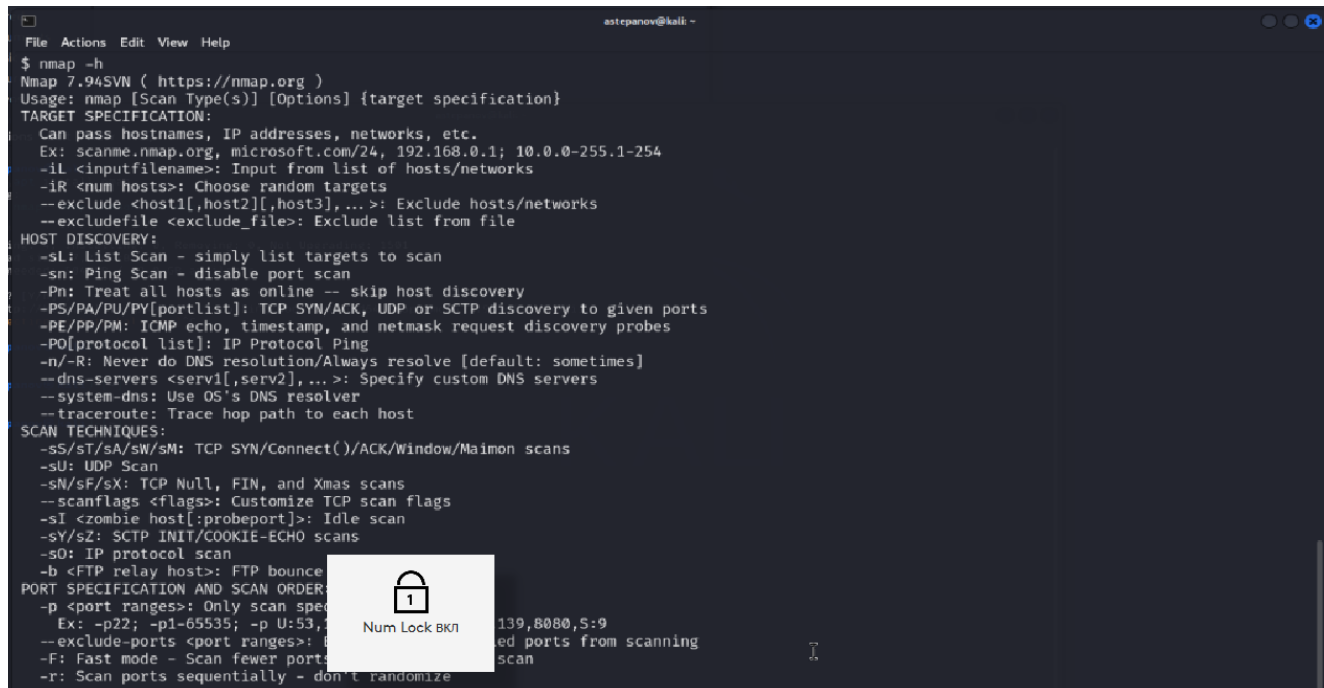


# Модуль 2. Сканирование сетей (HW)

## Лабораторная работа №2 (HW)

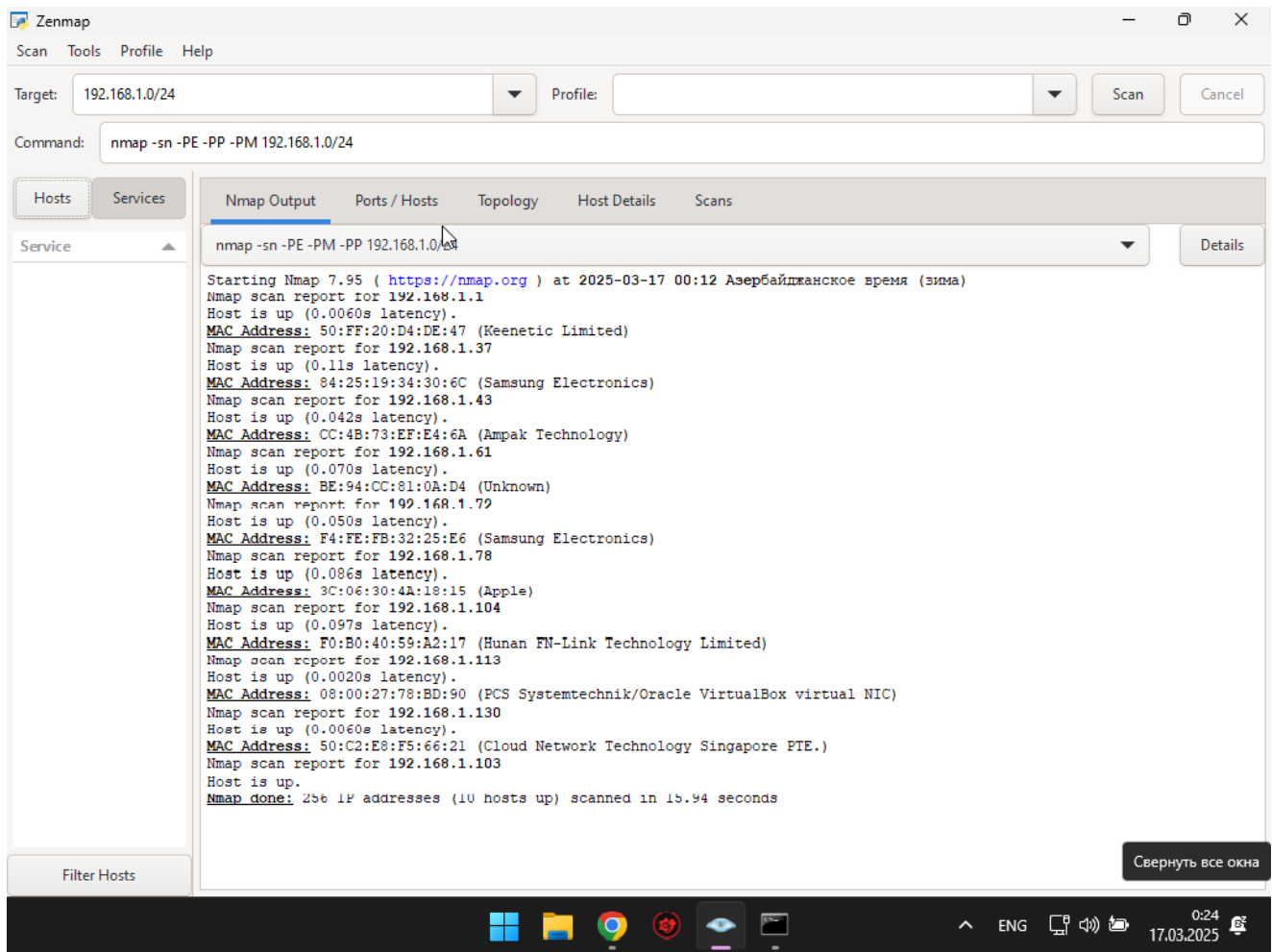
Для выполнения данной лабораторной работы пришлось устанавливать Windows на виртуальную машину

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



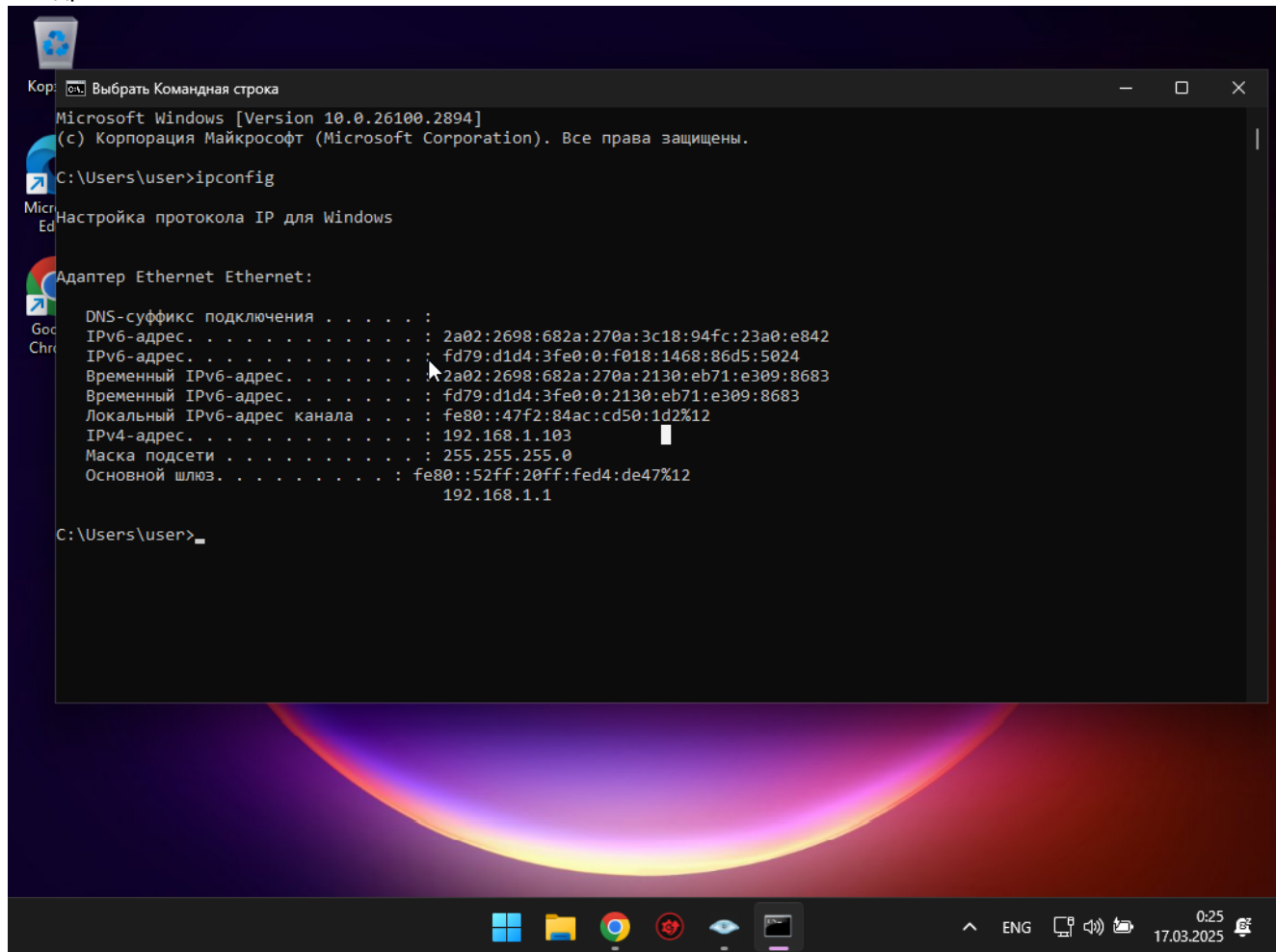
```
File Actions Edit View Help
$ nmap -h
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: 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/PA/PY/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/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/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,T:80
  --exclude-ports <port ranges>: Exclude ports from scanning
  -F: Fast mode - Scan fewer ports (the default)
  -r: Scan ports sequentially - don't randomize
```

