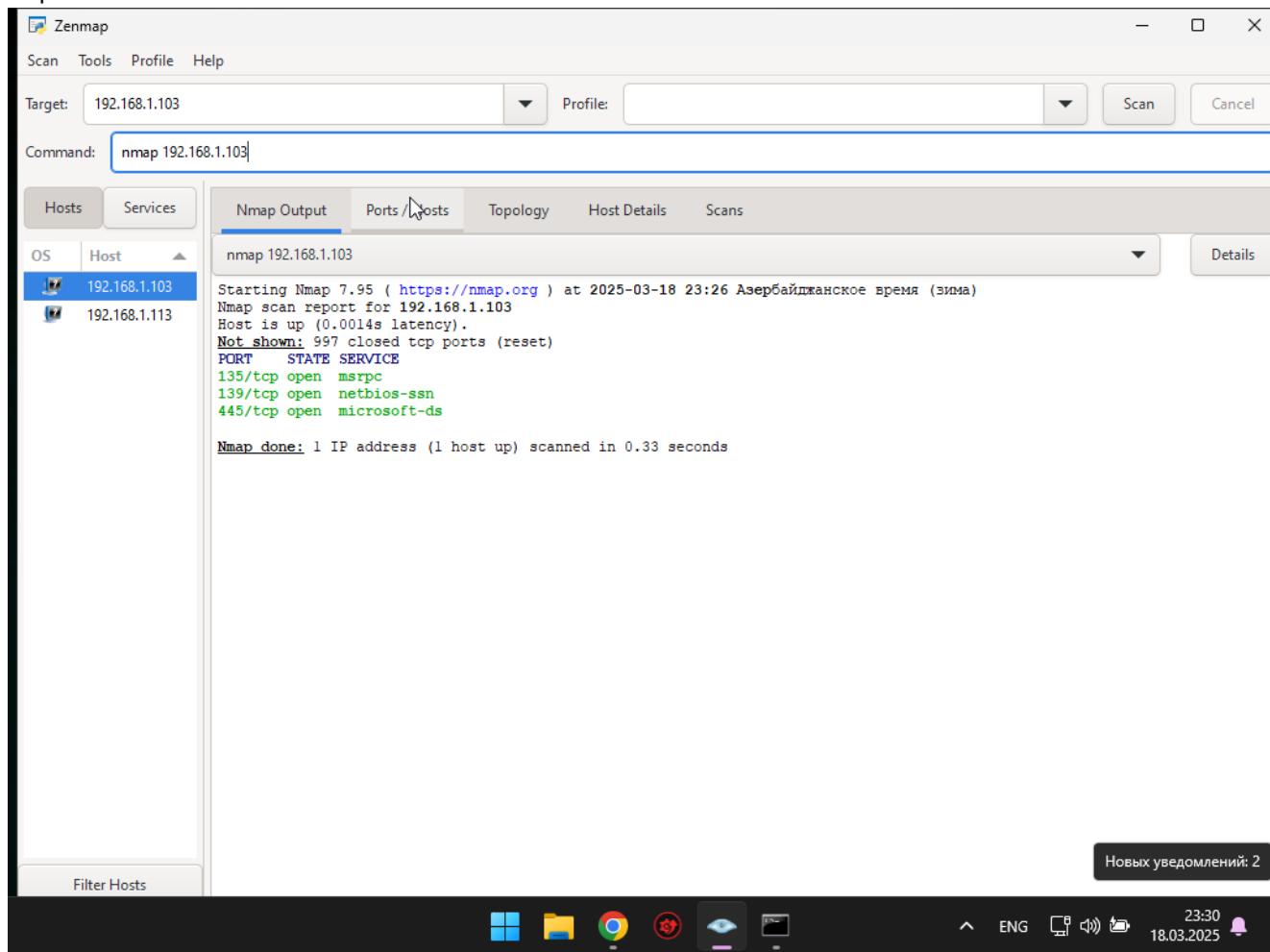
```
File Actions Edit View Help
Trash
(astepanov㉿kali)-[~]
$ nmap 192.168.1.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-18 15:23 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00066s latency).
All 1000 scanned ports on 192.168.1.103 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:16:2A:56 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 38.40 seconds

(astepanov㉿kali)-[~]
$
```

The terminal window shows the user's session and the command nmap 192.168.1.103. The output indicates that all 1000 ports are in an ignored state (filtered), and no response was received from the host. The MAC address of the host is listed as 08:00:27:16:2A:56.

Хотя если Windows-хост будет сканировать сам себя, то результат покажет наличие открытых tcp-портов:



Шаг 6. Выберите какой-нибудь порт, полученный в пункте 4 (видимо речь про п.5, так что берем 21-ый), и просканируйте его с помощью методов TCP SYN Scan, TCP Connect Scan, UDP Scan, TCP FIN Scan, TCP NULL Scan, TCP Xmas Scan и TCP ACK Scan. Сделайте скриншот каждого результата.

TCP SYN Scan

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113

Profile:

Command: nmap -sS -p 21 192.168.1.113

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

Service

ftp
http
microsoft-ds
msrpc
netbios-ssn

nmap -sS -p 21 192.168.1.113

Starting Nmap 7.95 (https://nmap.org) at 2025-03-19 00:06 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.001s latency).

PORT	STATE	SERVICE
21/tcp	open	ftp

MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.68 seconds

Filter Hosts

0:06 19.03.2025

Порт открыт

TCP Connect Scan

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113 Profile: Scan Cancel

Command: nmap -sT -p 21 192.168.1.113

Hosts Services

Service ▾

ftp
http
microsoft-ds
msrpc
netbios-ssn

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sT -p 21 192.168.1.113

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 00:07 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.001s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

Filter Hosts

0:07 19.03.2025

Порт открыт

UDP Scan

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113 Profile: Scan Cancel

Command: nmap -sU -p 21 192.168.1.113

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

Service ▲

ftp
http
microsoft-ds
msrpc
netbios-ssn

nmap -sU -p 21 192.168.1.113

Starting Nmap 7.95 (https://nmap.org) at 2025-03-19 00:07 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.0030s latency).

PORT STATE SERVICE
21/udp closed ftp
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

Filter Hosts

0:07 19.03.2025

Порт закрыт. Видимо, потому что это не UDP порт

TCP FIN Scan

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113 Profile: Scan Cancel

Command: nmap -sF -p 21 192.168.1.113

Hosts Services

Service ▾

ftp
http
microsoft-ds
msrpc
netbios-ssn

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sF -p 21 192.168.1.113

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 00:08 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.0010s latency).

PORT      STATE      SERVICE
21/tcp    open|filtered  ftp
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

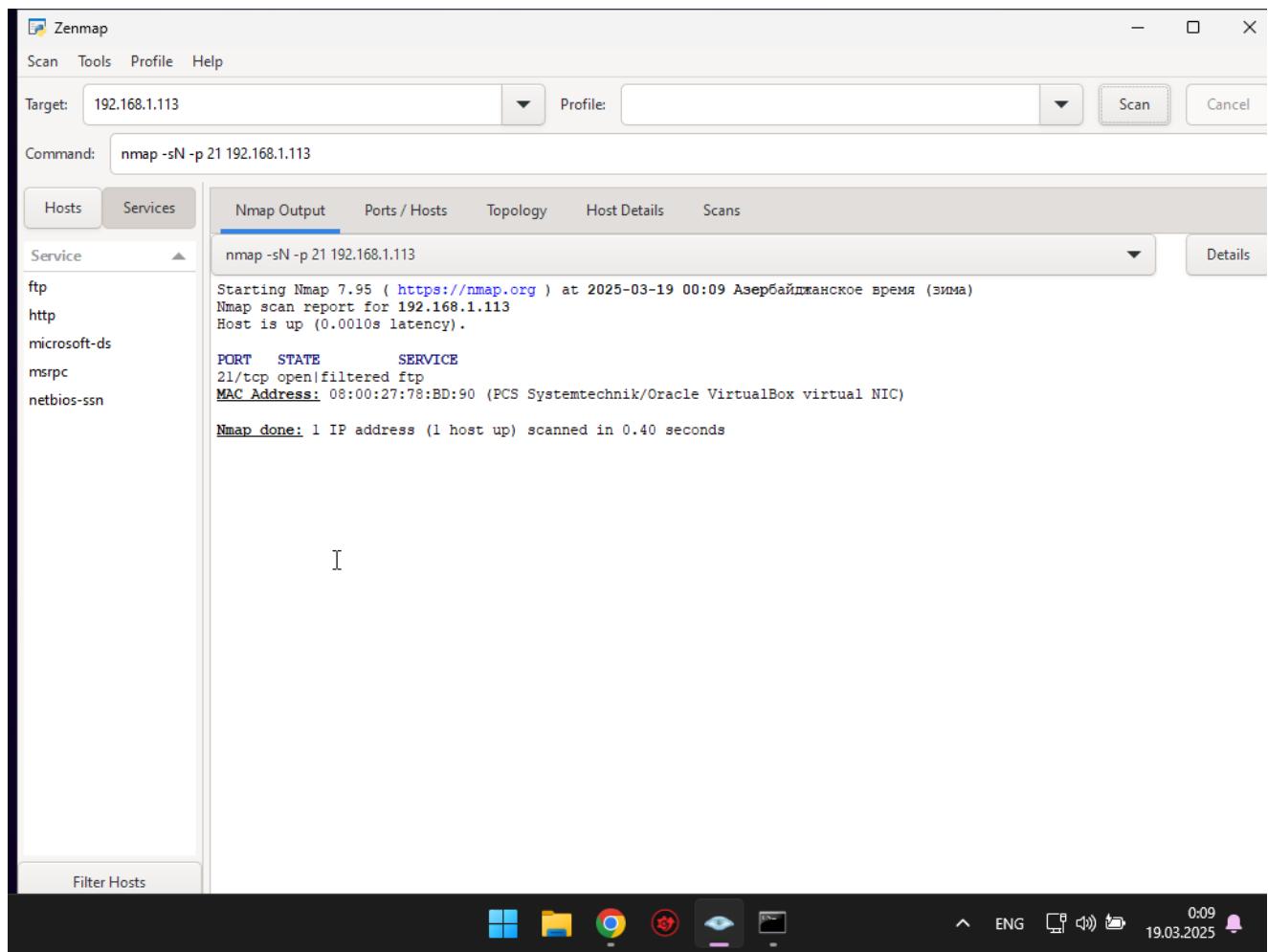
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

Filter Hosts

0:08 19.03.2025

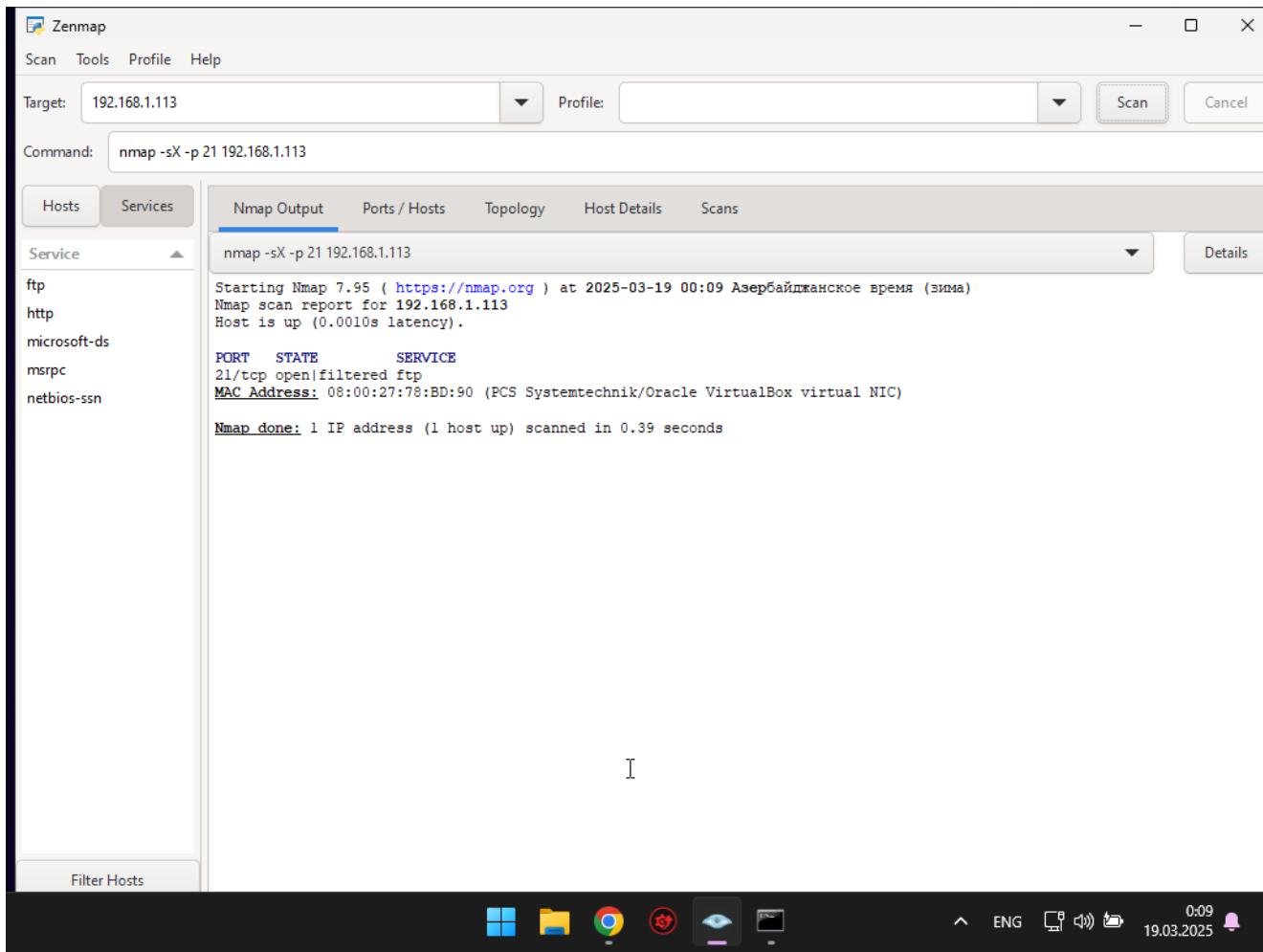
Порт открыт и не отвечает на нестандартные TCP-пакеты.

TCP NULL Scan



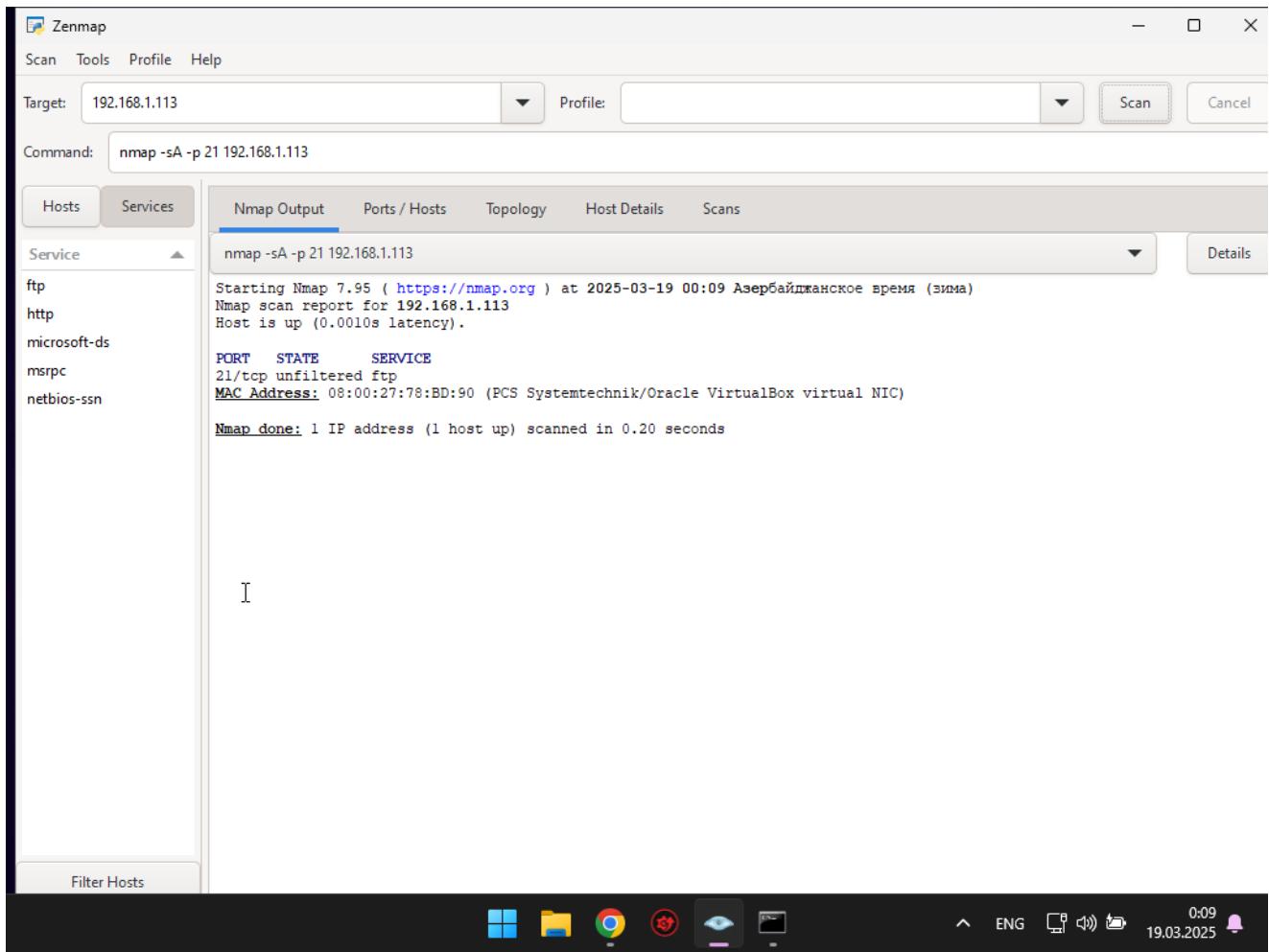
Порт открыт и не отвечает на нестандартные TCP-пакеты.