Шаг 2. Установите Nmap на Windows

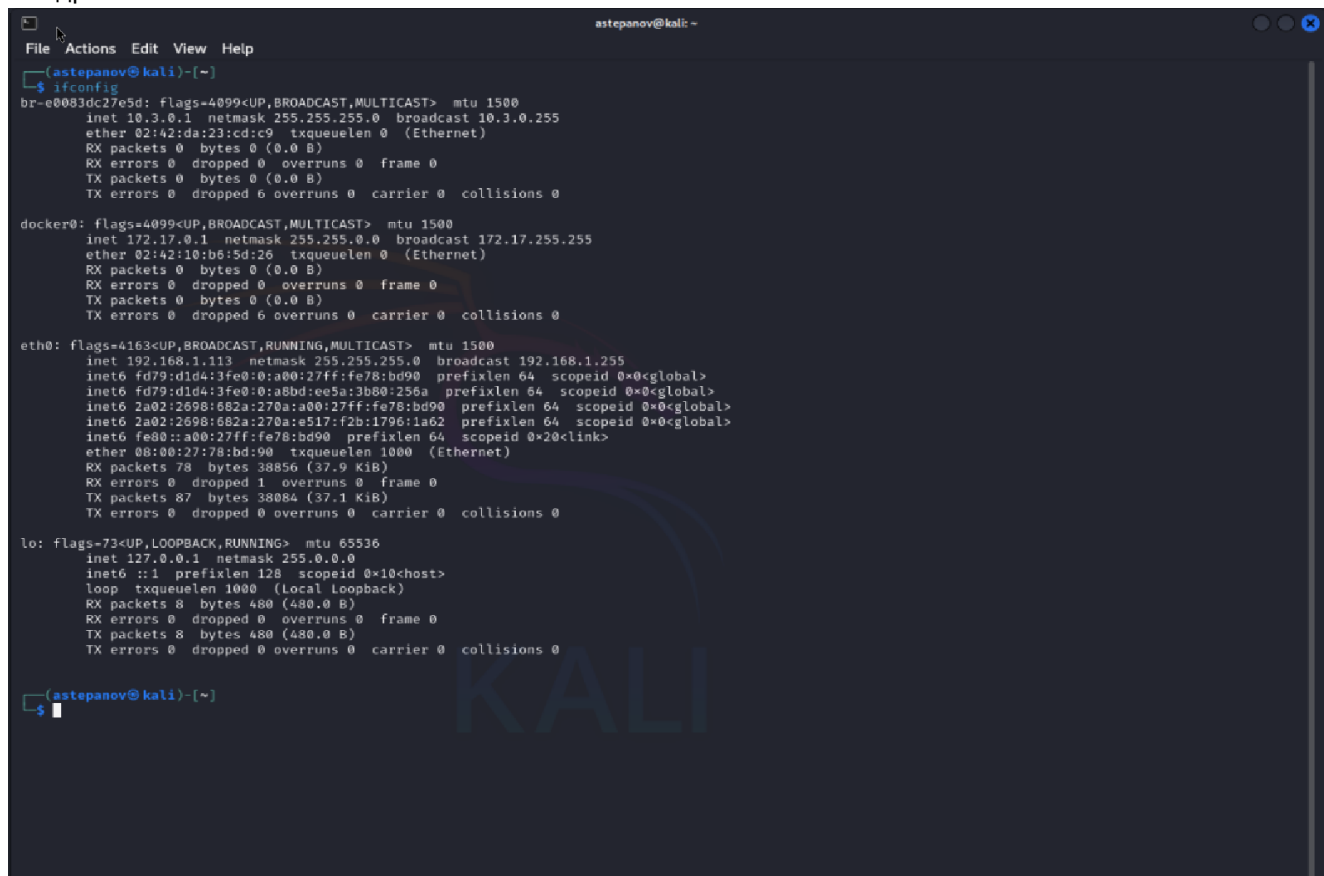


Шаг 3. Узнайте IP-адрес на двух машинах

## IP-адрес машины Windows - 192.168.1.103



## IP-адрес машины Kali Linux - 192.168.1.113



## Шаг 4. Исследуем доступность сети

С машины Windows

### TCP SYN Ping

The screenshot shows the Zenmap application window. The 'Target' field is set to '192.168.1.0/24'. The 'Command' field contains 'nmap -sn -PS80 192.168.1.0/24'. The 'Nmap Output' tab is selected, displaying the following text:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-17 00:26 Азербайджанское время (зима)
Nmap scan report for 192.168.1.1
Host is up (0.0057s 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 (0.090s latency).
MAC Address: BE:94:CC:81:0A:D4 (Unknown)
Nmap scan report for 192.168.1.72
Host is up (0.11s latency).
MAC Address: F4:FE:FB:32:25:E6 (Samsung Electronics)
Nmap scan report for 192.168.1.78
Host is up (0.078s latency).
MAC Address: 3C:06:30:4A:18:15 (Apple)
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 192.168.1.113
Host is up (0.0010s 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 (0.0040s 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 15.87 seconds
```

The Windows taskbar at the bottom shows the date and time as 17.03.2025 0:26.

## TCP ACK Ping

Zenmap

ScanToolsProfileHelp

Target: 192.168.1.0/24Profile: ScanCancel

Command: nmap -sn -PA80 192.168.1.0/24

HostsServices

Service

Filter Hosts

Nmap OutputPorts / HostsTopologyHost DetailsScans

nmap -sn -PA80 192.168.1.0/24Details

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-03-17 00:27 Азербайджанское время (зима)  
Nmap scan report for 192.168.1.1  
Host is up (0.0057s 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 (0.069s latency).  
**MAC Address:** CC:4B:73:EF:E4:6A (Ampak Technology)  
Nmap scan report for 192.168.1.61  
Host is up (0.081s latency).  
**MAC Address:** BE:94:CC:81:0A:D4 (Unknown)  
Nmap scan report for 192.168.1.72  
Host is up (0.092s latency).  
**MAC Address:** F4:FE:FB:32:25:E6 (Samsung Electronics)  
Nmap scan report for 192.168.1.78  
Host is up (0.068s latency).  
**MAC Address:** 3C:06:30:4A:18:15 (Apple)  
Nmap scan report for 192.168.1.104  
Host is up (0.080s 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 (0.0054s 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 (0.10s latency).  
**MAC Address:** 92:5F:4D:4B:0D:49 (Unknown)  
Nmap scan report for 192.168.1.103  
Host is up.  
**Nmap done:** 256 IP addresses (11 hosts up) scanned in 3.72 seconds

ENG

0:27

17.03.2025

## UDP Ping

Zenmap

Scan Tools Profile Help

Target: 192.168.1.0/24

Profile:

Scan Cancel

Command: nmap -sn -PU53 192.168.1.0/24

Hosts Services

Service

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sn -PU53 192.168.1.0/24

Details

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: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 (0.089s 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: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 3.01 seconds

0:28

ENG

17.03.2025

## ICMP Ping Types

Zenmap

Scan Tools Profile Help

Target: 192.168.1.0/24 Profile: 

Scan Cancel

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

Hosts Services

Service

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sn -PE -PM -PP 192.168.1.0/24 Details

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-03-17 00:29 Азербайджанское время (зима)  
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:** BK: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: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 2.56 seconds

ENG 

0:29

17.03.2025

## IP Protocol Ping

Zenmap

Scan Tools Profile Help

Target: 192.168.1.0/24

Profile:

Scan Cancel

Command: nmap -sn -PO 192.168.1.0/24

Hosts Services

Service

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sn -PO 192.168.1.0/24

Details

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-03-17 00:29 Азербайджанское время (зима)  
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:06:30:4A: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

0:29

ENG

17.03.2025



## Обычный ping-скан

Zenmap

Scan Tools Profile Help

Target: 192.168.1.0/24 Profile: Scan Cancel

Command: nmap -sn 192.168.1.0/24

Hosts Services

Service

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sn 192.168.1.0/24 Details

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-03-17 00:30 Азербайджанское время (зима)

Nmap scan report for 192.168.1.1  
Host is up (0.0057s latency).  
**MAC Address:** 50:FF:20:D4:DE:47 (Keenetic Limited)

Nmap scan report for 192.168.1.37  
Host is up (0.14s latency).  
**MAC Address:** 84:25:19:34:30:6C (Samsung Electronics)

Nmap scan report for 192.168.1.43  
Host is up (0.14s 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 (0.12s latency).  
**MAC Address:** F4:FE:FB:32:25:E6 (Samsung Electronics)

Nmap scan report for 192.168.1.78  
Host is up (0.094s latency).  
**MAC Address:** 3C:06:30:4A:18:15 (Apple)

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 192.168.1.113  
Host is up (0.0050s 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 (0.0064s 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 (0.10s latency).  
**MAC Address:** 92:5F:4D:4B:0D:49 (Unknown)

Nmap scan report for 192.168.1.139  
Host is up (0.043s latency).  
**MAC Address:** 16:GD:6D:D0:FG:C9 (Unknown)

Filter Hosts

0:30 17.03.2025

С машины Kali Linux

TCP SYN Ping

```
astepanov@kali: ~  
File Actions Edit View Help  
  
(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 192.168.1.78
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 -PO 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

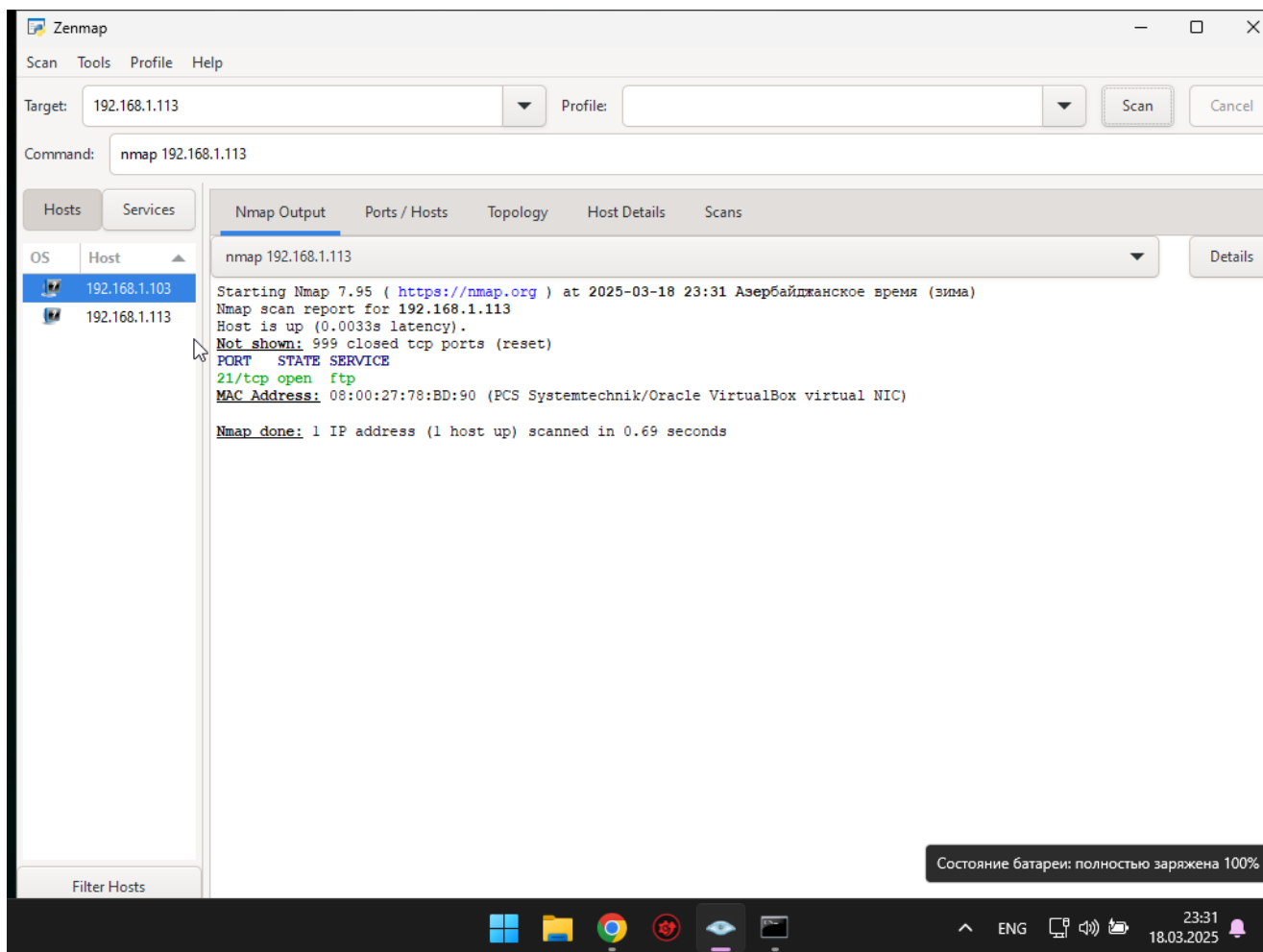
```
(astepanov@kali)-[~]
$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 16:39 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0035s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.16s latency).
MAC Address: 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
<b>TCP SYN Ping</b>	Отправляет SYN на порт (обычно 80), ждет SYN/ACK	Определяет хосты с открытым портом 80	Средняя скорость, зависит от количества открытых портов
<b>TCP ACK Ping</b>	Отправляет ACK, ждет RST	Полезно для обхода фильтров, определяет активные хосты за брандмауэрами	Средняя, но может быть быстрее, чем SYN Ping, в некоторых случаях
<b>UDP Ping</b>	Отправляет UDP-пакет (обычно 53), ждет ICMP Port Unreachable	Хорошо работает, если ICMP не фильтруется	Медленнее, чем TCP, из-за необходимости ожидания ICMP