TCP Xmas Scan



Порт открыт и не отвечает на нестандартные TCP-пакеты.

TCP ACK Scan



ACK-пакеты не могут определить, открыт ли порт. Они только говорят, что он не фильтруется.

Шаг 7. На машину с Ubuntu установите веб-сервер Apache2

```
(asstepanov㉿kali)-[~]
$ sudo apt install apache2
apache2 is already the newest version (2.4.63-1).
apache2 set to manually installed.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1499
(asstepanov㉿kali)-[~]
```

Шаг 8. Настройка и запуск веб-сервера Apache2

Прописываем слушать 5000 порт в конфиге



```
GNU nano 3.2                               /etc/apache2/ports.conf *  
# If you just change the port or add more ports here, you will likely also  
# have to change the VirtualHost statement in  
# /etc/apache2/sites-enabled/000-default.conf  
  
Listen 5000  
<IfModule ssl_module>  
    Listen 443  
</IfModule>  
  
<IfModule mod_gnutls.c>  
    Listen 443  
</IfModule>  
  
[...]
```

File Actions Edit View Help

Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark To Bracket Copy Where Was Previous Next Back Forward Prev Word Next Word Home End

Перезапускаем сервер для того, чтобы подхватился конфиг

```
(astepanov㉿kali)-[~]
└─$ sudo apt install apache2
apache2 is already the newest version (2.4.63-1).
apache2 set to manually installed.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1499

(astepanov㉿kali)-[~]
└─$ sudo nano /etc/apache2/ports.conf

(astepanov㉿kali)-[~]
└─$ sudo systemctl restart apache2

(astepanov㉿kali)-[~]
└─$ sudo systemctl status apache2.service
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Tue 2025-03-18 14:03:26 EDT; 13s ago
   Invocation: 8888cf957a2483cb4c27a8eb10e0f0
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 25513 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 25537 (apache2)
   Tasks: 6 (limit: 4555)
     Memory: 20.2M (peak: 21M)
        CPU: 3.44ms
      CGroup: /system.slice/apache2.service
          ├─25537 /usr/sbin/apache2 -k start
          ├─25540 /usr/sbin/apache2 -k start
          ├─25541 /usr/sbin/apache2 -k start
          ├─25542 /usr/sbin/apache2 -k start
          ├─25543 /usr/sbin/apache2 -k start
          ├─25544 /usr/sbin/apache2 -k start

Mar 18 14:03:25 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Mar 18 14:03:26 kali apachectl[25536]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Mar 18 14:03:26 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

(astepanov㉿kali)-[~]
└─$ sudo systemctl enable apache2.service
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → '/usr/lib/systemd/system/apache2.service'.

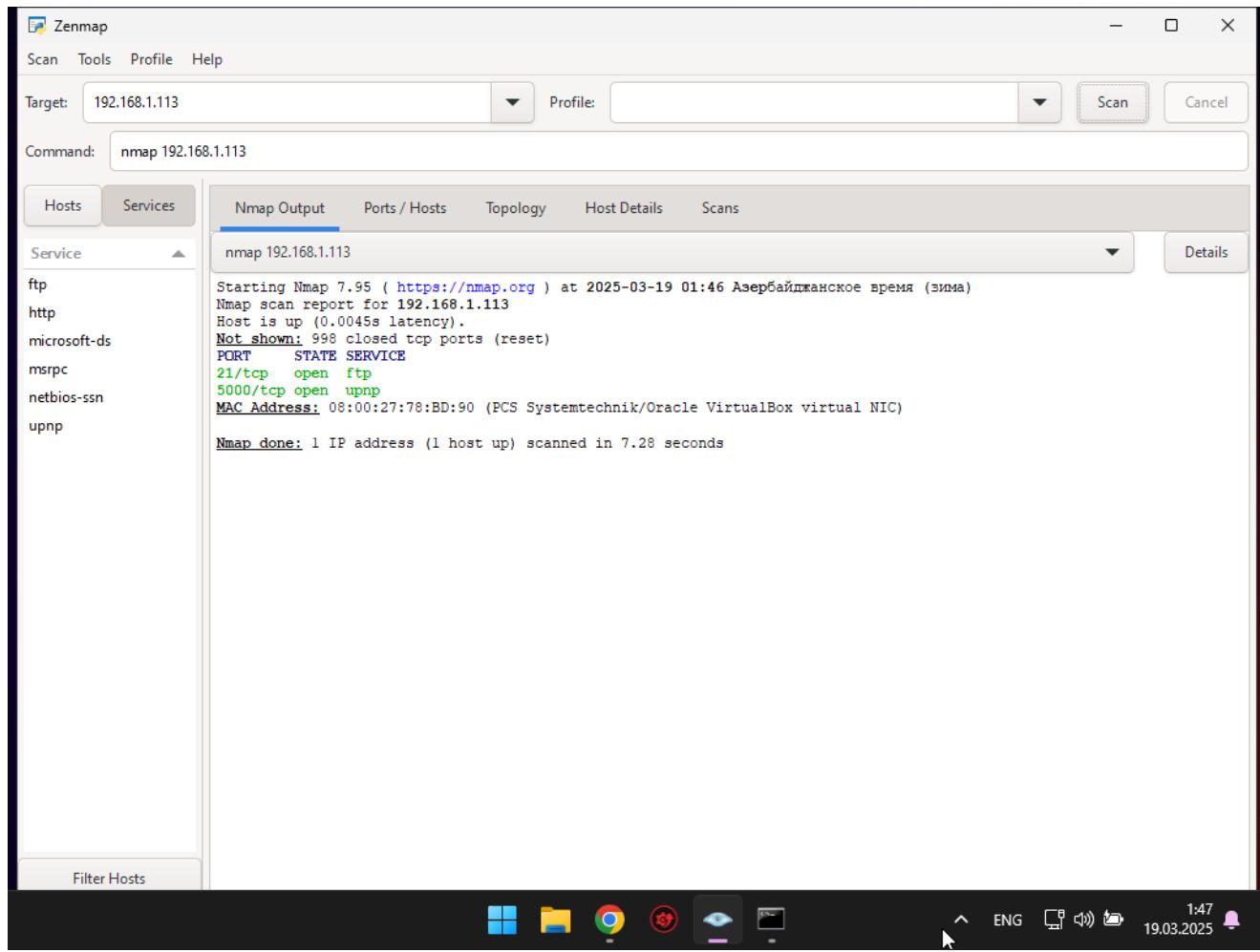
(astepanov㉿kali)-[~]
└─$ sudo systemctl status apache2.service
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: disabled)
     Active: active (running) since Tue 2025-03-18 14:03:26 EDT; 32s ago
   Invocation: 8888cf957a2483cb4c27a8eb10e0f0
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 25537 (apache2)
   Tasks: 6 (limit: 4555)
     Memory: 20.2M (peak: 21M)
        CPU: 3.46ms
      CGroup: /system.slice/apache2.service
          ├─25537 /usr/sbin/apache2 -k start
          ├─25540 /usr/sbin/apache2 -k start
          ├─25541 /usr/sbin/apache2 -k start
          ├─25542 /usr/sbin/apache2 -k start
          ├─25543 /usr/sbin/apache2 -k start
          ├─25544 /usr/sbin/apache2 -k start

Mar 18 14:03:25 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Mar 18 14:03:26 kali apachectl[25536]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Mar 18 14:03:26 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

(astepanov㉿kali)-[~]
└─$
```

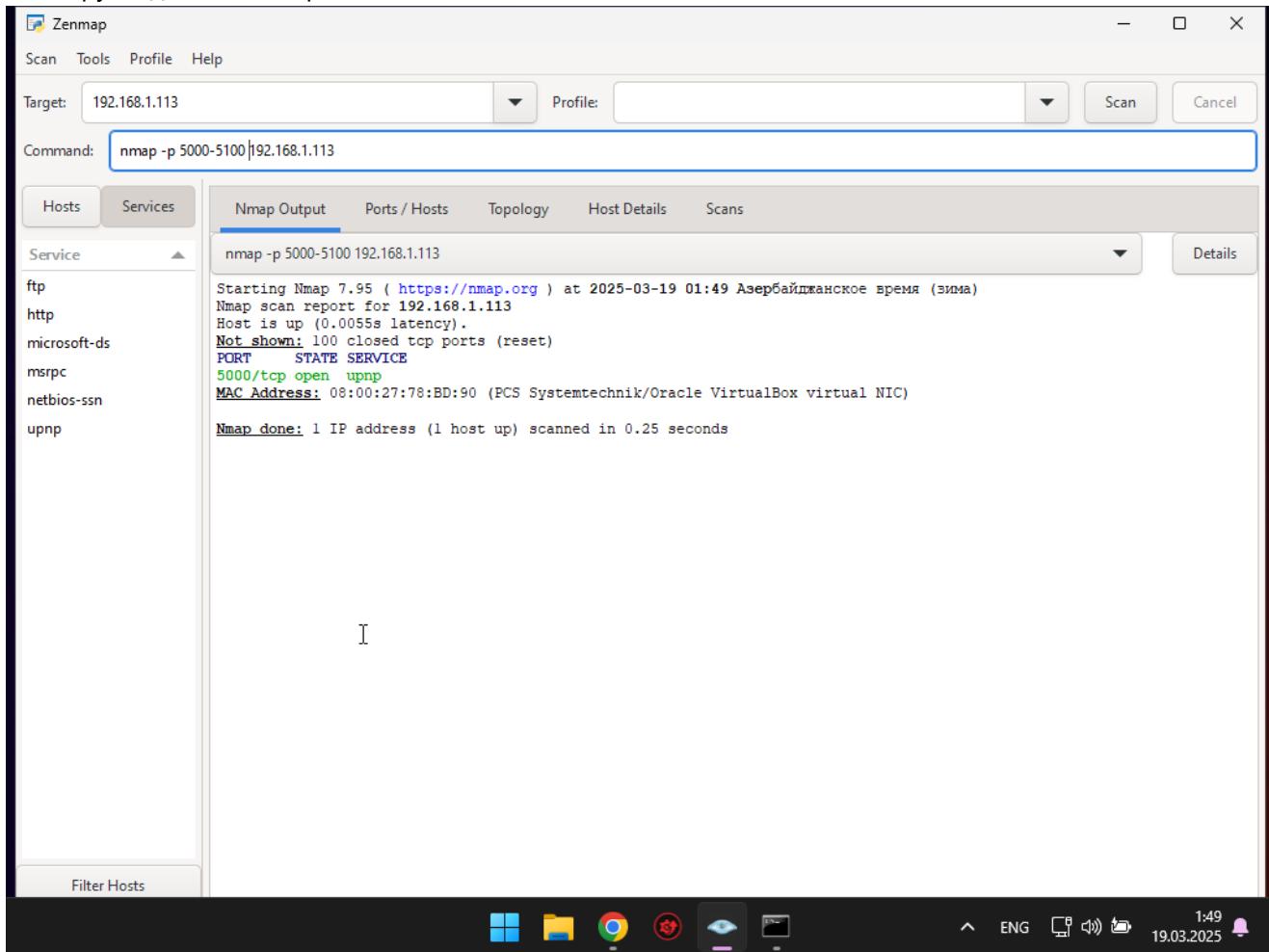
Шаг 9. С Windows повторите команду из пункта 4 (видимо речь про п.5). Появился ли ранее указанный порт?

После того, как на Kali был поднят Apache веб-сервер, видим что 5000-ый порт появился в результатах сканирования...



Просканируйте диапазон, в который входит порт, указанный в пункте 7 (тут путаница с пунктами, они не соответствуют пунктам из задания, поэтому остается только догадываться, что имелось ввиду, видимо речь снова про 5000-ый порт)

Сканируем диапазон портов 5000-5100



В общем-то, результат довольно очевидный – видим открытый 5000-й порт

Проверьте на этом порту методы сканирования из пункта 5 (видимо речь про п. 6).

TCP SYN Scan

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113 Profile: Scan Cancel

Command: nmap -sS -p 5000-5100 192.168.1.113

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

Service ▲

ftp
http
microsoft-ds
msrpc
netbios-ssn
upnp

nmap -sS -p 5000-5100 192.168.1.113

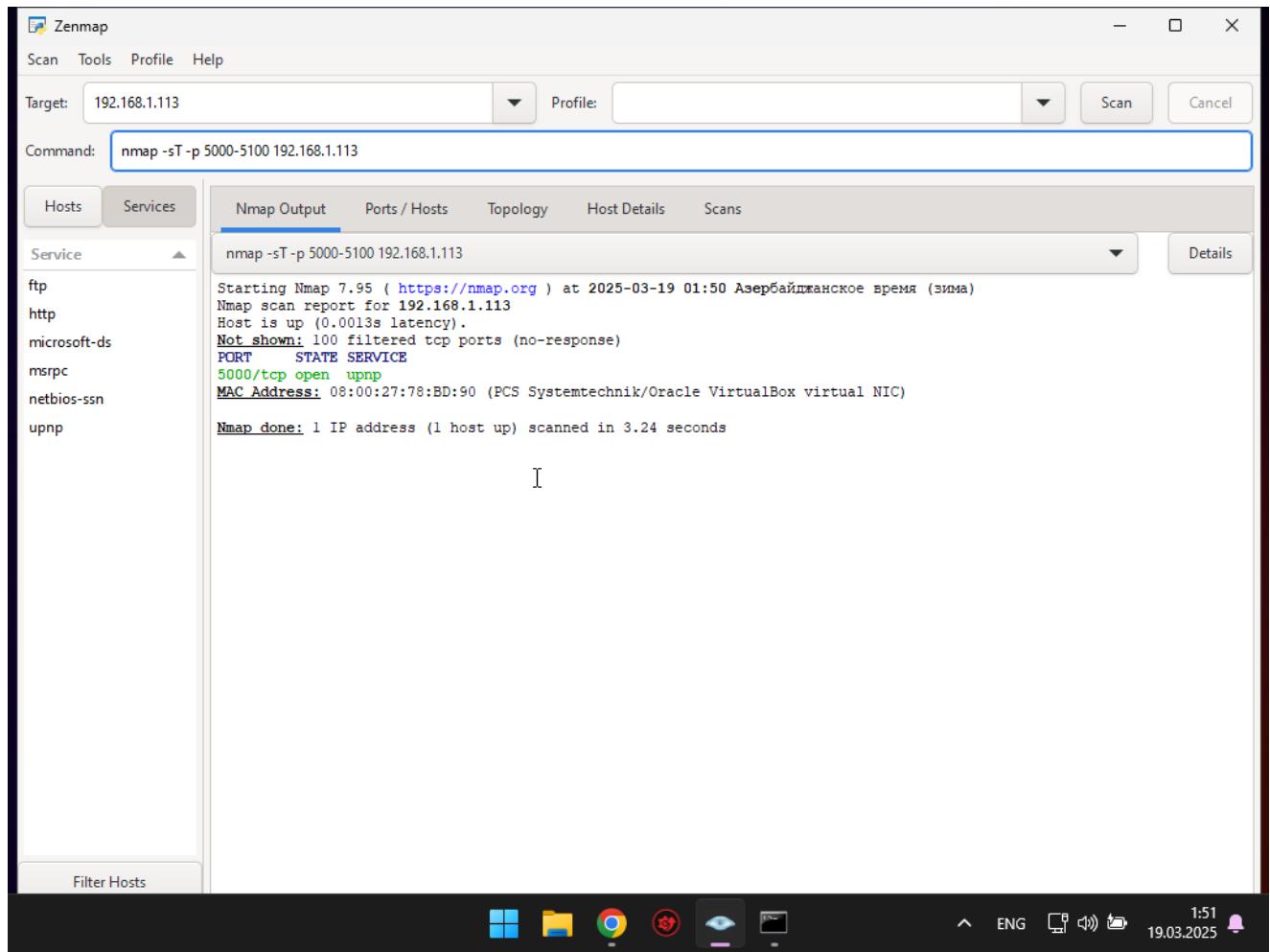
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 01:50 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.0040s latency).
Not shown: 100 closed tcp ports (reset)
PORT      STATE SERVICE
5000/tcp   open  upnp
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

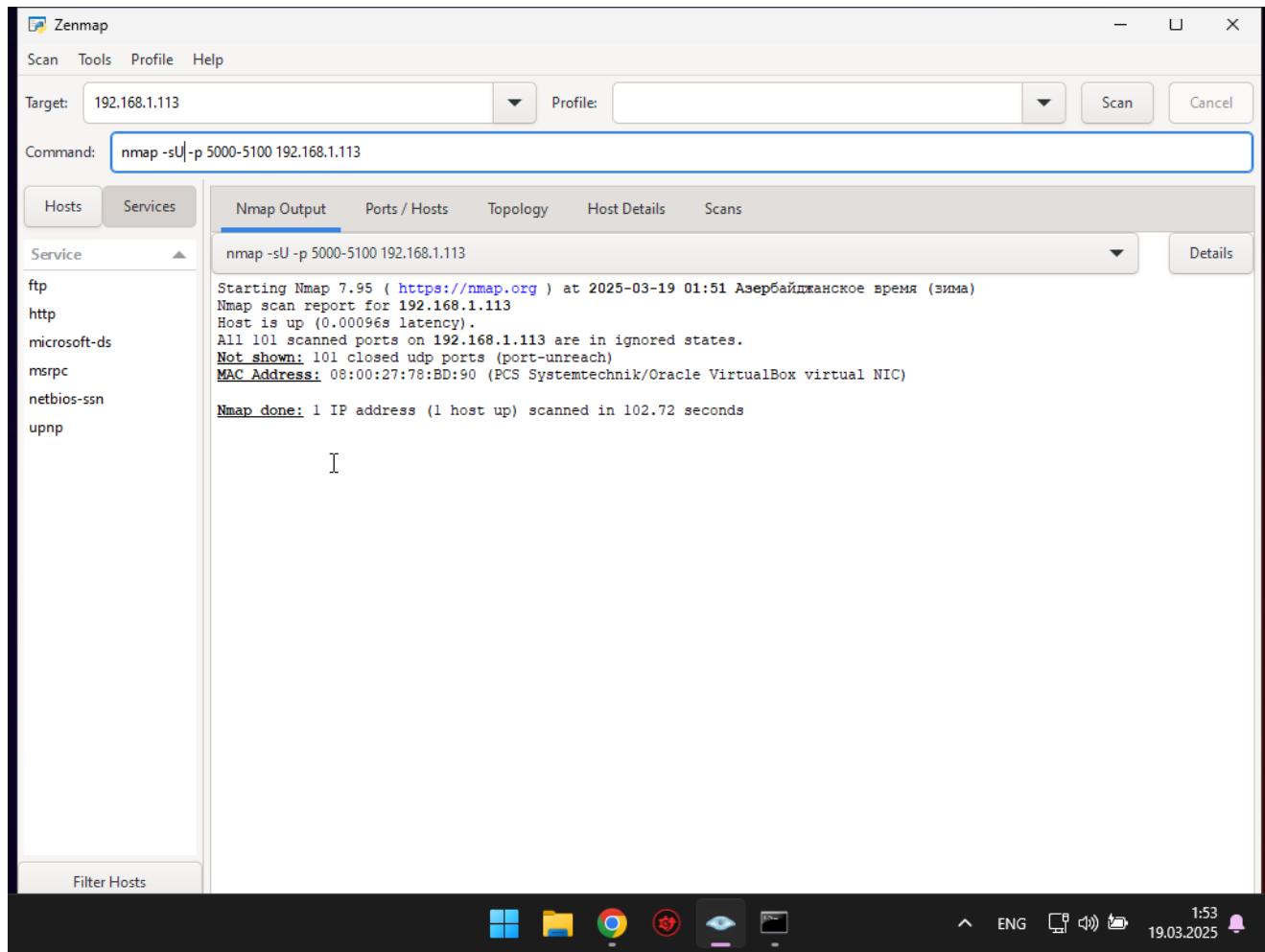
Filter Hosts

1:50 19.03.2025

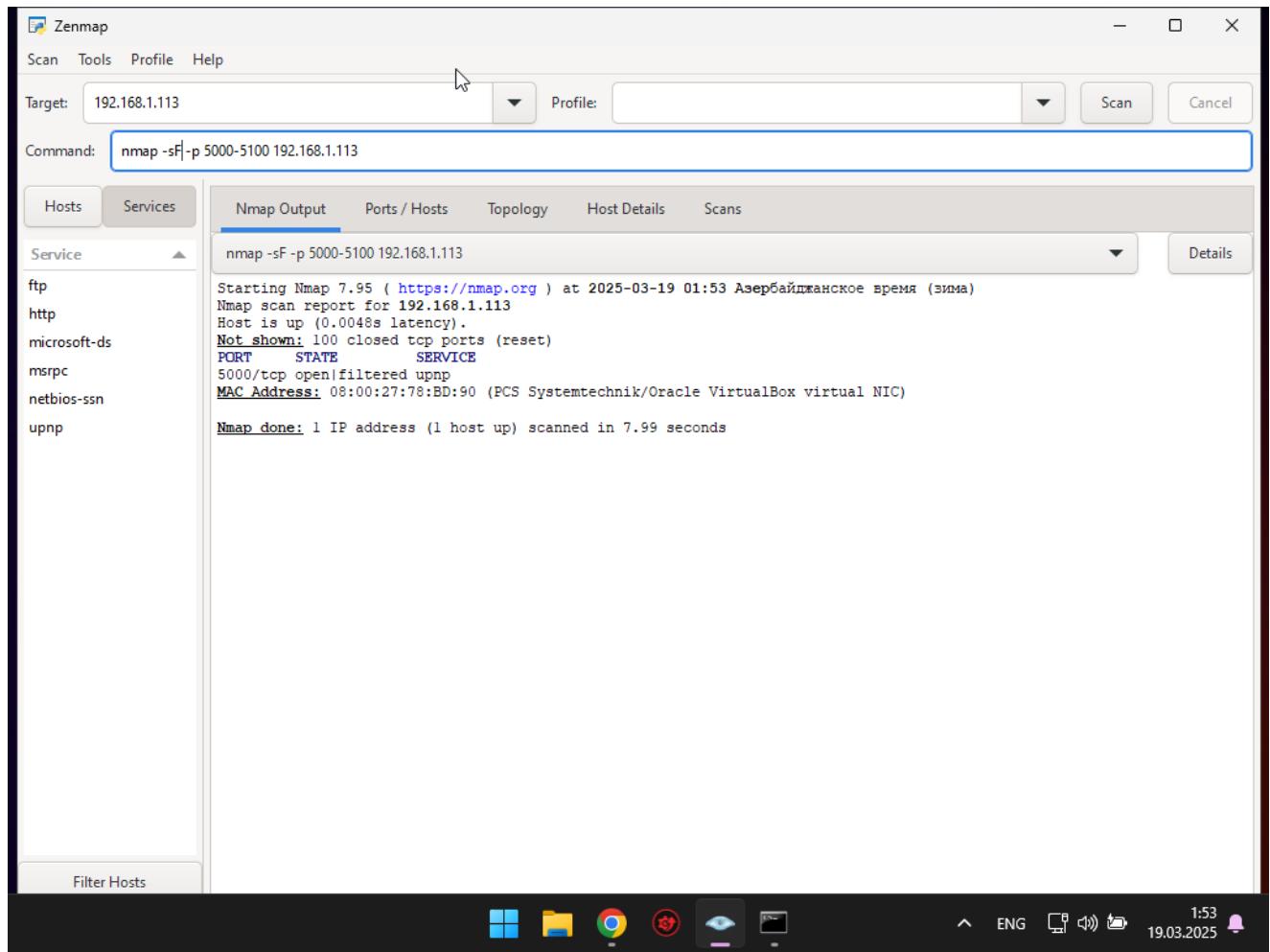
TCP Connect Scan



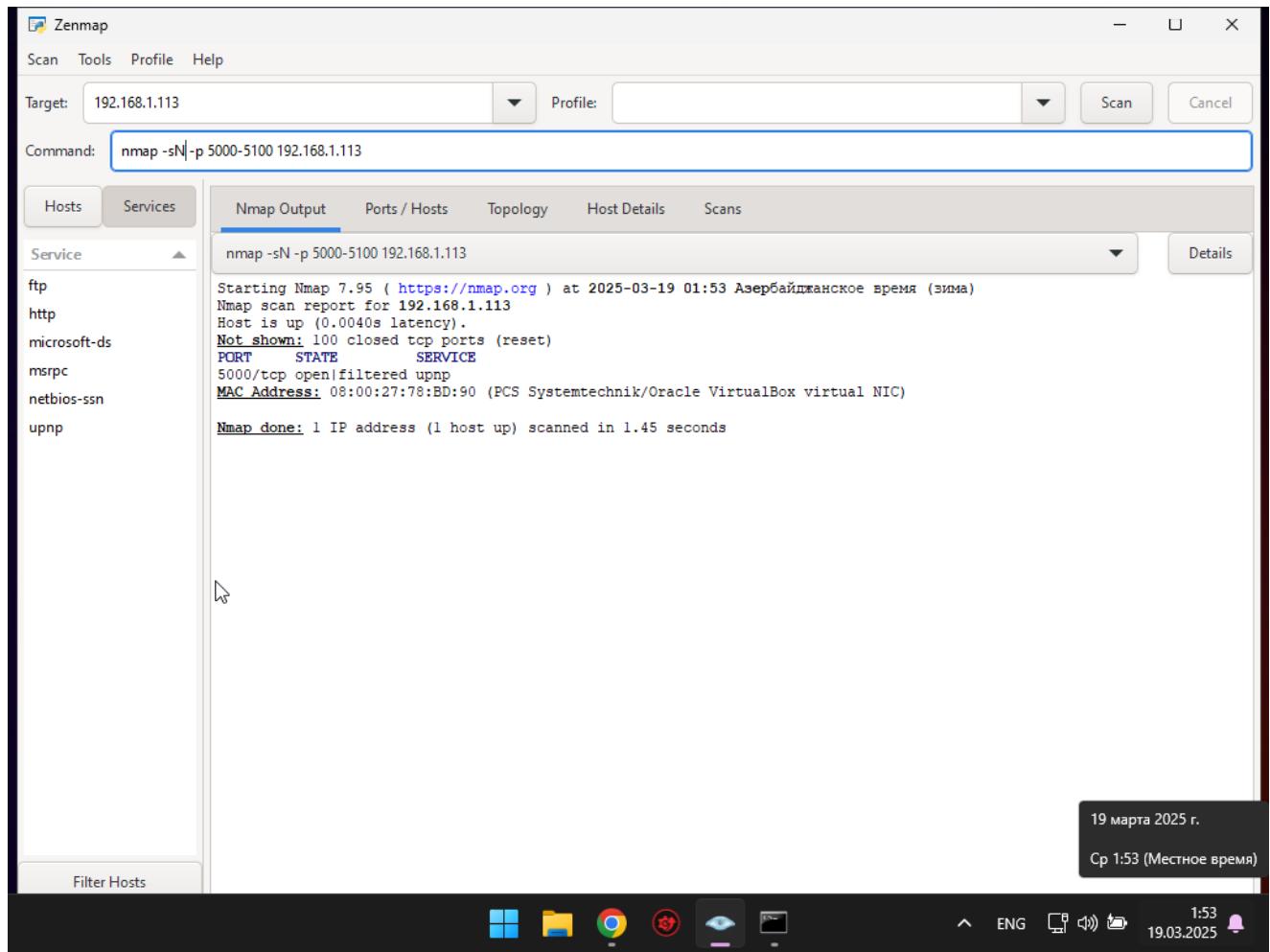
UDP Scan



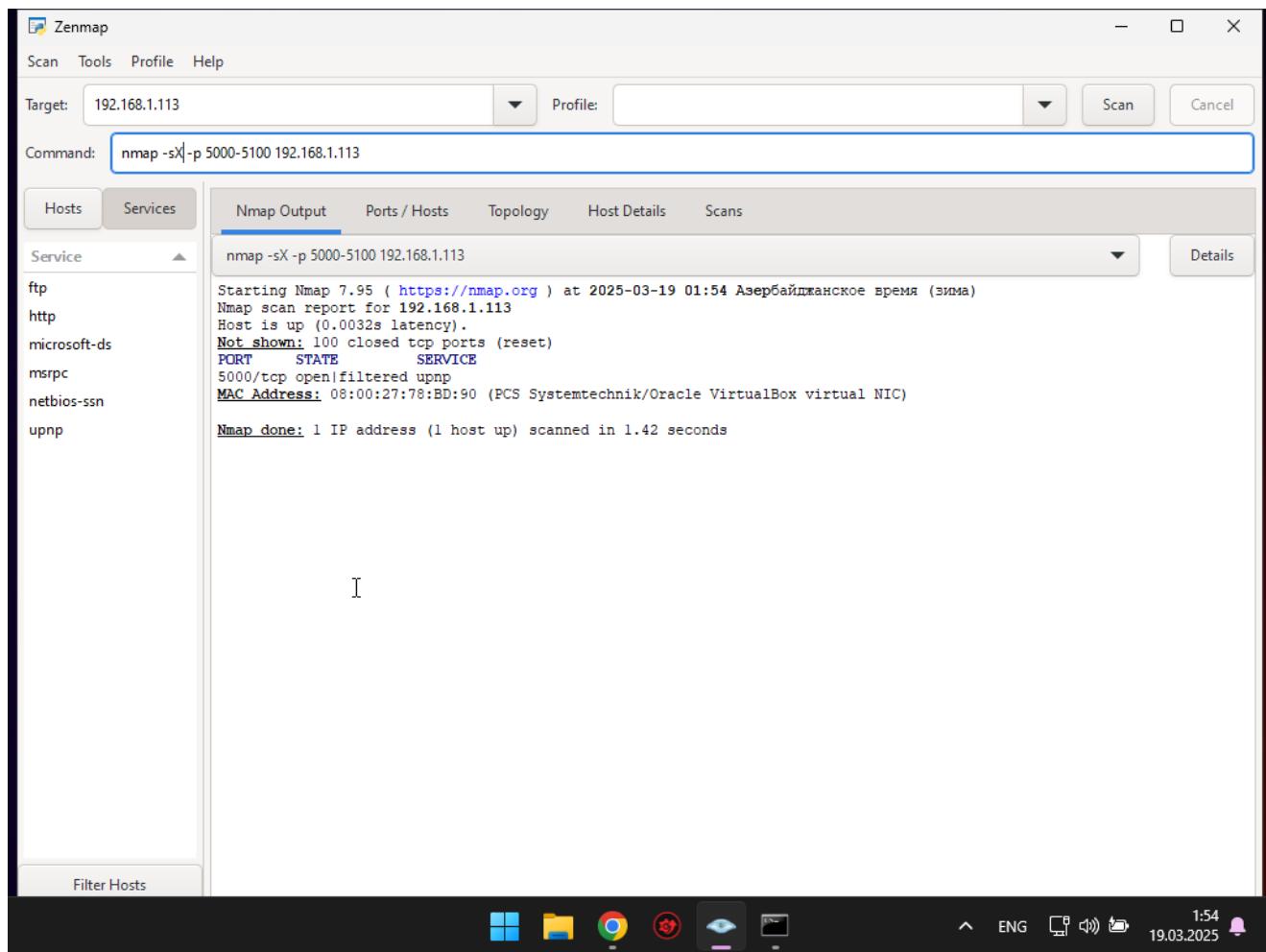
TCP FIN Scan



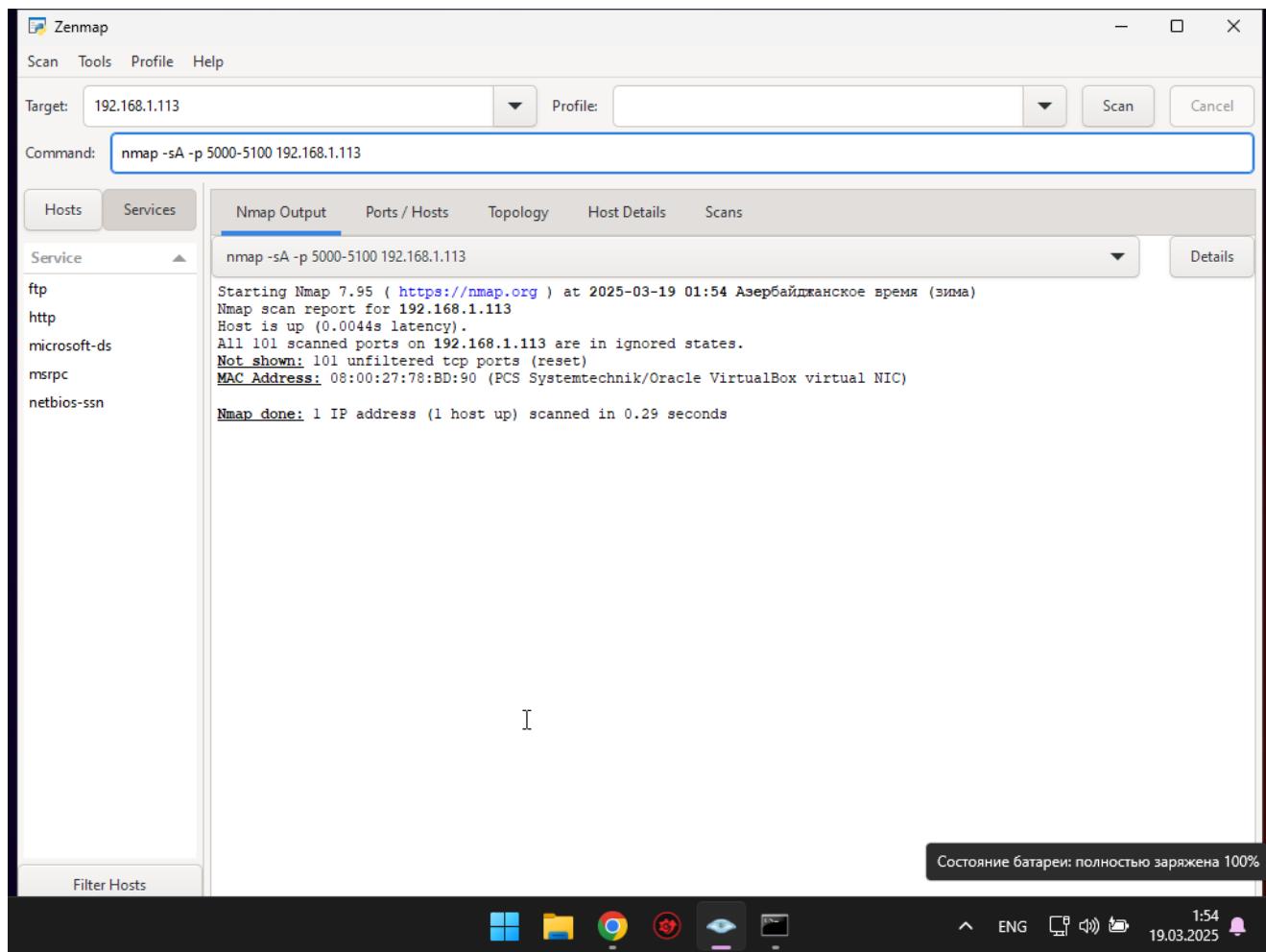
TCP NULL Scan



TCP Xmas Scan

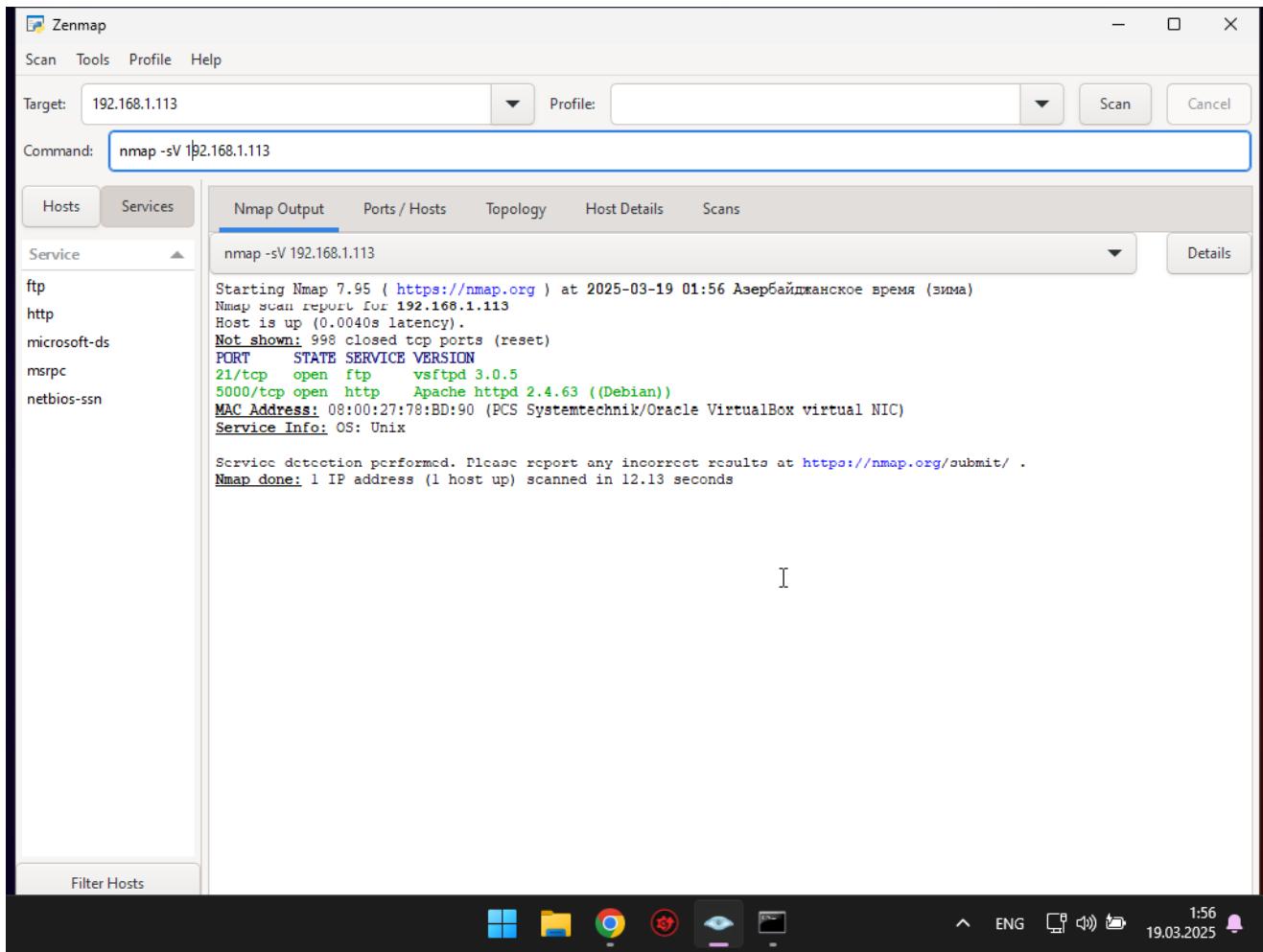


TCP ACK Scan



Шаг 10. Просканируйте машину Linux с помощью команды nmap -sV <ip-адрес>. Опишите полученные результаты

Опция -sV включает определение версий сервисов, работающих на открытых портах.



В результате сканирования мы видим не только открытые порты, но и версии сервисов, запущенных на них.

Видим, что на 21-ом порту запущен ftp-сервис vsftpd v.3.0.5, а на 5000-ом порту - веб-сервер Apache 2.4.63 Debian версия

Шаг 11. Установите Postgresql на Linux командой sudo apt install postgresql

```
/usr/lib/postgresql/17/bin/psql: option requires an argument -- 'v'
psql: hint: Try "psql --help" for more information.

[astepanov@kali] ~
$ psql --version
/usr/lib/postgresql/17/bin/psql: option '-v' is ambiguous; possibilities: '--variable' '--version'
psql: hint: Try "psql --help" for more information.

[astepanov@kali] ~
$ psql --help
psql is the PostgreSQL interactive terminal.

Usage:
  psql [OPTION]... [DBNAME [USERNAME]]

General options:
  -c, --command=COMMAND    run only single command (SQL or internal) and exit
  -d, --dbname=DBNAME      database name to connect to
  -f, --file=FILENAME       execute commands from file, then exit
  -l, --list                list available databases, then exit
  -v, --setvar=NAME=VALUE   set psql variable NAME to VALUE
                           (e.g., -v ON_ERROR_STOP=1)
  -V, --version             output version information, then exit
  -X, --no-psqlrc           do not read startup file (~/.psqlrc)
  -i ("one"), --single-transaction
                           execute as a single transaction (if non-interactive)
  -?, --help[options]        show this help, then exit
  -h, --help[commands]      list backslash commands, then exit
  -h[elp]variables          list special variables, then exit

Input and output options:
  -a, --echo-all            echo all input from script
  -b, --echo-errors         echo failed commands
  -e, --echo-messages       echo messages sent to server
  -E, --Echo-hidden          display queries that internal commands generate
  -L, --log-file=FILENAME   send session log to file
  -n, --no-readline         disable enhanced command line editing (readline)
  -o, --output=FILENAME     send query results to file (or |pipe)
  -q, --quiet               run quietly (no messages, only query output)
  -s, --single-step          single-step mode (confirm each query)
  -S, --single-line          single-line mode (end of line terminates SQL command)

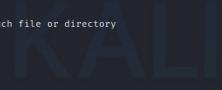
Output format options:
  -A, --no-align            unaligned table output mode
  -c, --csv                 CSV (Comma-Separated Values) table output mode
  -F, --field-separator=STRING
                           field separator for unaligned output (default: "|")
  -H, --html                HTML table output mode
  -P, --pset=VAR[=ARG]        set printing option VAR to ARG (see \pset command)
  -R, --record-separator=STRING
                           record separator for unaligned output (default: newline)
  -t, --tuple-only           print rows only
  -T, --table-attr=TEXT      set HTML table tag attributes (e.g., width, border)