<b>ICMP Ping Types</b>	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
<b>IP Protocol Ping</b>	Использует нестандартные IP-протоколы (GRE, ESP, AH)	Полезно против фильтрации ICMP и TCP	Медленное выполнение, так как использует нестандартные протоколы
<b>Обычный -sn</b>	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

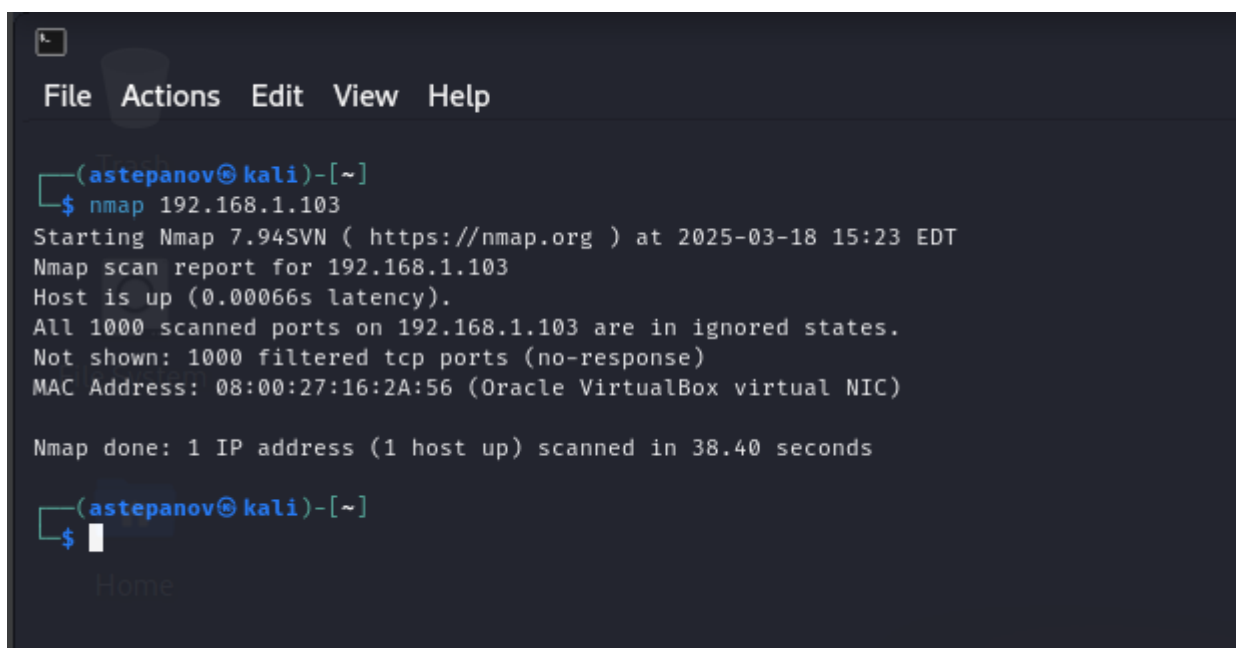
#### Сканирование с Windows



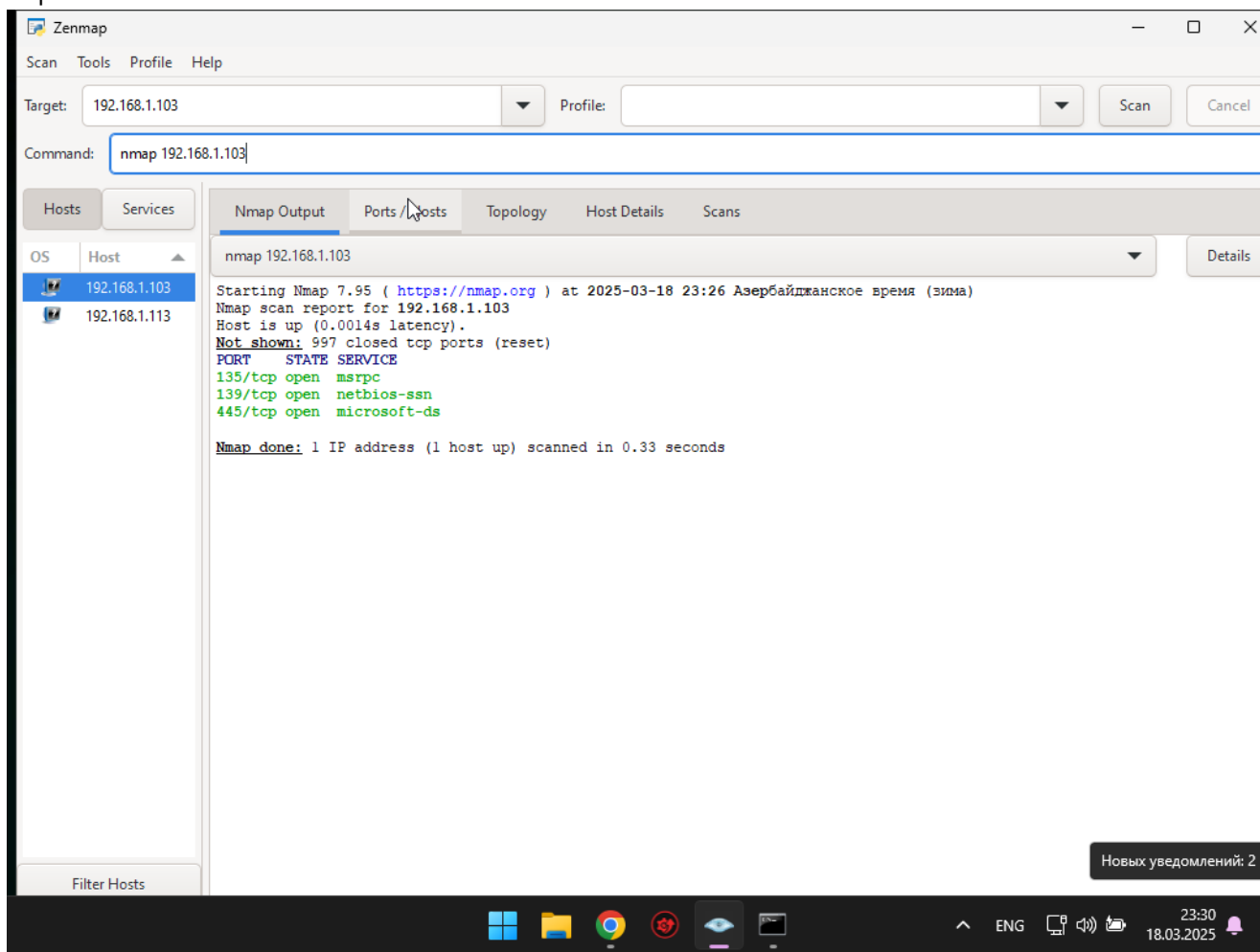
Видим, что на хосте Kali открыт 21-ый порт, порт управляющего соединения FTP, который был открыт в рамках предыдущей ЛР

## Сканирование с Kali Linux

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

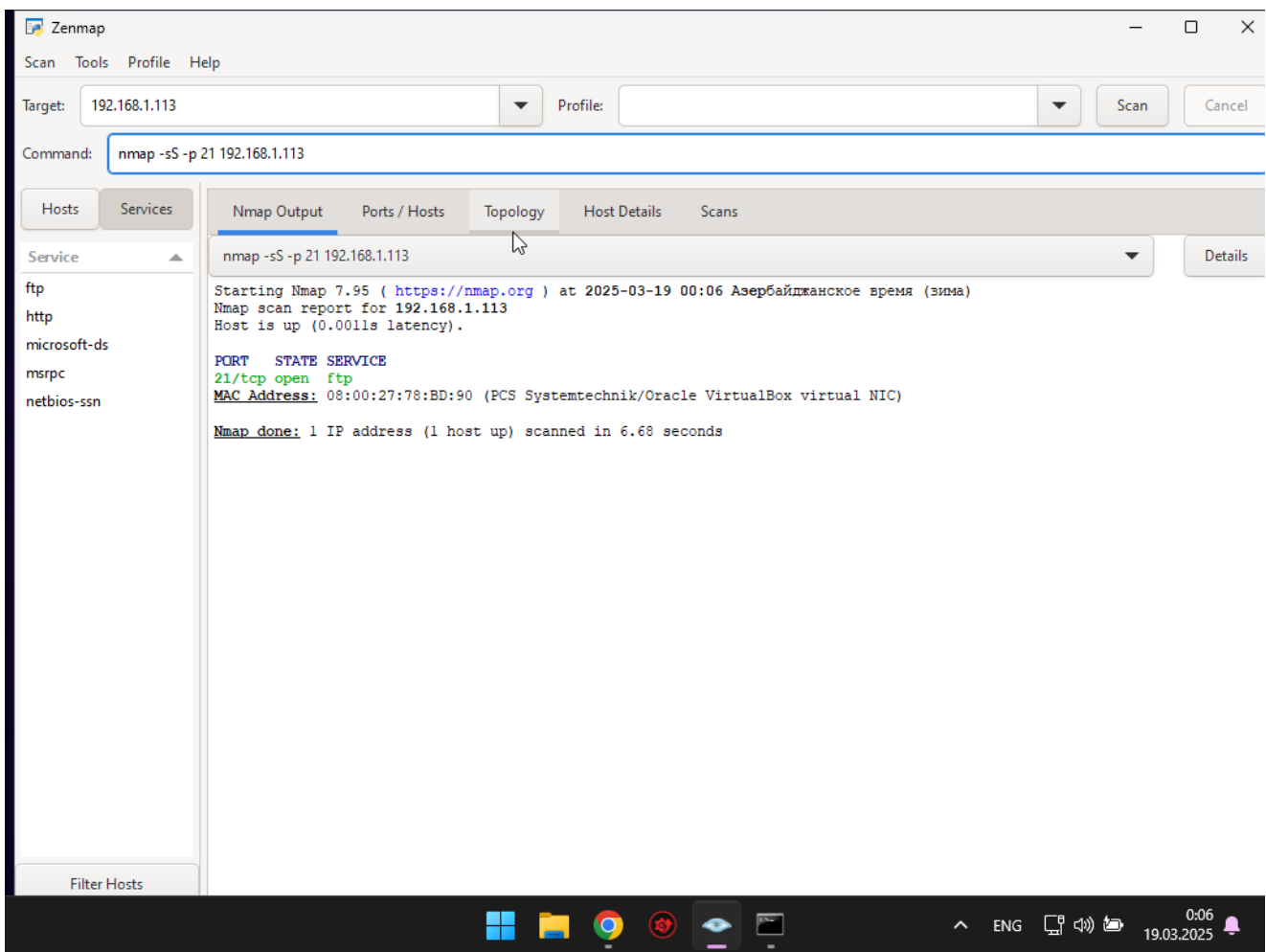


Хотя если Windows-хост будет сканировать сам себя, то результат покажет наличие открытых tcp-портов:



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.

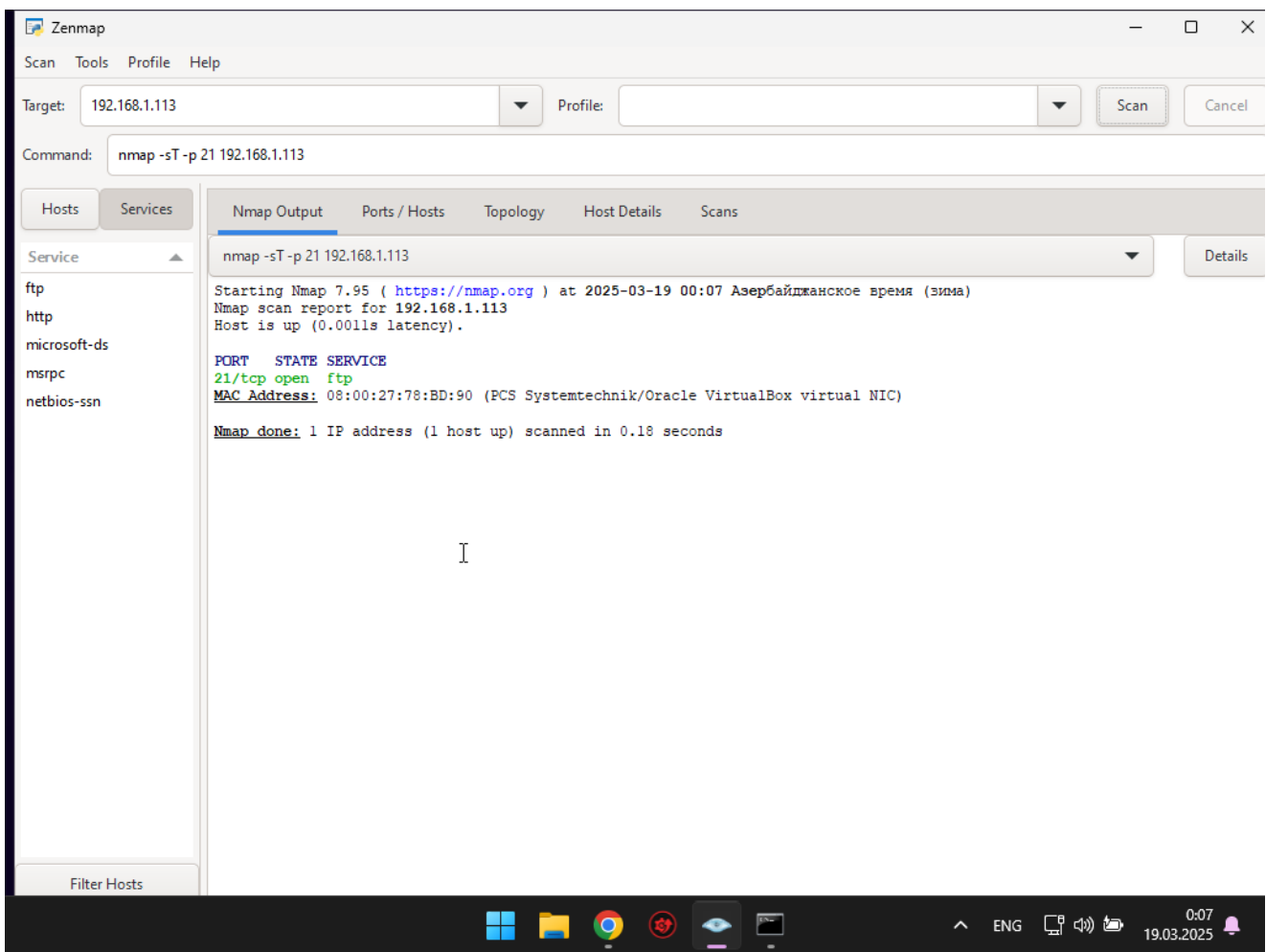
### TCP SYN Scan



Порт открыт

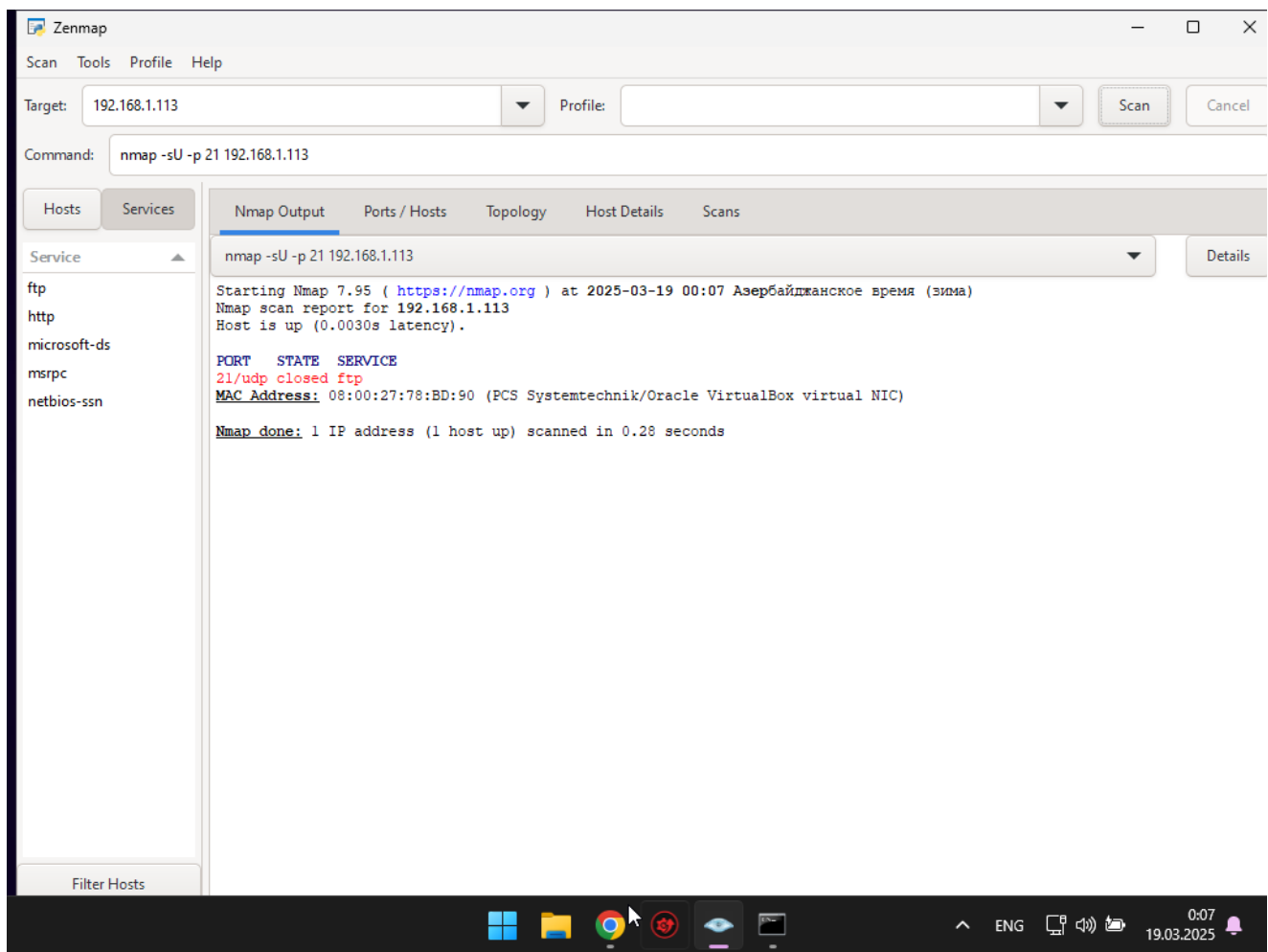
**TCP Connect Scan**





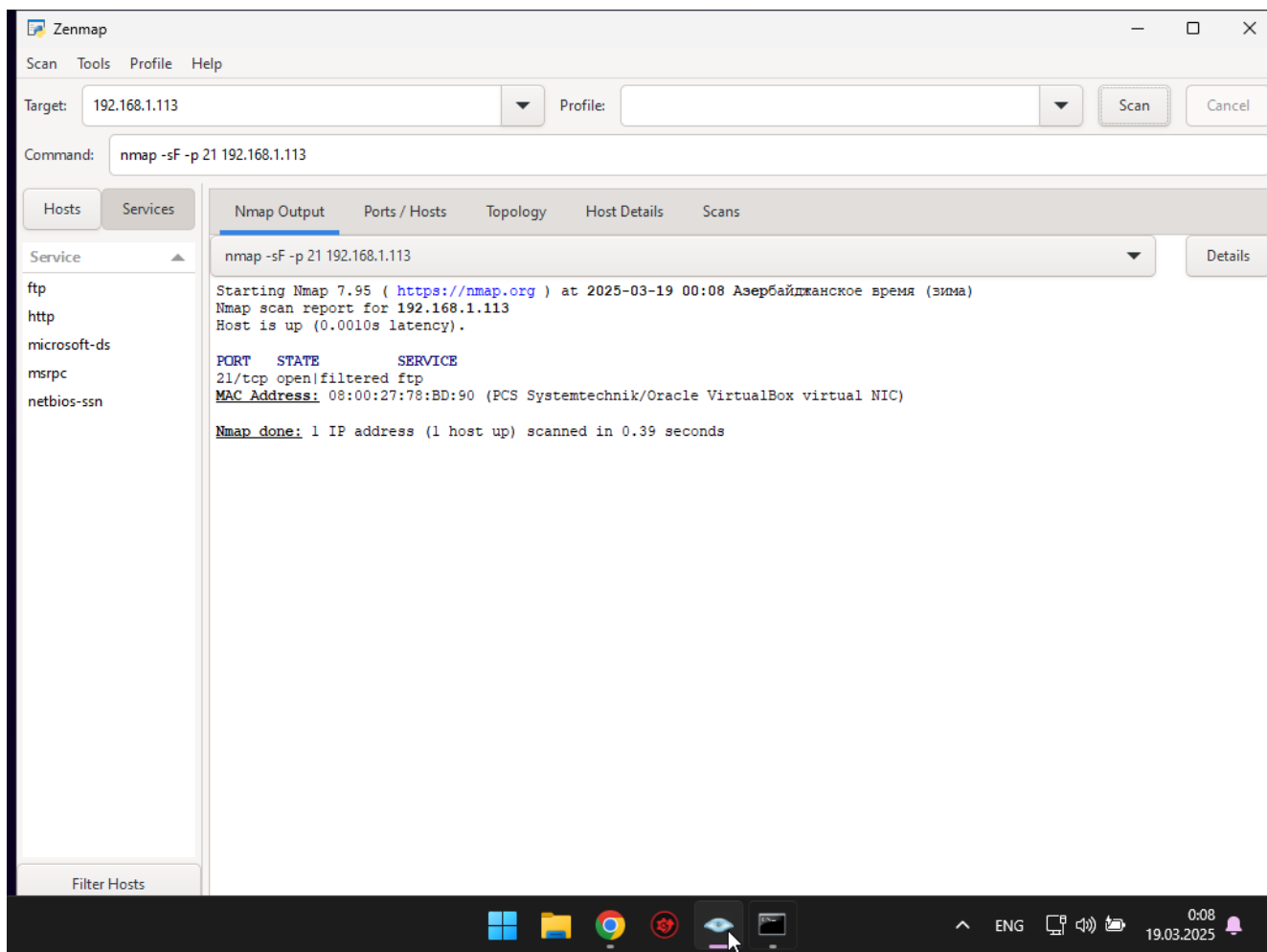
Порт открыт

**UDP Scan**



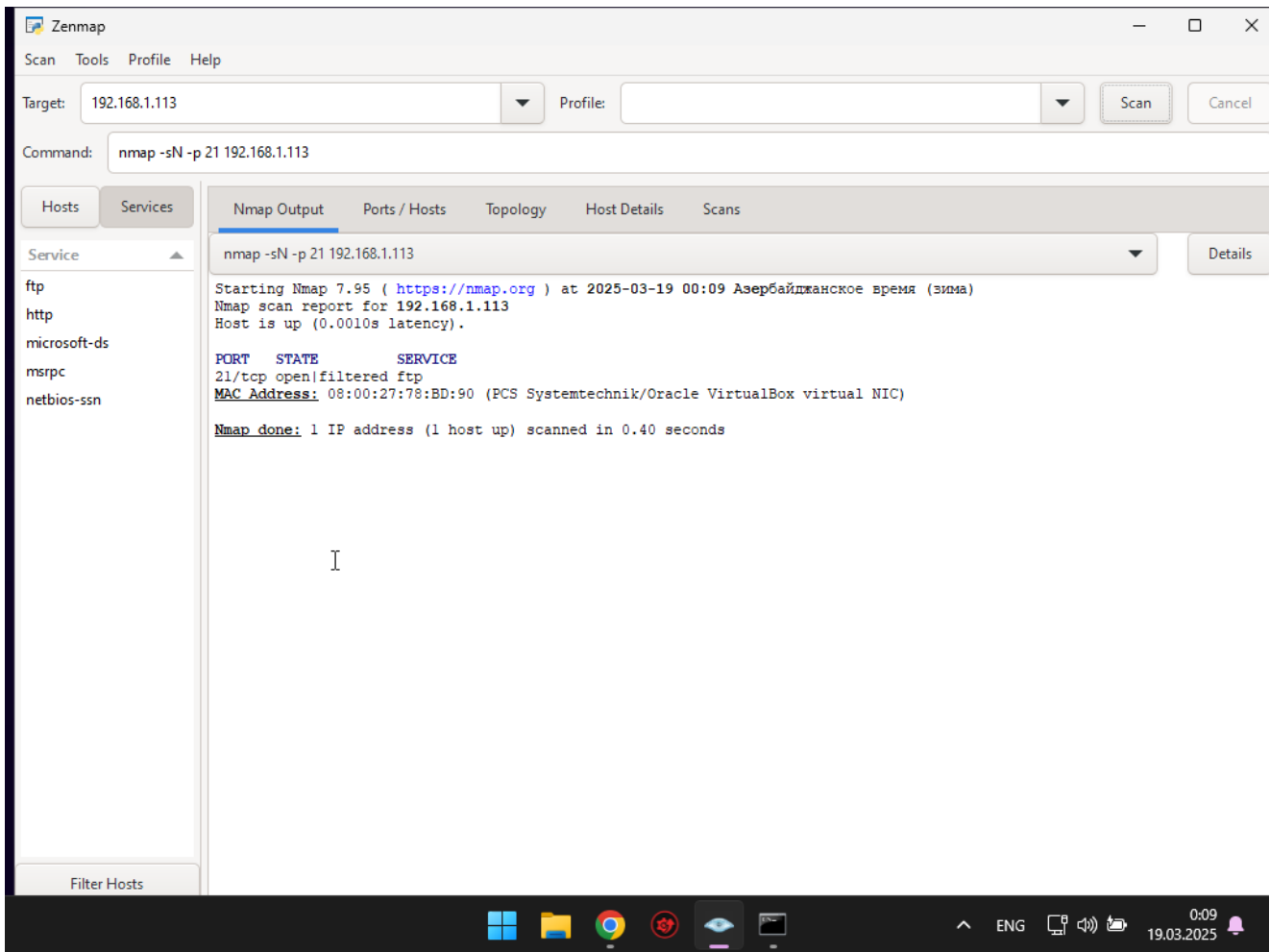
Порт закрыт. Видимо, потому что это не UDP порт

## TCP FIN Scan



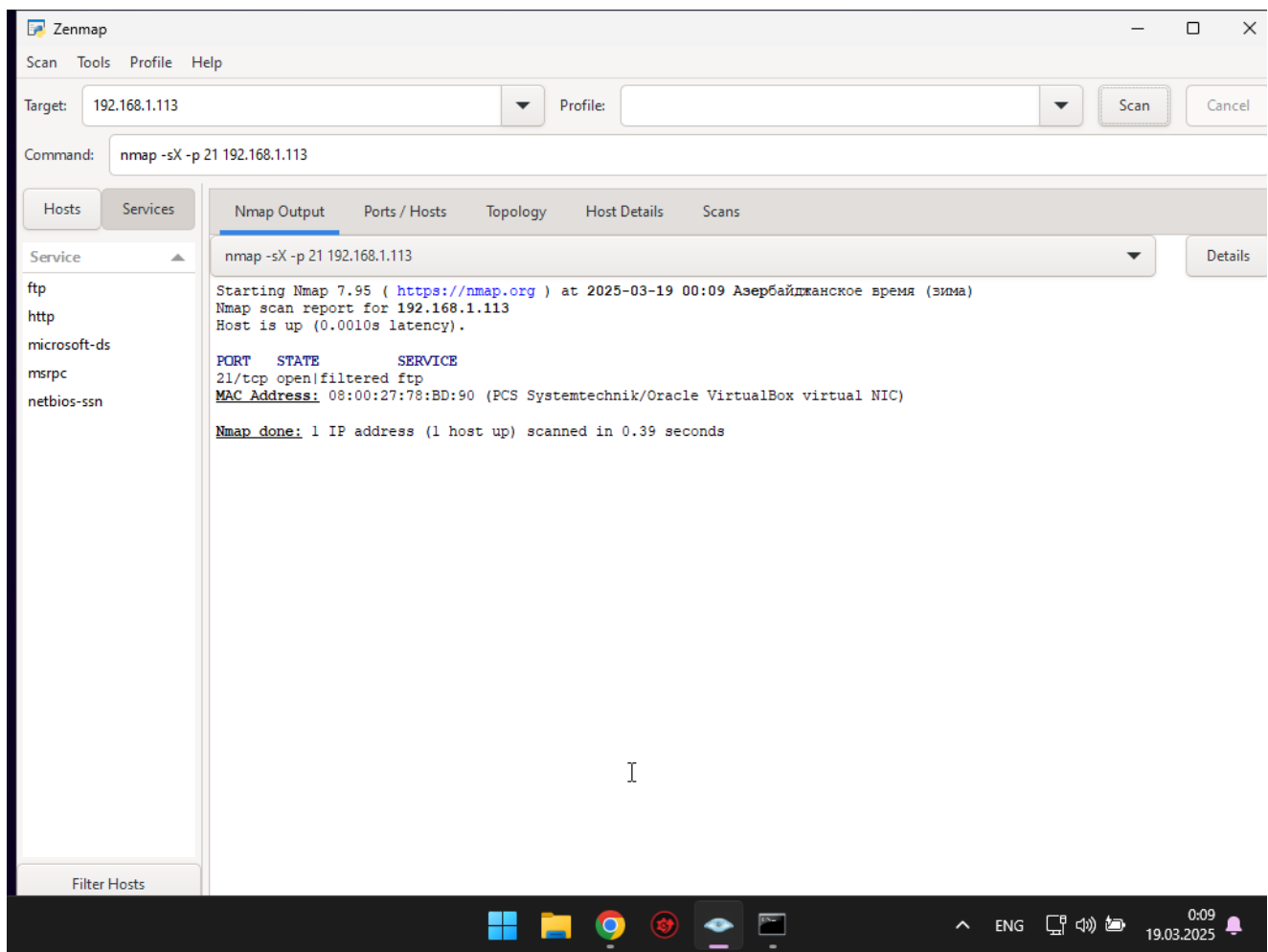
Порт открыт и не отвечает на нестандартные TCP-пакеты.

## TCP NULL Scan



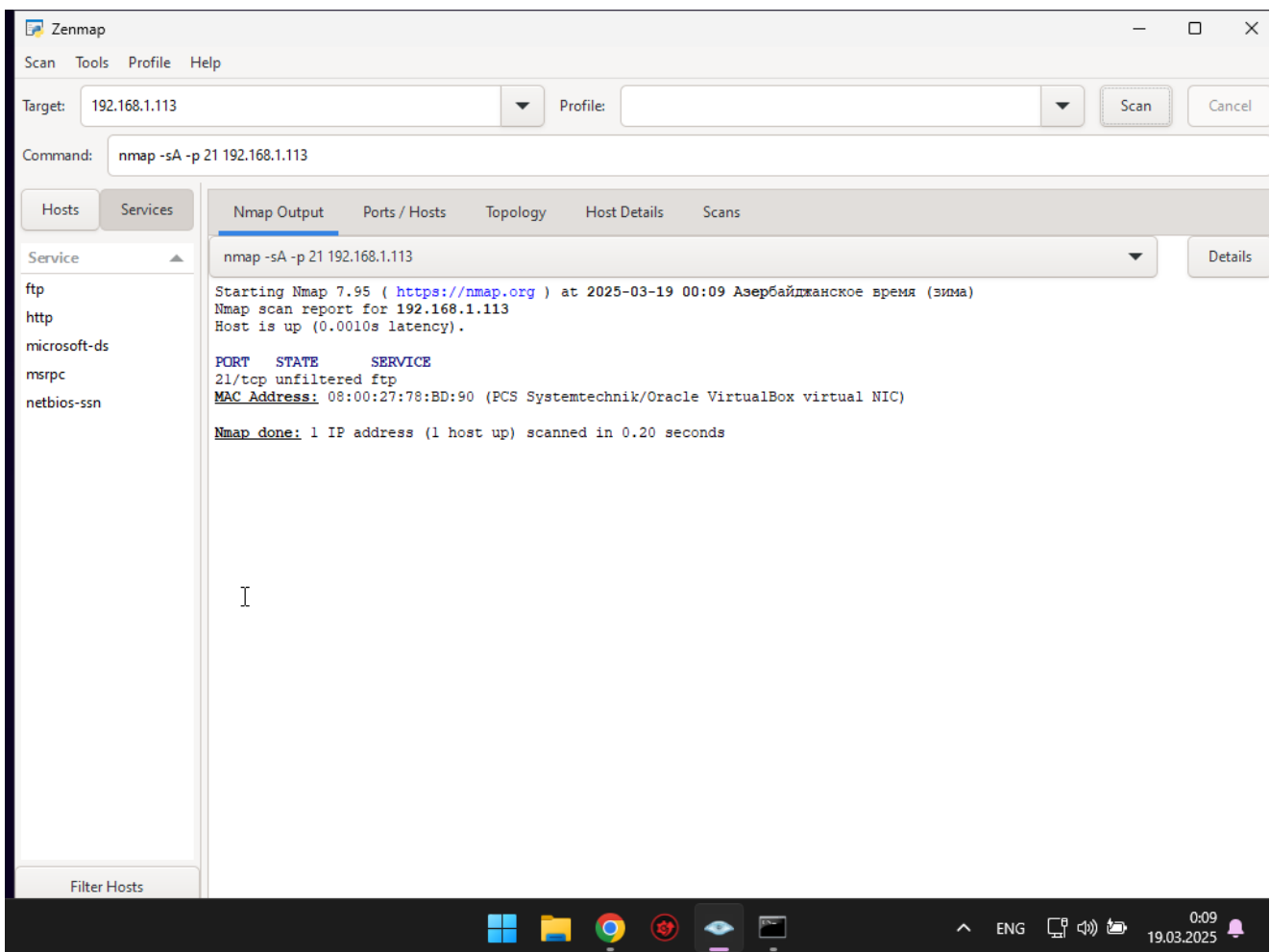
Порт открыт и не отвечает на нестандартные TCP-пакеты.

## TCP Xmas Scan



Порт открыт и не отвечает на нестандартные TCP-пакеты.

## TCP ACK Scan



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

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

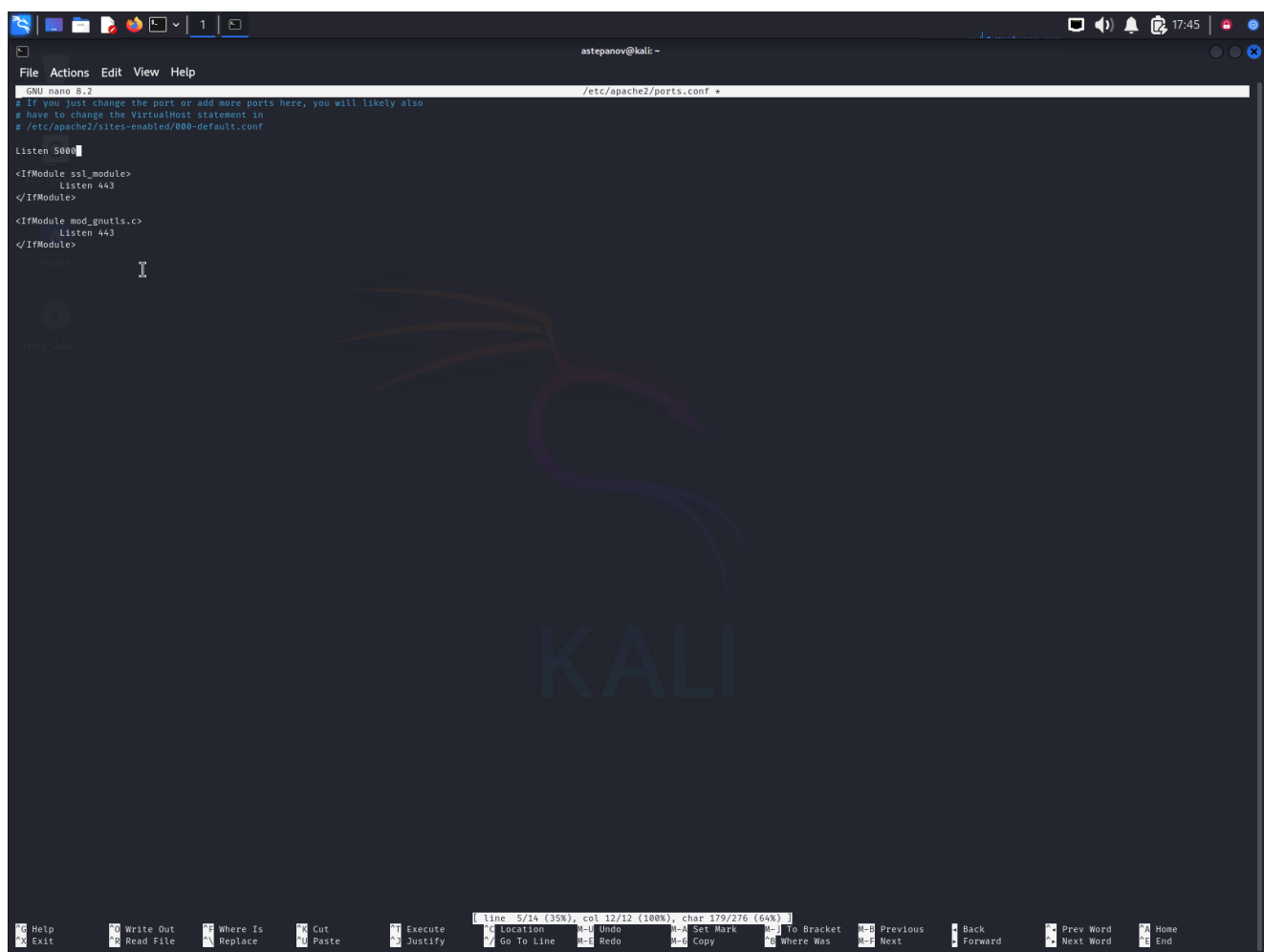
```
File Actions Edit View Help