  -x, --expanded             turn on expanded table output
  -z, --field-separator-zero
                           set field separator for unaligned output to zero byte
  -0, --record-separator-zero
                           set record separator for unaligned output to zero byte

Connection options:
  -h, --host=HOSTNAME        database server host or socket directory
  -p, --port=PORT             database server port
  -U, --username=USERNAME    database user name
  -w, --no-password          never prompt for password
  -W, --password              force password prompt (should happen automatically)

For more information, type "\?" (for internal commands) or "help" (for SQL
commands) from within psql, or consult the psql section in the PostgreSQL
documentation.

Report bugs to <pgsql-bugs@lists.postgresql.org>.
PostgreSQL home page: <https://www.postgresql.org/>
```

Проверяем наличие psql (Postgresql предустановлена на Kali)



```
astepanov@kali: ~
```

```
File Actions Edit View Help
-0, --record-separator-zero
      set record separator for unaligned output to zero byte

Connection options:
-h, --host=HOSTNAME      database server host or socket directory
-p, --port=PORT          database server port
-U, --username=USERNAME   database user name
-w, --no-password        never prompt for password
-W, --password           force password prompt (should happen automatically)

For more information, type "\?" (for internal commands) or "\help" (for SQL
commands) from within psql, or consult the psql section in the PostgreSQL
documentation.

Report bugs to <pgsql-bugs@lists.postgresql.org>.
PostgreSQL home page: <https://www.postgresql.org/>

└─(astepanov@kali)─[~]
$ systemctl start postgresql
Failed to start postgresql.service: Unit postgresql.service not found.

└─(astepanov@kali)─[~]
$ systemctl status postgresql
Unit postgresql.service could not be found.

└─(astepanov@kali)─[~]
$ sudo systemctl start postgresql
Failed to start postgresql.service: Unit postgresql.service not found.

└─(astepanov@kali)─[~]
$ which pgsql
/usr/bin/pgsql

└─(astepanov@kali)─[~]
$ pgsql --version
Command 'pgsql' not found, did you mean:
  command 'p1l' from deb gnustep-base-runtime
  command 'sql' from deb parallel
  command 'psql' from deb postgresql-client-common
  command 'p1l' from deb picolisp
  command 'pd1' from deb pd1
  command 'pal' from deb pal
  command 'ps1' from deb ps1
Try: sudo apt install <deb name>

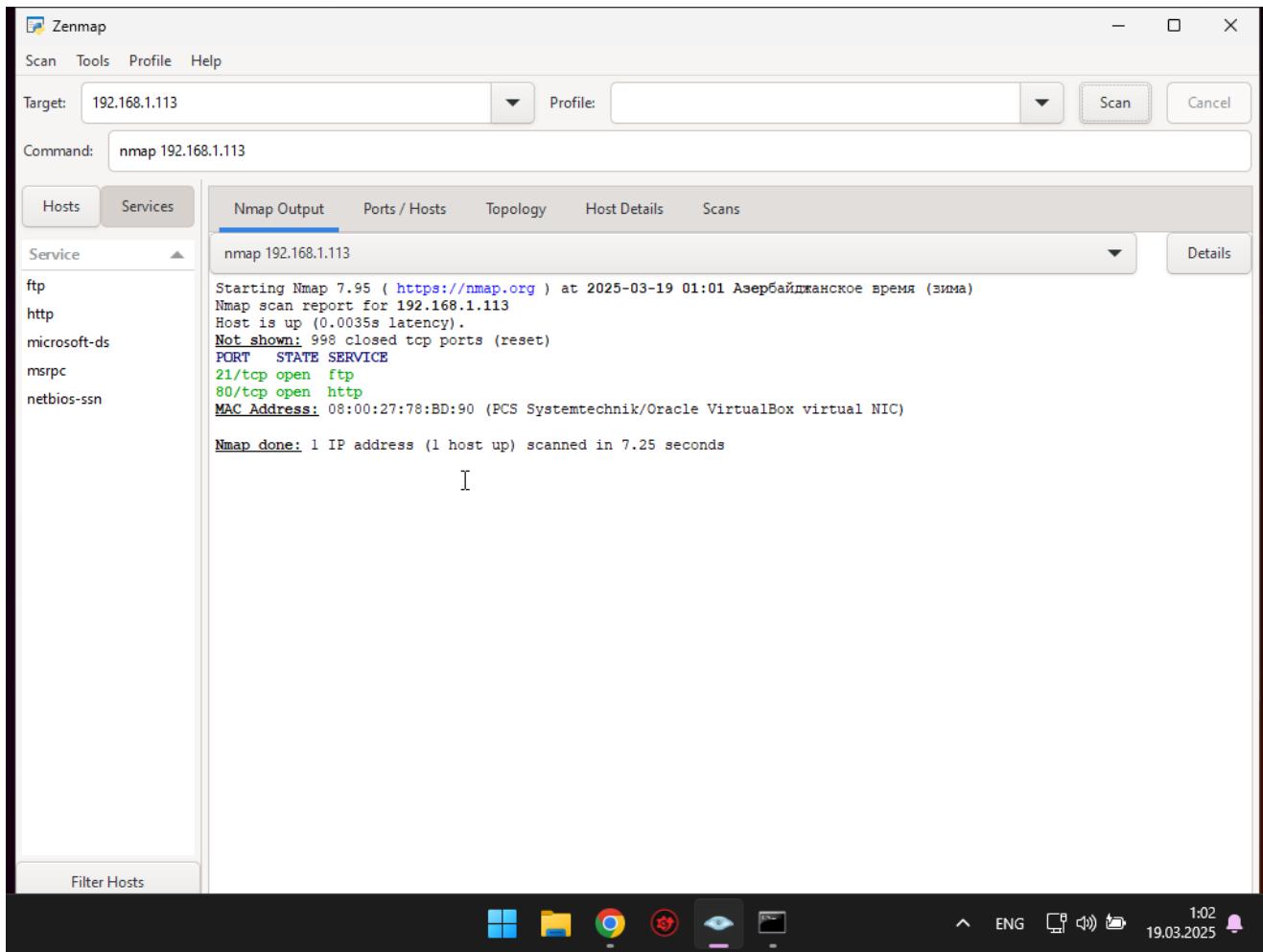
└─(astepanov@kali)─[~]
$ psql --version
psql: error: connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: No such file or directory
  Is the server running locally and accepting connections on that socket?

└─(astepanov@kali)─[~]
$ psql --version
psql (PostgreSQL) 17.0 (Debian 17.0-1+b2)

└─(astepanov@kali)─[~]
$ sudo systemctl start postgresql
└─(astepanov@kali)─[~]
$ sudo systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
  Loaded: loaded (/usr/lib/systemd/system/postgresql.service; disabled; preset: disabled)
    Active: active (exited) since Tue 2025-03-18 16:42:04 EDT; 5s ago
      Invocation: /cedee0043be48f88cc2bd245e4f73e6
     Process: 87783 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 87783 (code=exited, status=0/SUCCESS)
      Mem peak: 1.6M
        CPU: 1ms
Mar 18 16:42:04 kali systemd[1]: Starting PostgreSQL RDBMS ...
Mar 18 16:42:04 kali systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.
└─(astepanov@kali)─[~]
```

Запускаем сервис postgresql

Шаг 12. Повторите пункт 9. Напишите, что изменилось.

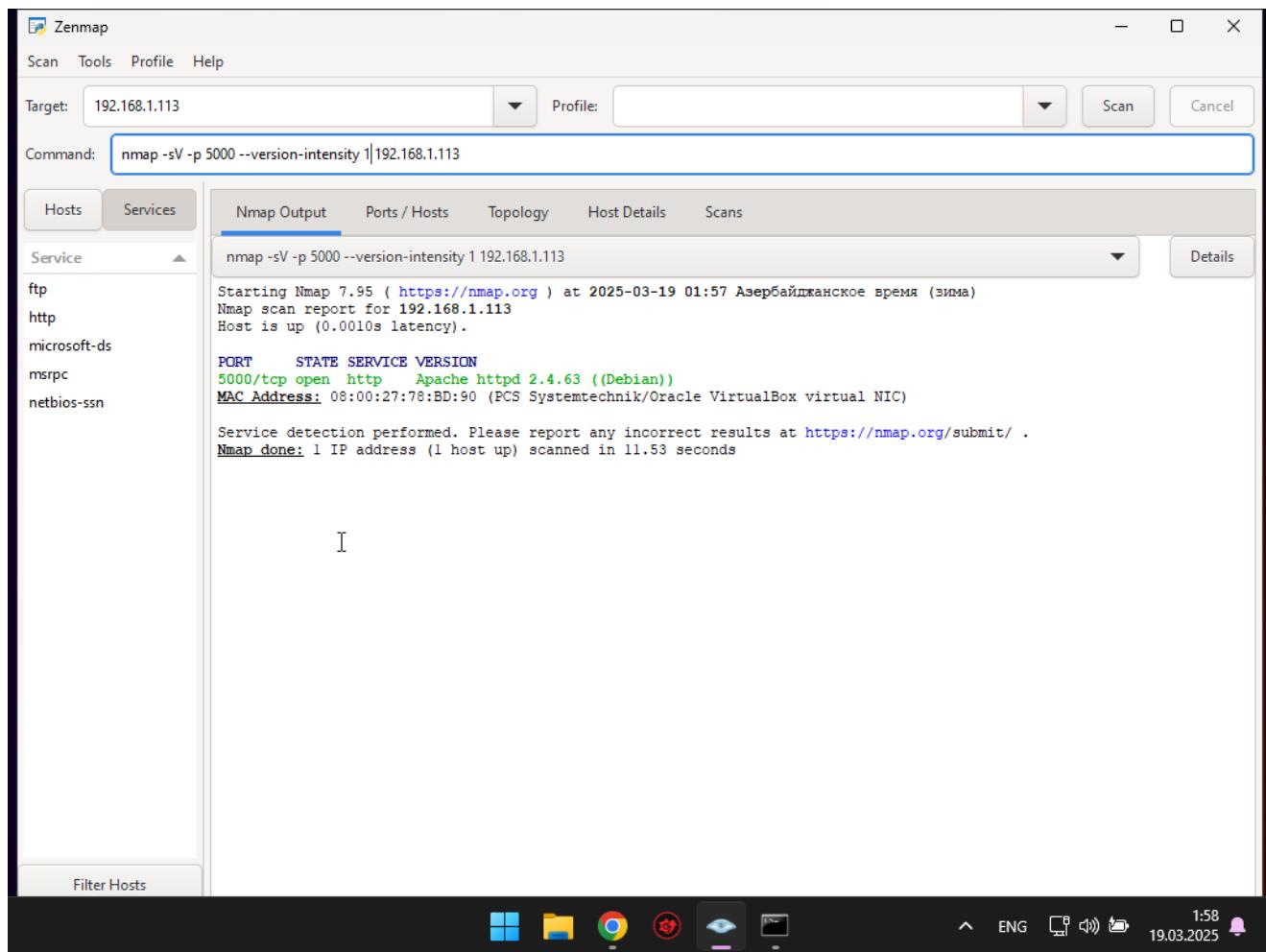


Результат сканирования не изменился. Видимо в задании предполагалось, что после запуска сервиса pgsql должен появиться порт pg, однако это требует дополнительной настройки сервиса, т.к. по умолчанию pg слушает только localhost.

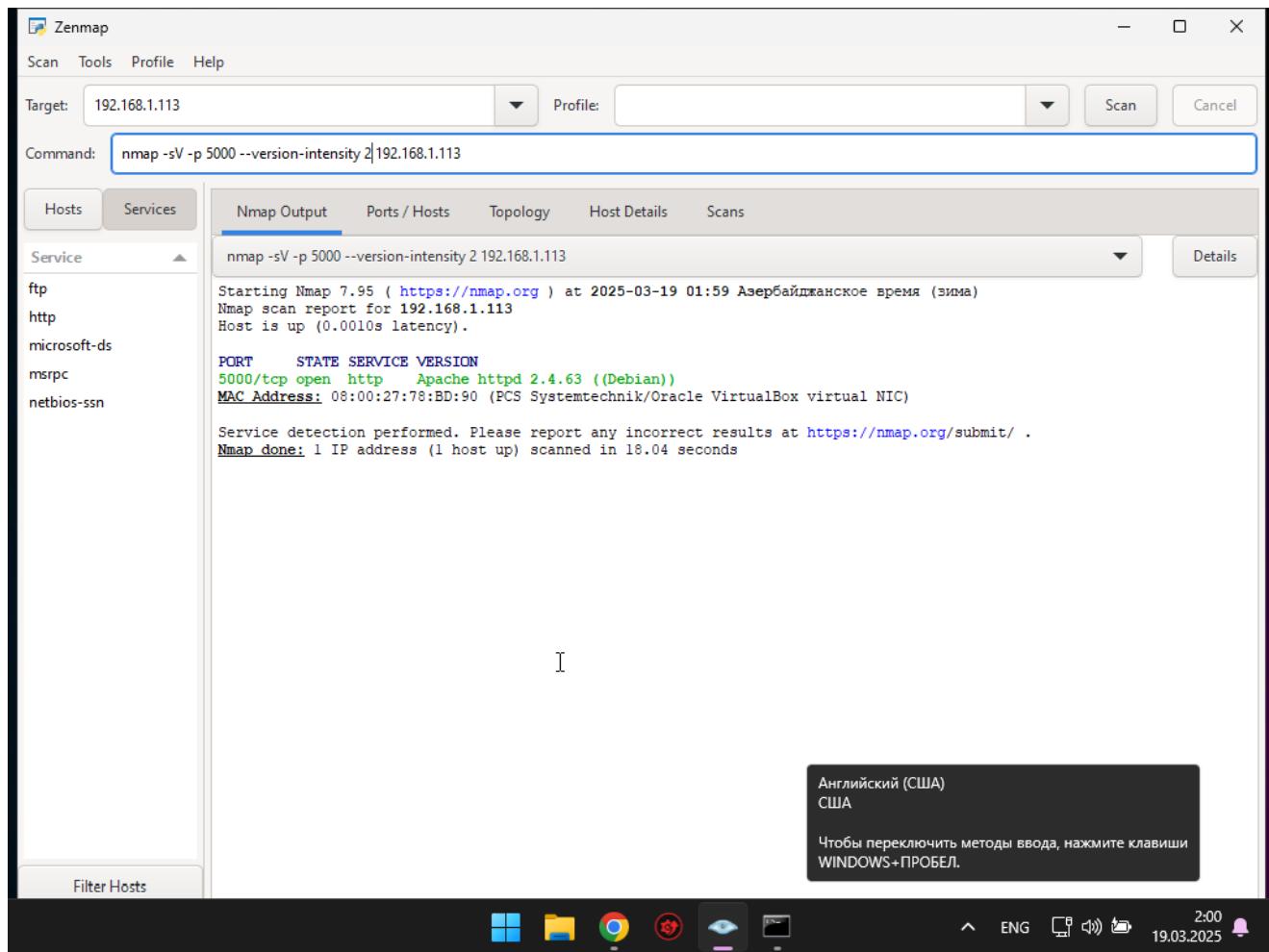
Шаг 13. Просканируйте нестандартный порт из 7 и порт Postgresql, указывая уровни интенсивности от 1 до 9. Сравните полученные результаты и опишите, какие результаты соответствуют действительности.

* Из-за того, что postgresql настроен и его порт не виден результаты отражены для порта 5000

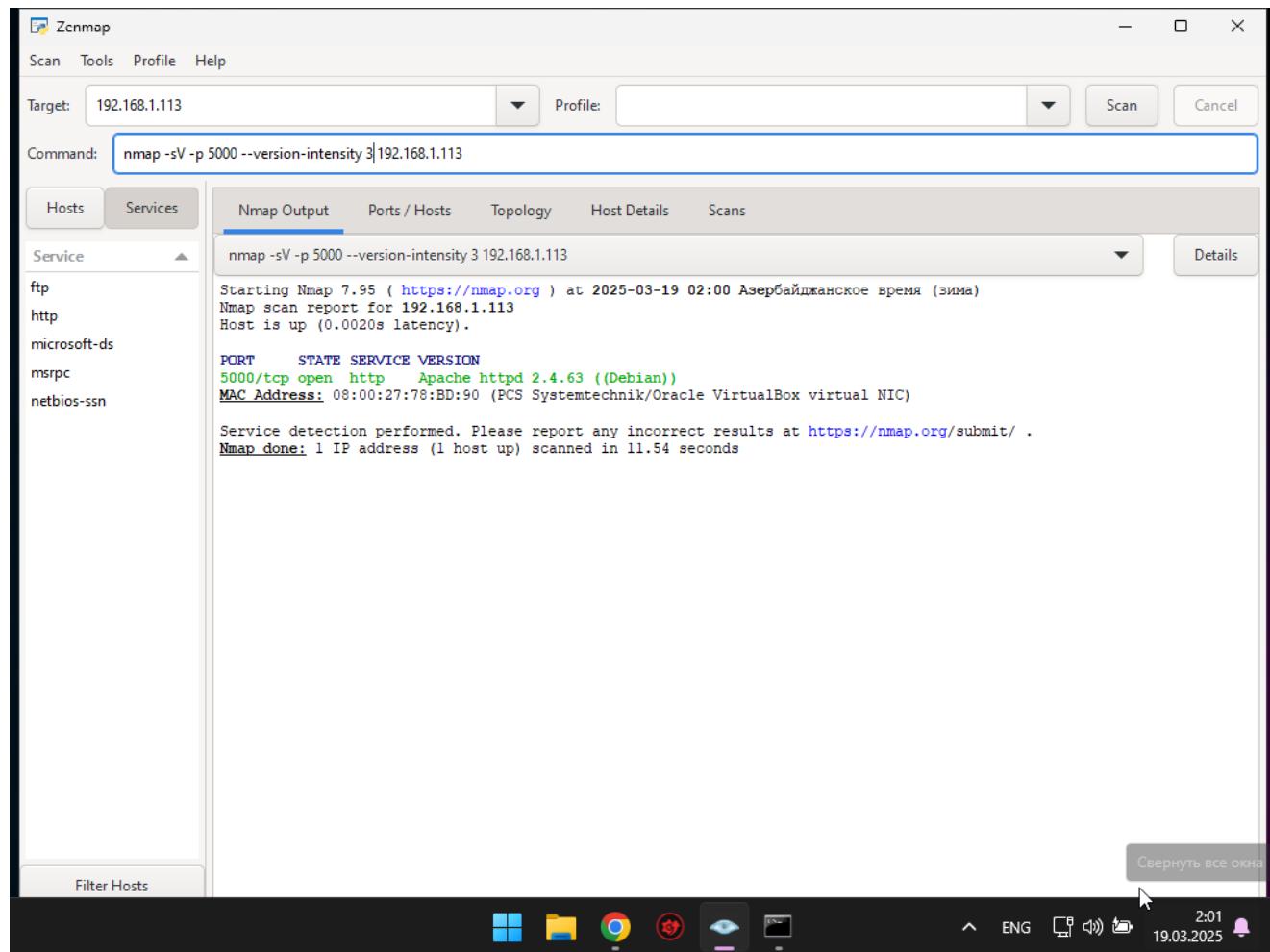
Интенсивность 1



Интенсивность 2



Интенсивность 3



Интенсивность 4

Zenmap window showing an Nmap scan report for host 192.168.1.113. The command used was nmap -sV -p 5000 --version-intensity 4 192.168.1.113.

Hosts **Services**

Service

- ftp
- http
- microsoft-ds
- msrpc
- netbios-ssn

Nmap Output

```
nmap -sV -p 5000 --version-intensity 4 192.168.1.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 02:01 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.0019s latency).

PORT      STATE SERVICE VERSION
5000/tcp  open  http    Apache httpd 2.4.63 ((Debian))
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.55 seconds
```

Filter Hosts

Windows taskbar icons: File Explorer, Google Chrome, Task View, Task Manager, Task Scheduler, Taskbar settings, Date/Time (2:01, 19.03.2025).

Интенсивность 5

Zenmap window showing the results of an Nmap scan. The target IP is 192.168.1.113. The command used was nmap -sV -p 5000 --version-intensity 5 192.168.1.113.

The output shows:

```
nmap -sV -p 5000 --version-intensity 5 192.168.1.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 02:01 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.0021s latency).

PORT      STATE SERVICE VERSION
5000/tcp   open  http    Apache httpd 2.4.63 ((Debian))
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.50 seconds
```

The Services tab is selected, showing the following services:

- ftp
- http
- microsoft-ds
- msrpc
- netbios-ssn

The status bar at the bottom right shows the date and time: 19.03.2025 2:01.

Интенсивность 6

Zenmap window showing an Nmap scan report for host 192.168.1.113. The command used was nmap -sV -p 5000 --version-intensity 6 192.168.1.113.

Nmap Output:

```
nmap -sV -p 5000 --version-intensity 6 192.168.1.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 02:02 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.001s latency).

PORT      STATE SERVICE VERSION
5000/tcp  open  http    Apache httpd 2.4.63 ((Debian))
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.53 seconds
```

Services:

- ftp
- http
- microsoft-ds
- msrpc
- netbios-ssn

Filter Hosts:

Windows taskbar icons: File Explorer, Chrome, Task View, Task Manager, Task Scheduler, Taskbar settings, Start button, ENG, Battery, Date/Time (19.03.2025).

Интенсивность 7

Zenmap window showing an Nmap scan report for host 192.168.1.113. The command used was nmap -sV -p 5000 --version-intensity 7 192.168.1.113.

Nmap Output:

```
nmap -sV -p 5000 --version-intensity 7 192.168.1.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 02:02 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.0010s latency).

PORT      STATE SERVICE VERSION
5000/tcp   open  http    Apache httpd 2.4.63 ((Debian))
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.59 seconds
```

Services:

- ftp
- http
- microsoft-ds
- msrpc
- netbios-ssn

Filter Hosts:

Windows taskbar icons: File Explorer, Chrome, Task View, Task Manager, Task Scheduler, Taskbar settings, Date/Time (2:02, 19.03.2025).

Интенсивность 8

Zenmap window showing the results of an Nmap scan. The target IP is 192.168.1.113. The command used was nmap -sV -p 5000 --version-intensity 8 192.168.1.113.