(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)-[~]
```

Шаг 8. Настройка и запуск веб-сервера Apache2

**Прописываем слушать 5000 порт в конфиге**



```
GNU nano 8.2 /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>
```

line 5/14 (35%), col 12/12 (100%), char 179/276 (64%)

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

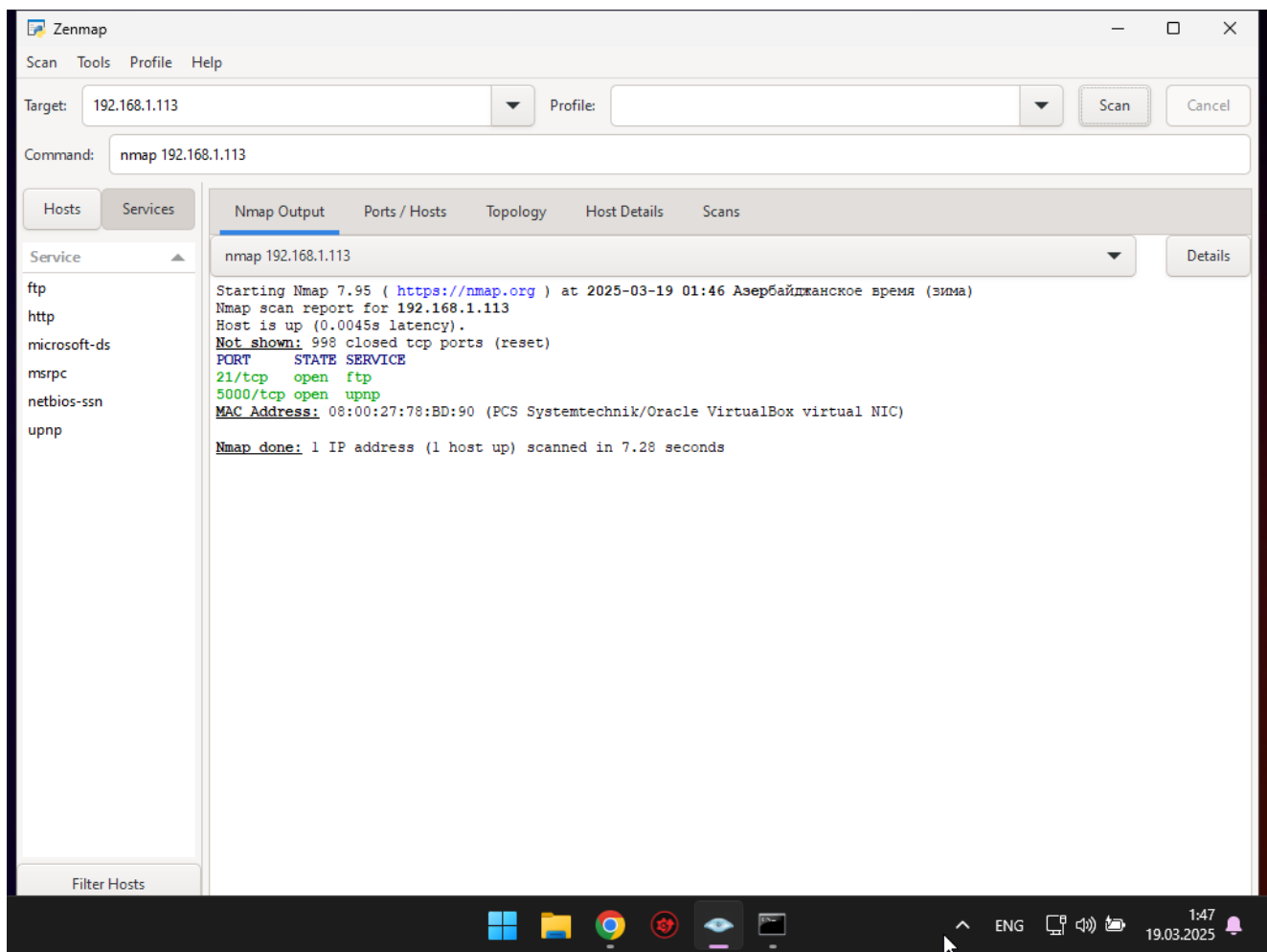
Перезапускаем сервер для того, чтобы подхватился конфиг