The output shows:

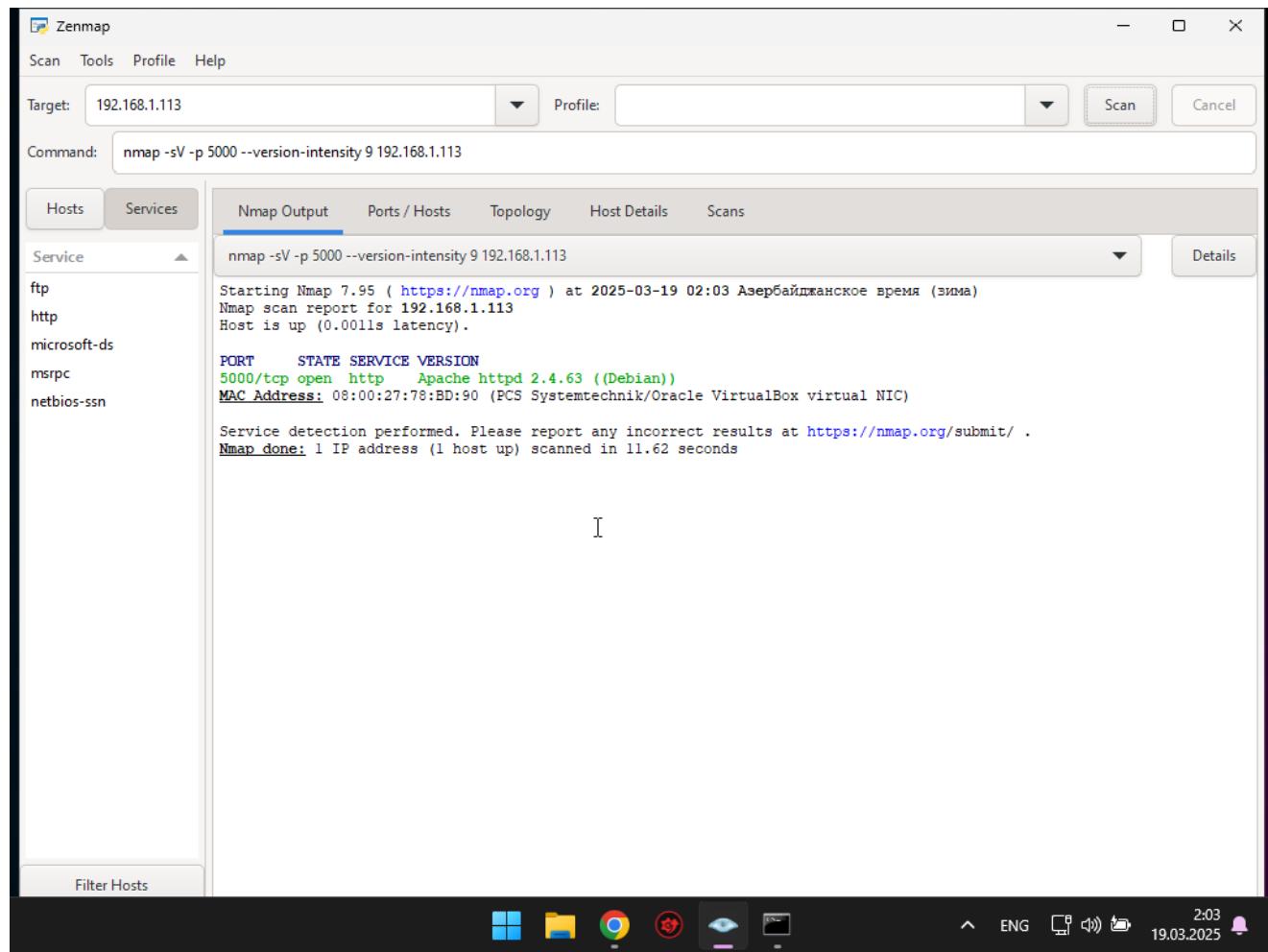
```
nmap -sV -p 5000 --version-intensity 8 192.168.1.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 02:02 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.0010s latency).

PORT      STATE SERVICE VERSION
5000/tcp   open  http    Apache httpd 2.4.63 ((Debian))
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

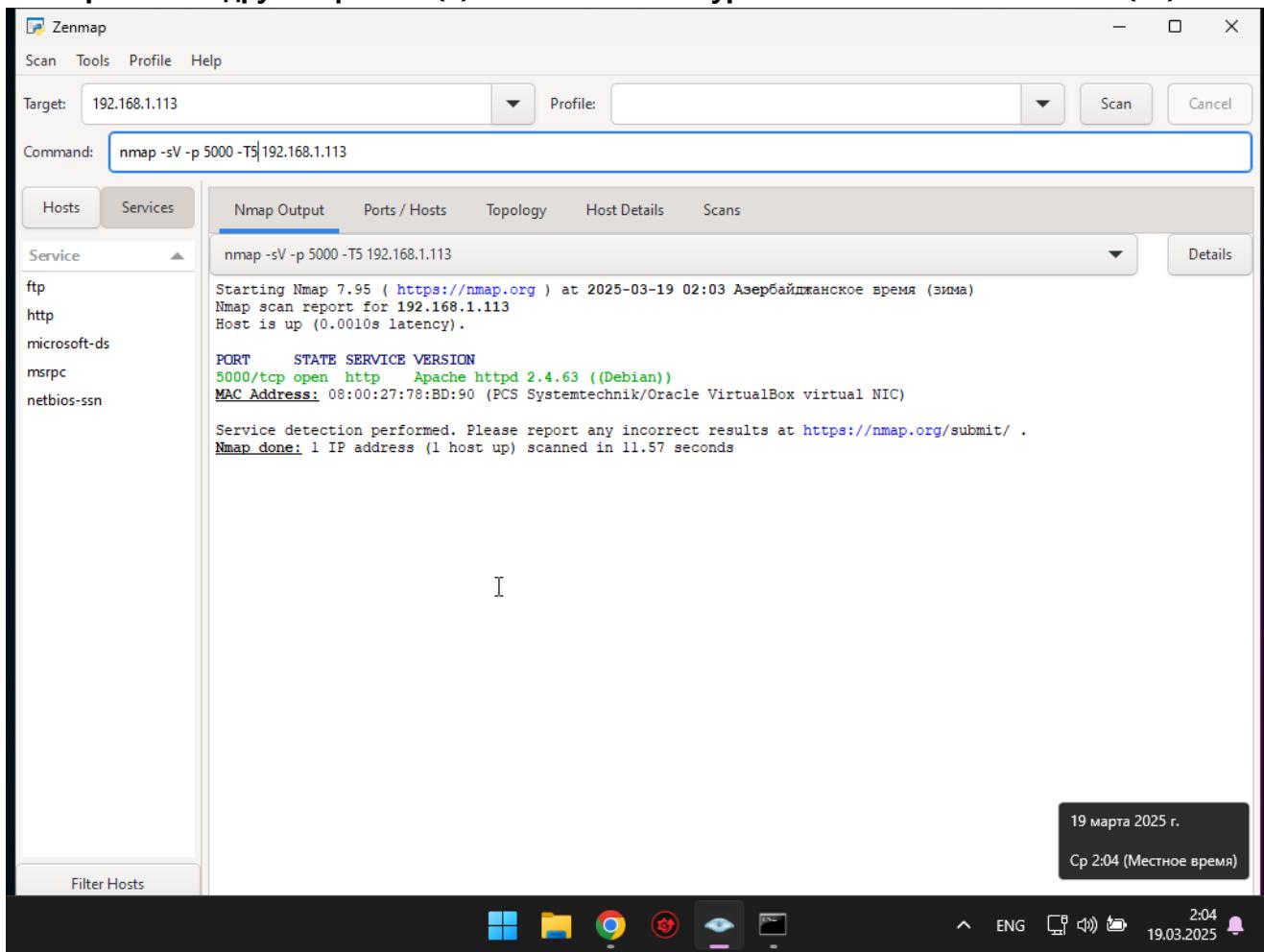
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.67 seconds
```

The Services tab is selected. On the left, a sidebar lists services: ftp, http, microsoft-ds, msrpc, netbios-ssn. At the bottom, there's a "Filter Hosts" input field and a system tray with icons for File Explorer, Google Chrome, Task View, Task Manager, and others, along with system status information like ENG, battery level, and date/time (19.03.2025, 2:02).

Интенсивность 9



Сканирование с другим флагом (T) с максимальным уровнем интенсивности insane (T5)



В результате пробовал использовать все уровни интенсивности от 1 до 9 - результат одинаковый

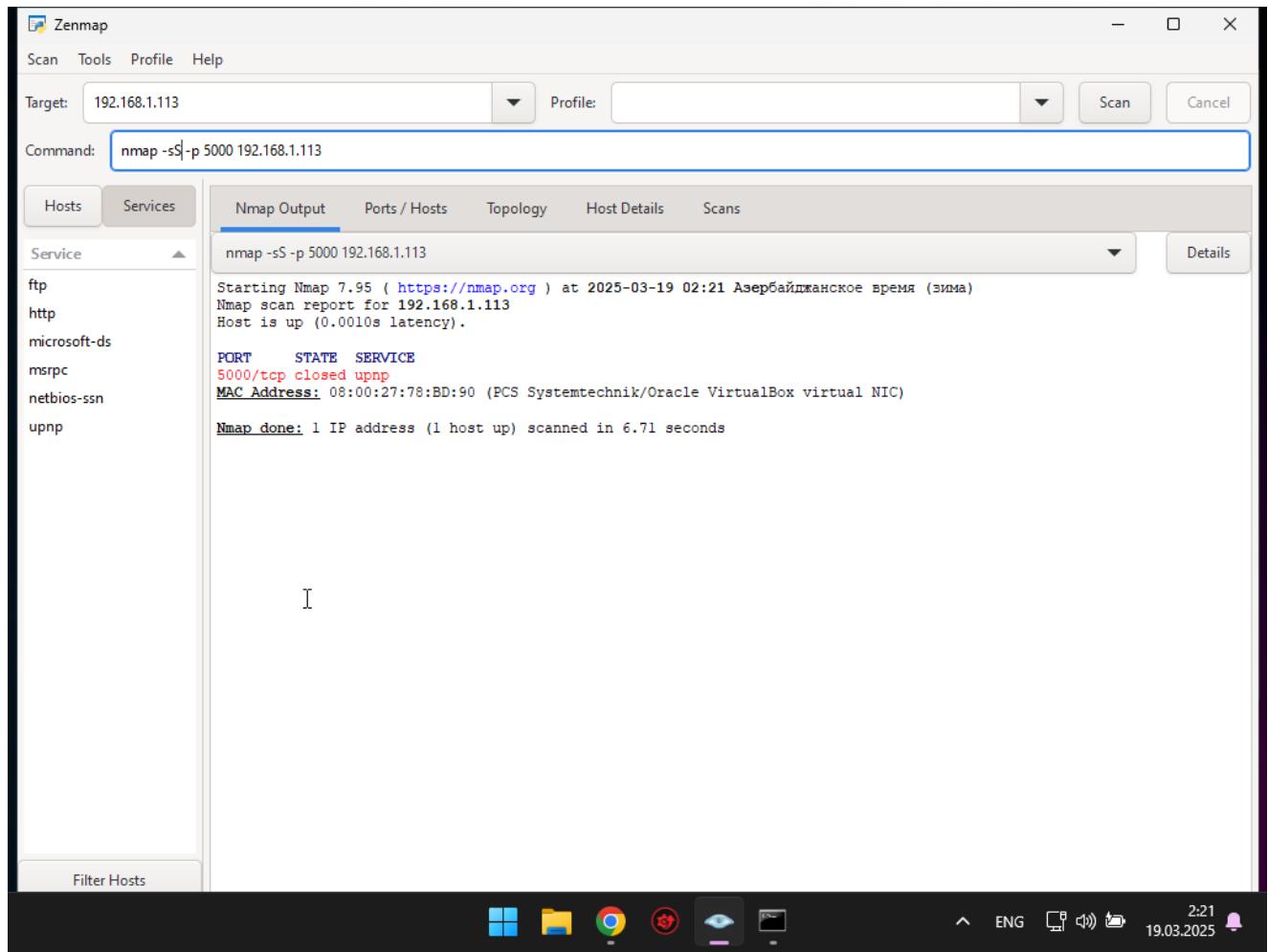
Шаг 14. Заблокируйте любой порт из открытых на машине Linux с помощью iptables по политике REJECT.

Блокируем 5000-ый порт

```
sudo: iptables: command not found
└──(astepanov㉿kali)-[~]
$ sudo iptables -A INPUT -p tcp --dport 5000 -j REJECT
└──(astepanov㉿kali)-[~]
$ ┌─[~]─[~]
```

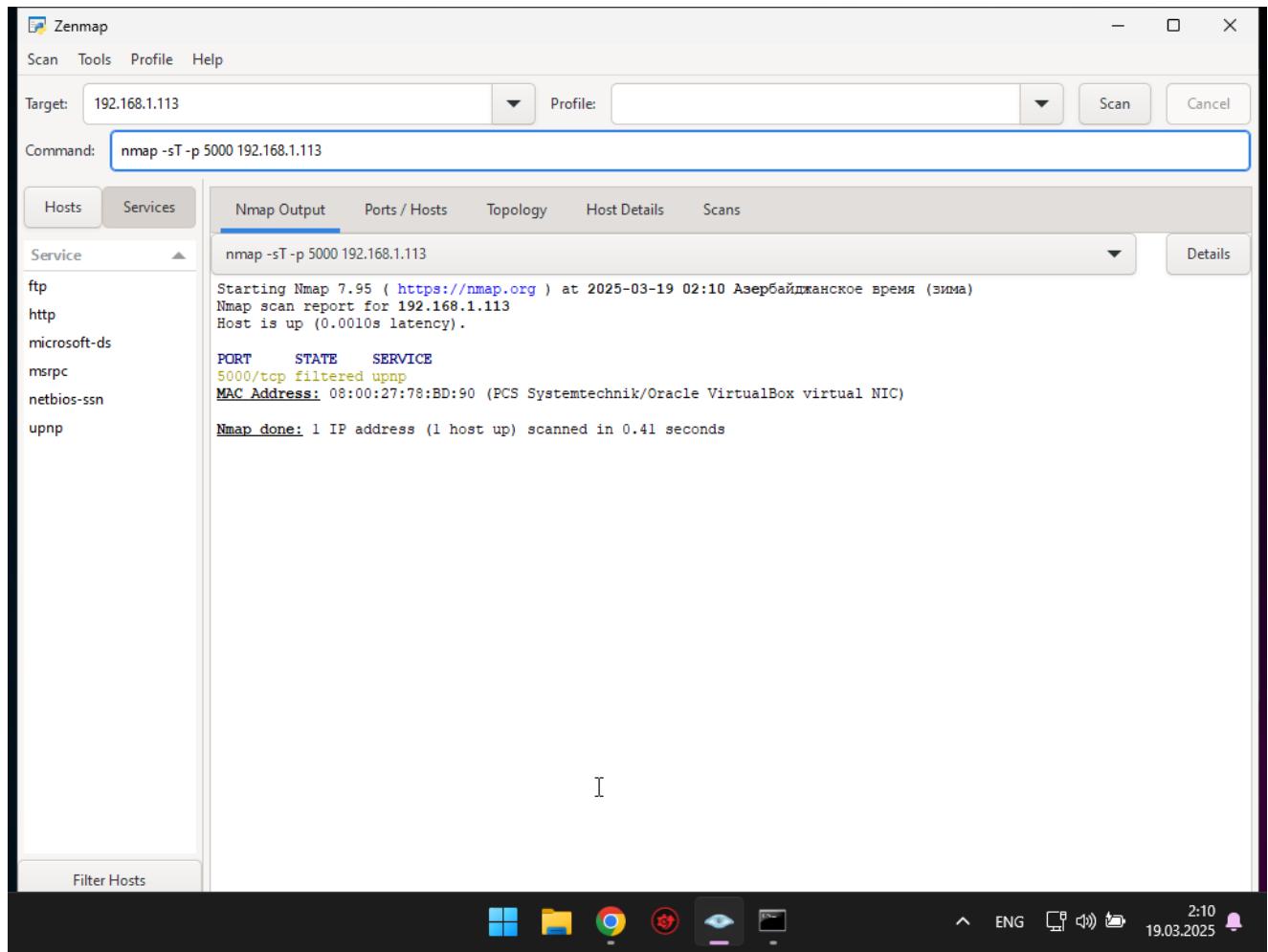
Шаг 15. Просканируйте заблокированный в пункте 13 (14) порт типами сканирования TCP SYN Scan, TCP Connect Scan, UDP Scan, TCP FIN Scan, TCP NULL Scan, TCP Xmas Scan и TCP ACK Scan. Сравните полученные результаты.

TCP SYN Scan



REJECT отправляет ответ RST, нмар считает порт закрытым.

TCP Connect Scan



Порт показывается как filtered

UDP Scan

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113

Profile:

Command: nmap -sU -p 5000 192.168.1.113

Hosts Services

Service ▾

- ftp
- http
- microsoft-ds
- msrpc
- netbios-ssn
- upnp

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sU -p 5000 192.168.1.113

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 02:10 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.001s latency).

PORT      STATE    SERVICE
5000/udp  closed   upnp
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

Filter Hosts

Состояние батареи: полностью заряжена 100%

2:10 19.03.2025

Windows taskbar icons: File Explorer, Google Chrome, Task View, Taskbar settings.

Порт показывается как closed

TCP FIN Scan

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113 Profile: Scan Cancel

Command: nmap -sF -p 5000 192.168.1.113

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

Service ▲

ftp
http
microsoft-ds
msrpc
netbios-ssn
upnp

nmap -sF -p 5000 192.168.1.113

Starting Nmap 7.95 (https://nmap.org) at 2025-03-19 02:22 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.0021s latency).

PORT	STATE	SERVICE
5000/tcp	closed	upnp

MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

Filter Hosts

2:22 19.03.2025

Порт показывается как closed

TCP NULL Scan

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113 Profile: Scan Cancel

Command: nmap -sN -p 5000 192.168.1.113

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

Service ▲

ftp
http
microsoft-ds
msrpc
netbios-ssn
upnp

nmap -sN -p 5000 192.168.1.113

Starting Nmap 7.95 (https://nmap.org) at 2025-03-19 02:22 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.0010s latency).

PORT	STATE	SERVICE
5000/tcp	closed	upnp

MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

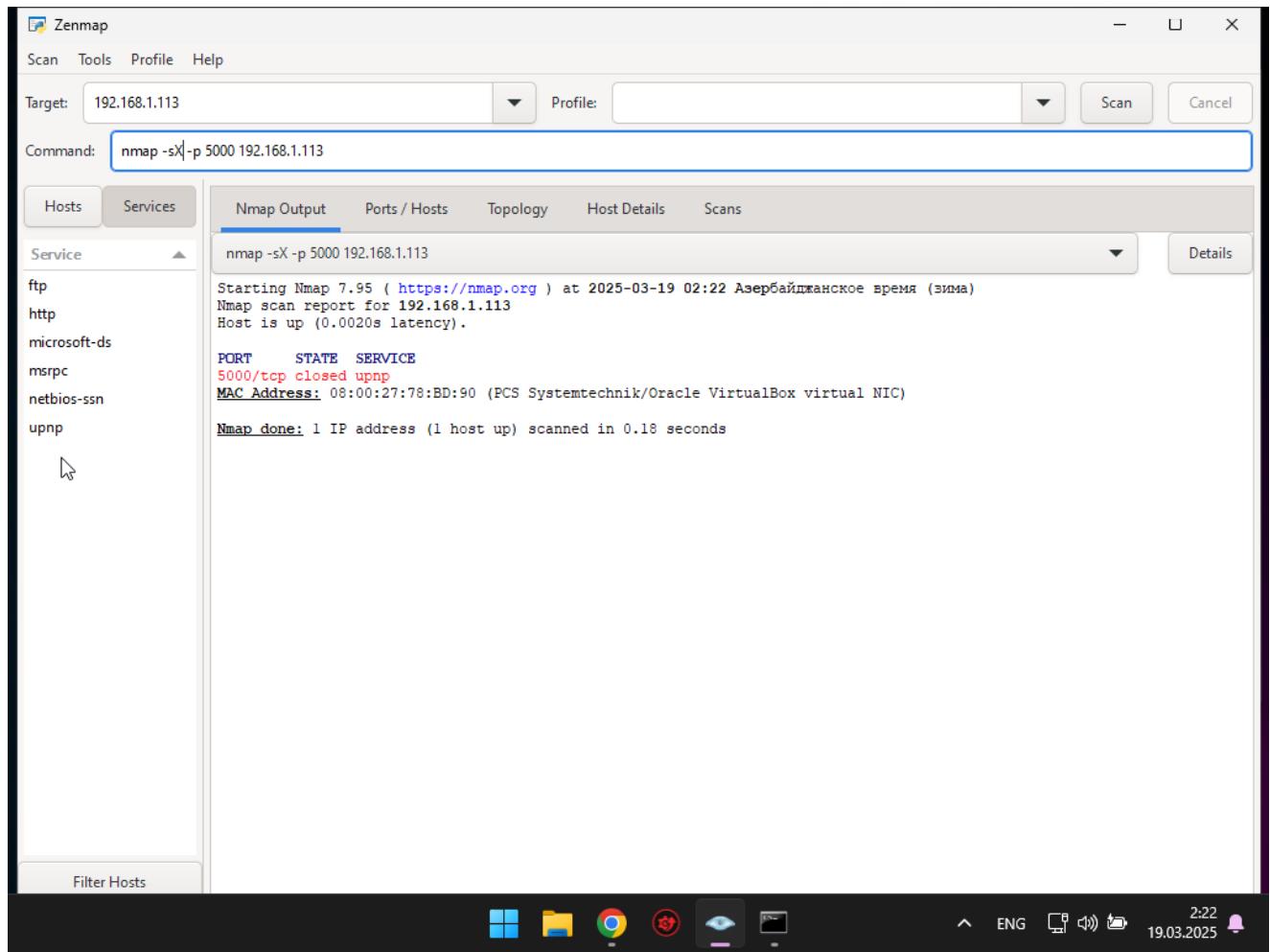
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds

Filter Hosts

2:22 ENG 19.03.2025

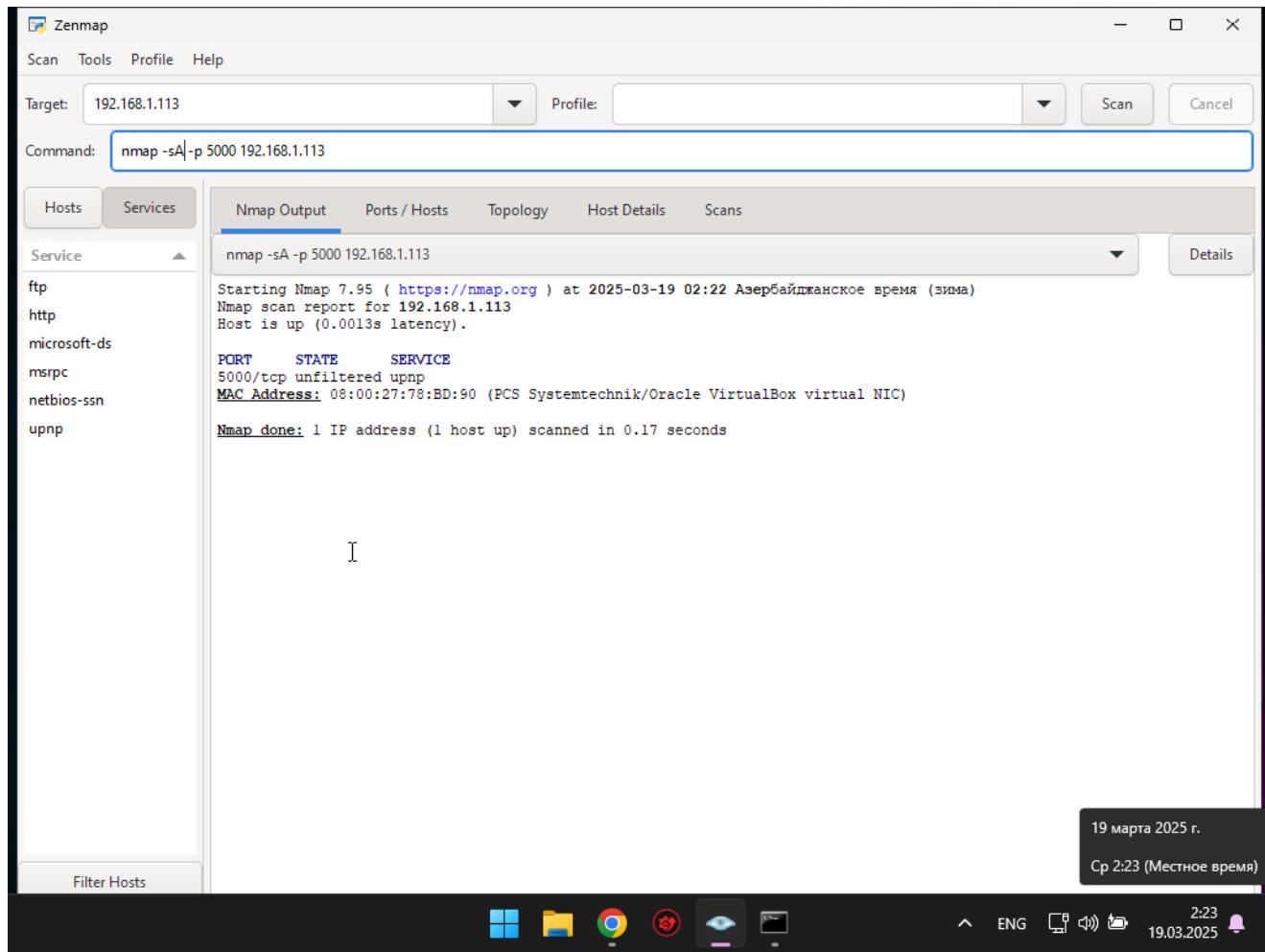
Порт показывается как closed

TCP Xmas Scan



Порт показывается как closed

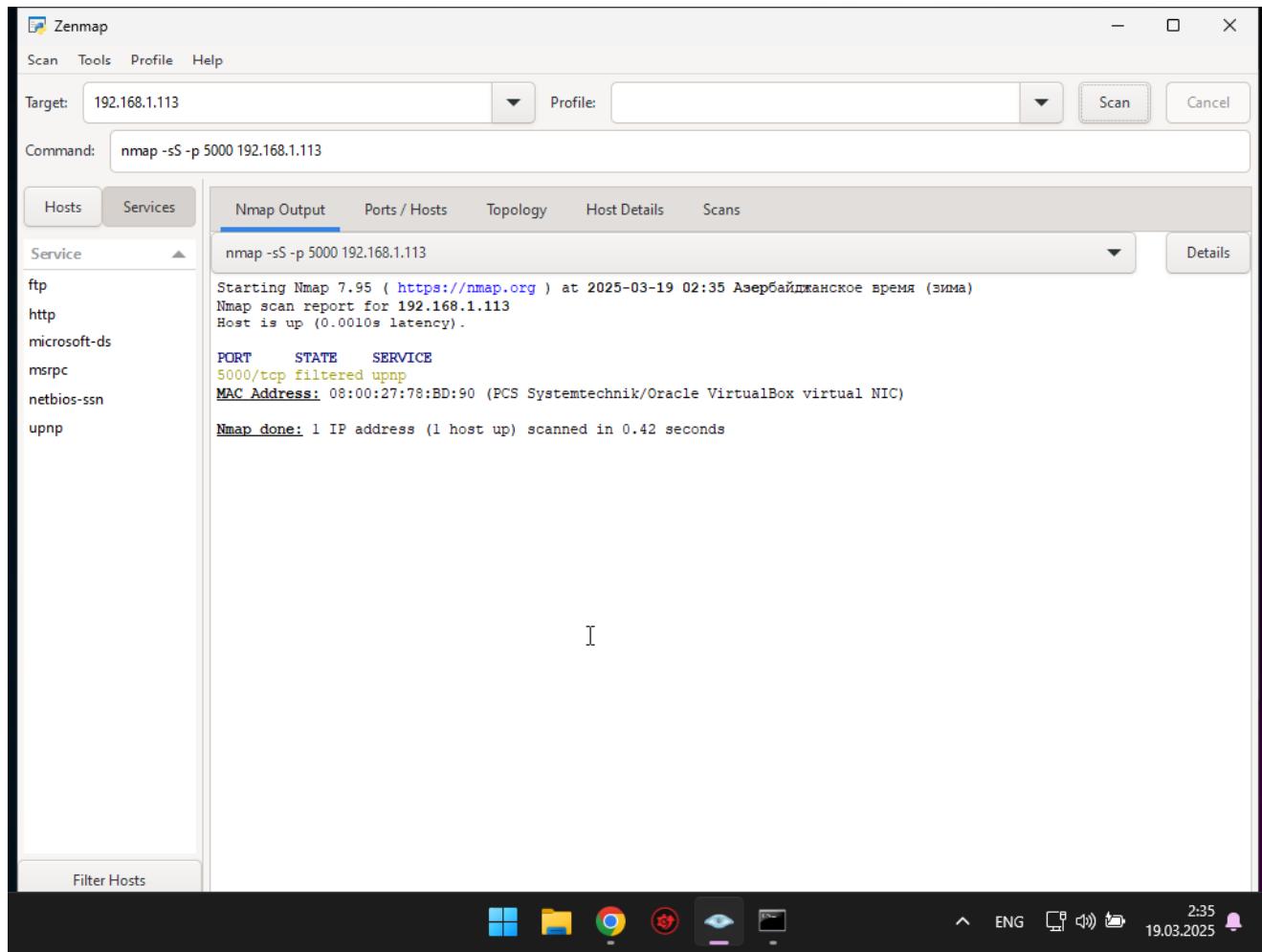
TCP ACK Scan



Порт показывается как unfiltered

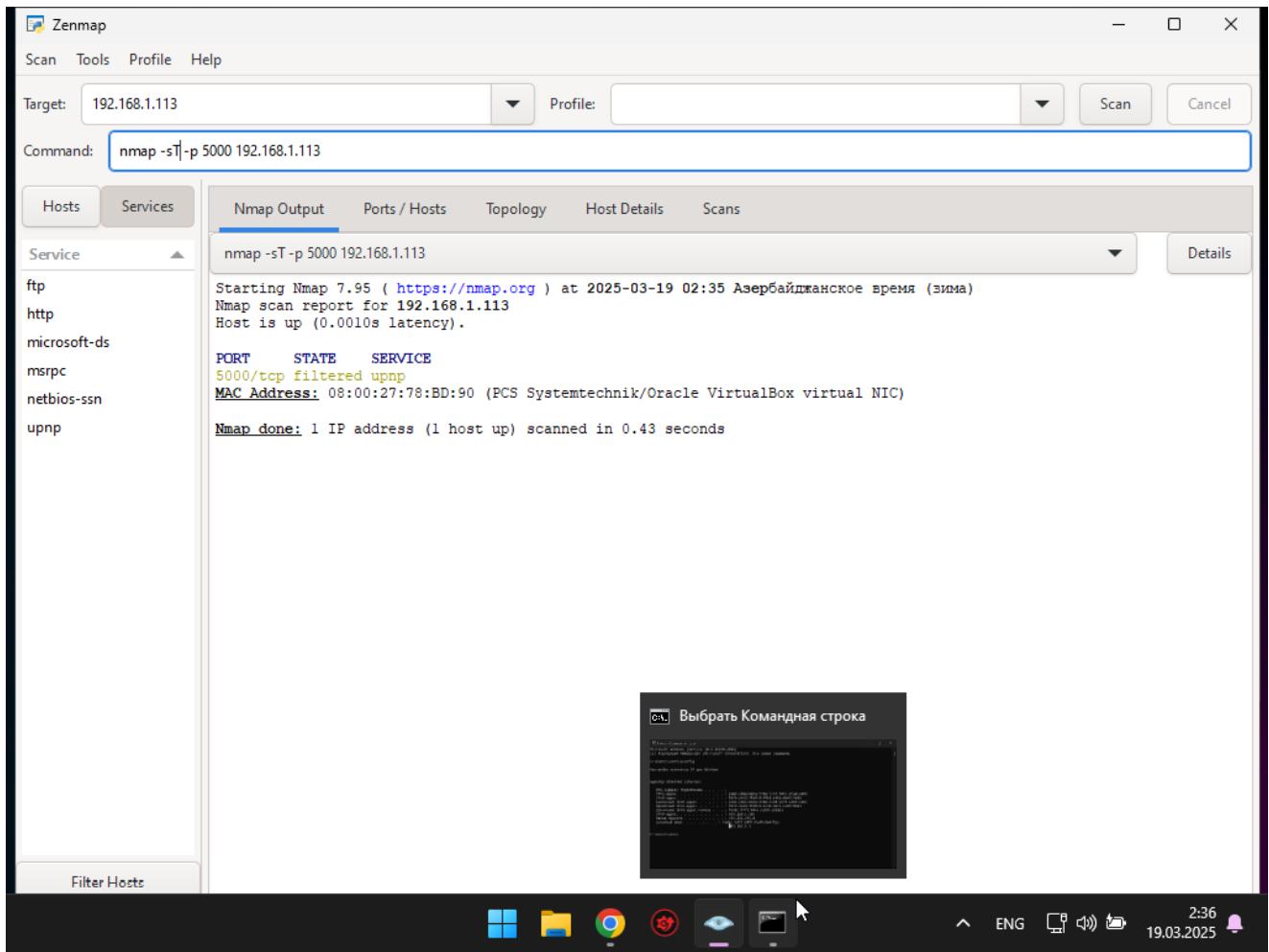
Шаг 16. Удалите правило из пункта 13 (14) и добавьте аналогичное, но с политикой DROP. Повторите пункт 14 (15). Сравните результаты с пунктом 14 (15).