```
astepanov@kali: ~  
File Actions Edit View Help  
[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: 8888ecf95742483cbd4c27a8eb10e60f  
    Docs: https://httpd.apache.org/docs/2.4/  
  Process: 25533 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)  
 Main PID: 25537 (apache2)  
   Tasks: 6 (limit: 4555)  
  Memory: 20.2M (peak: 21M)  
    CPU: 144ms  
   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: 8888ecf95742483cbd4c27a8eb10e60f  
    Docs: https://httpd.apache.org/docs/2.4/  
  Main PID: 25537 (apache2)  
   Tasks: 6 (limit: 4555)  
  Memory: 20.2M (peak: 21M)  
    CPU: 146ms  
   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?

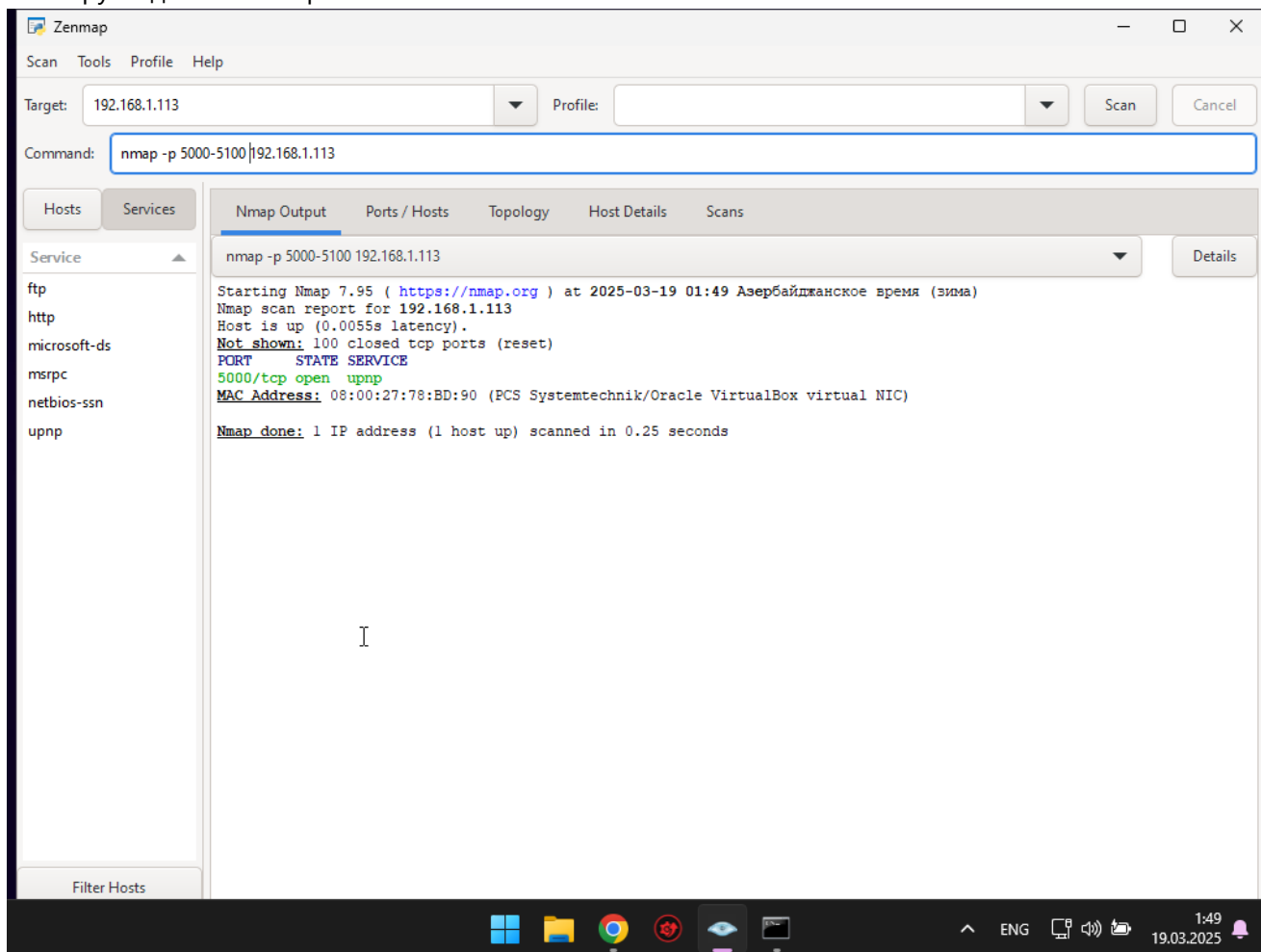
После того, как на Kali был поднят Apache веб-сервер, видим что 5000-ый порт появился в результатах сканирования...