TCP SYN Scan



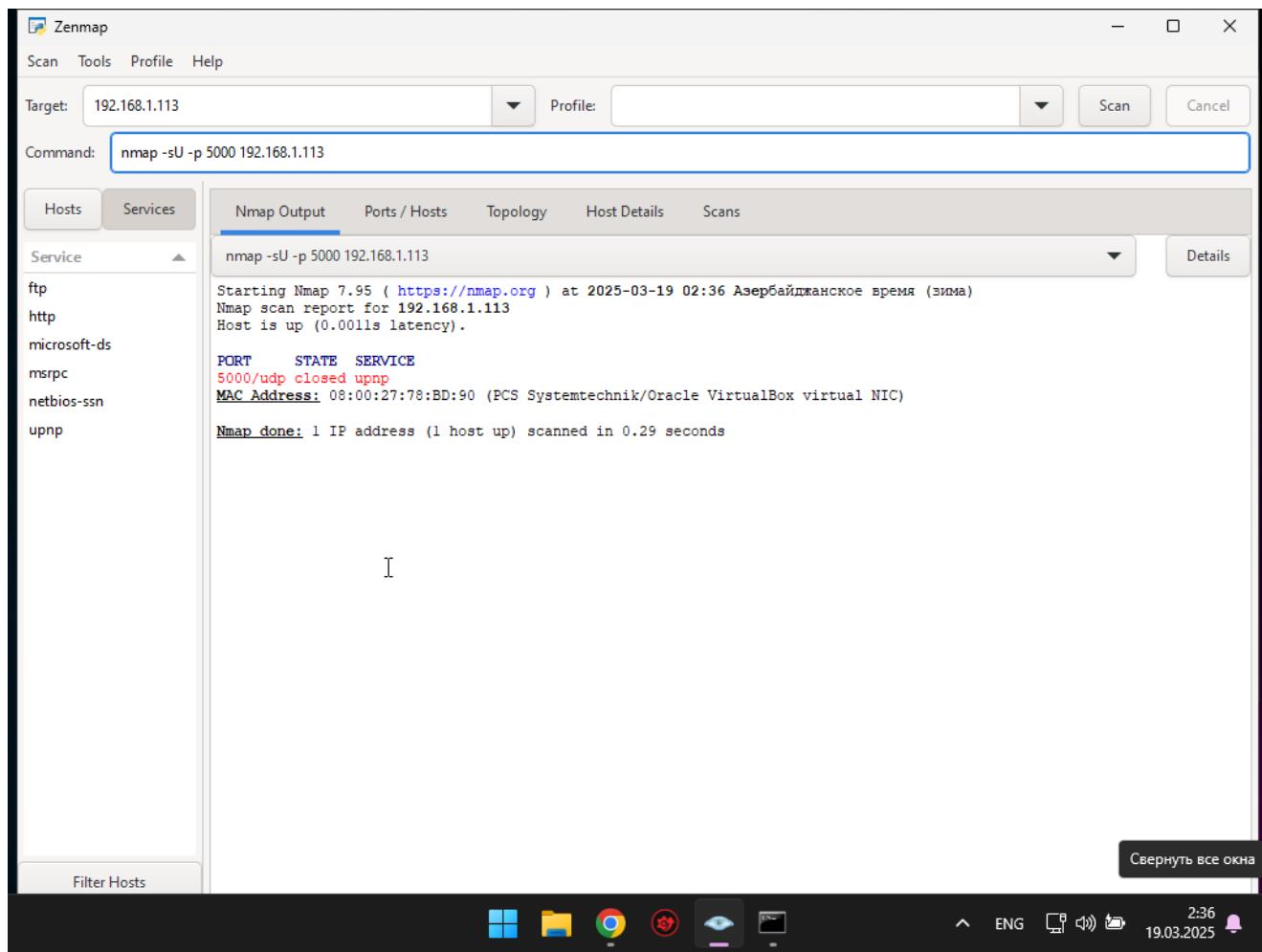
Порт показывается как filtered

TCP Connect Scan



Порт показывается как filtered

UDP Scan



Порт показывается как closed

TCP FIN Scan

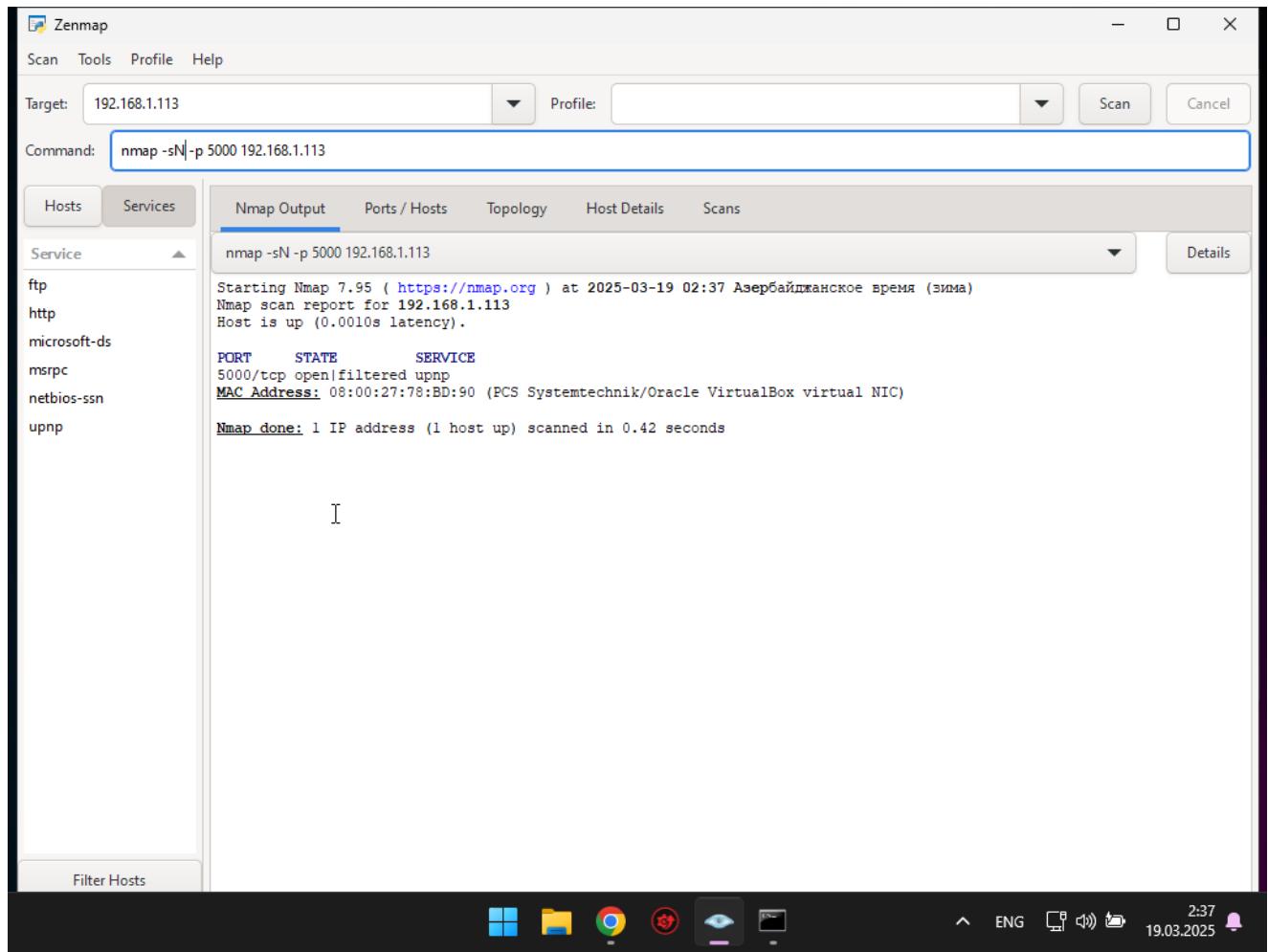
```
nmap -sF -p 5000 192.168.1.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 02:36 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.0010s latency).

PORT      STATE      SERVICE
5000/tcp  open|filtered  upnp
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.95 seconds
```

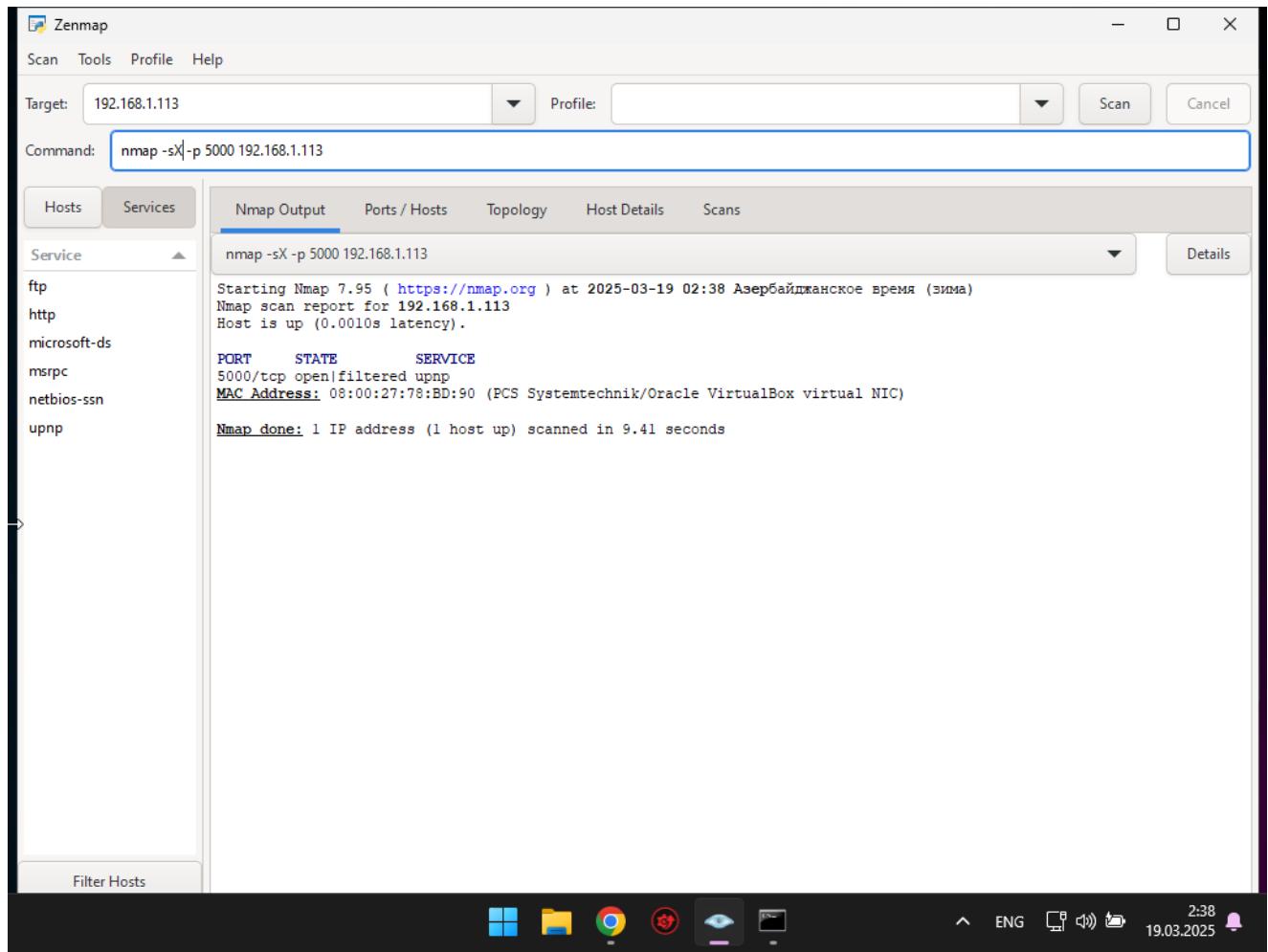
Порт показывается как open|filtered

TCP NULL Scan



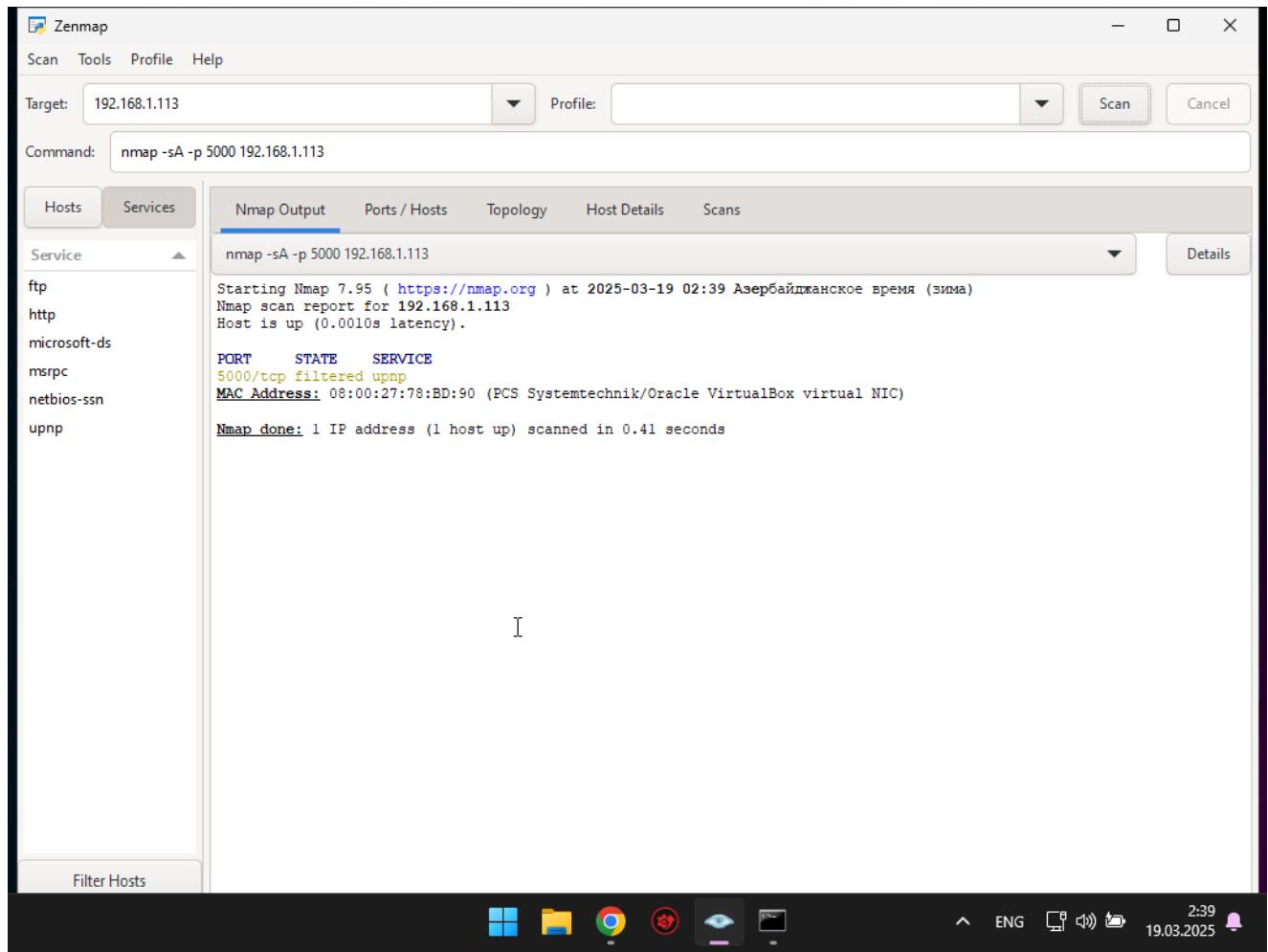
Порт показывается как open|filtered

TCP Xmas Scan



Порт показывается как open|filtered

TCP ACK Scan



Порт показывается как filtered