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)

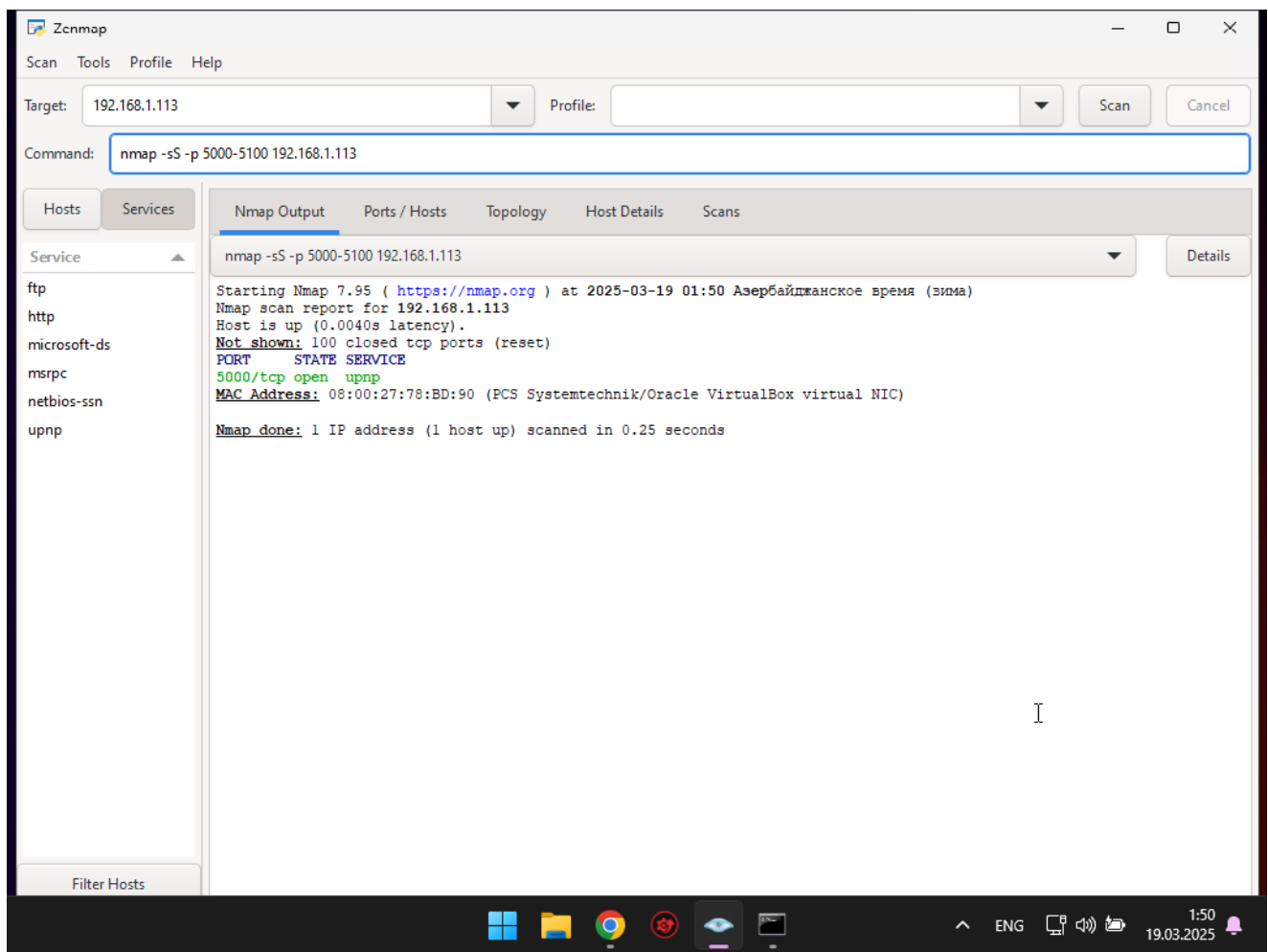
## Сканируем диапазон портов 5000-5100



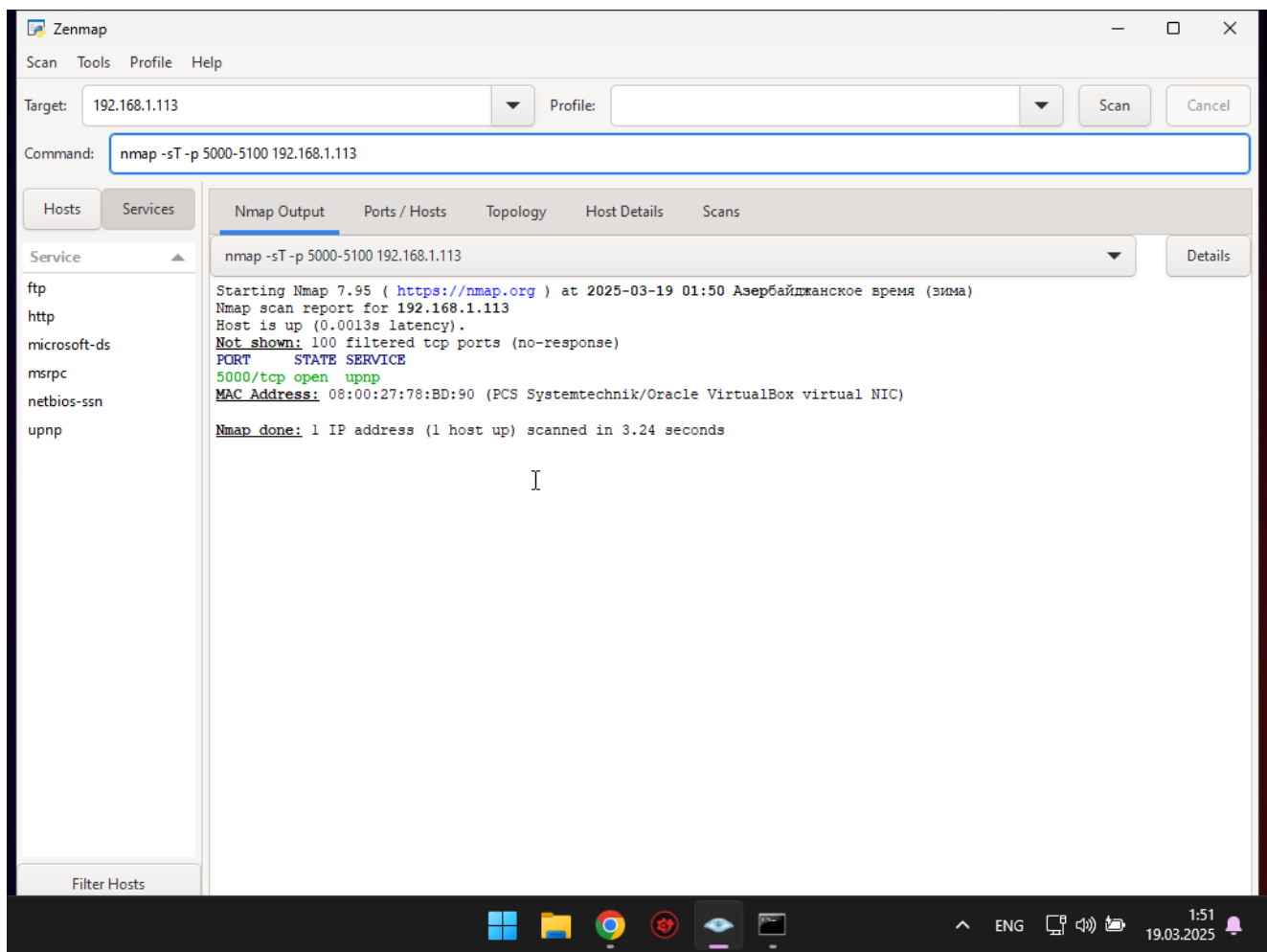
В общем-то, результат довольно очевидный - видим открытый 5000-ый порт

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

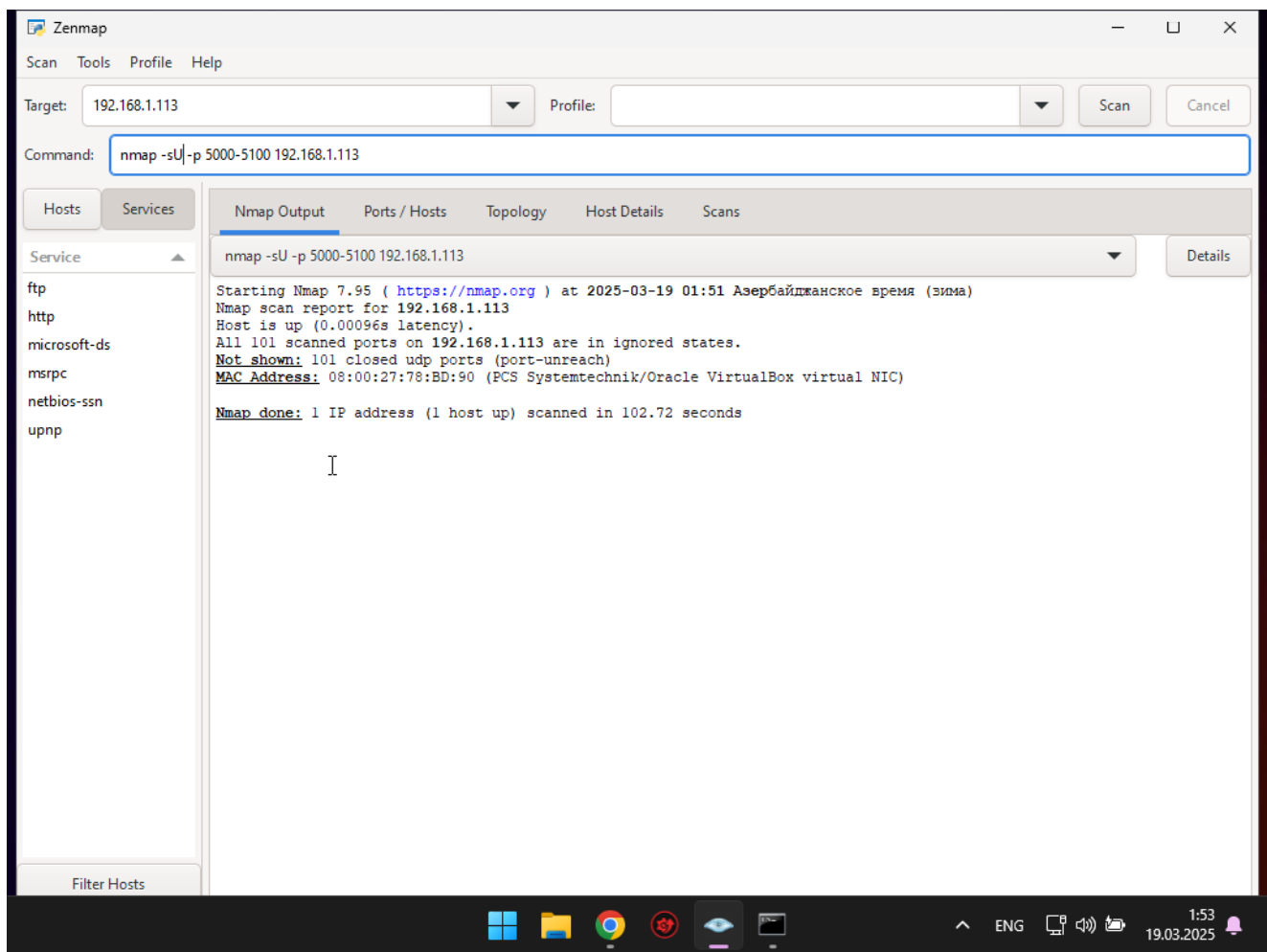
### TCP SYN Scan



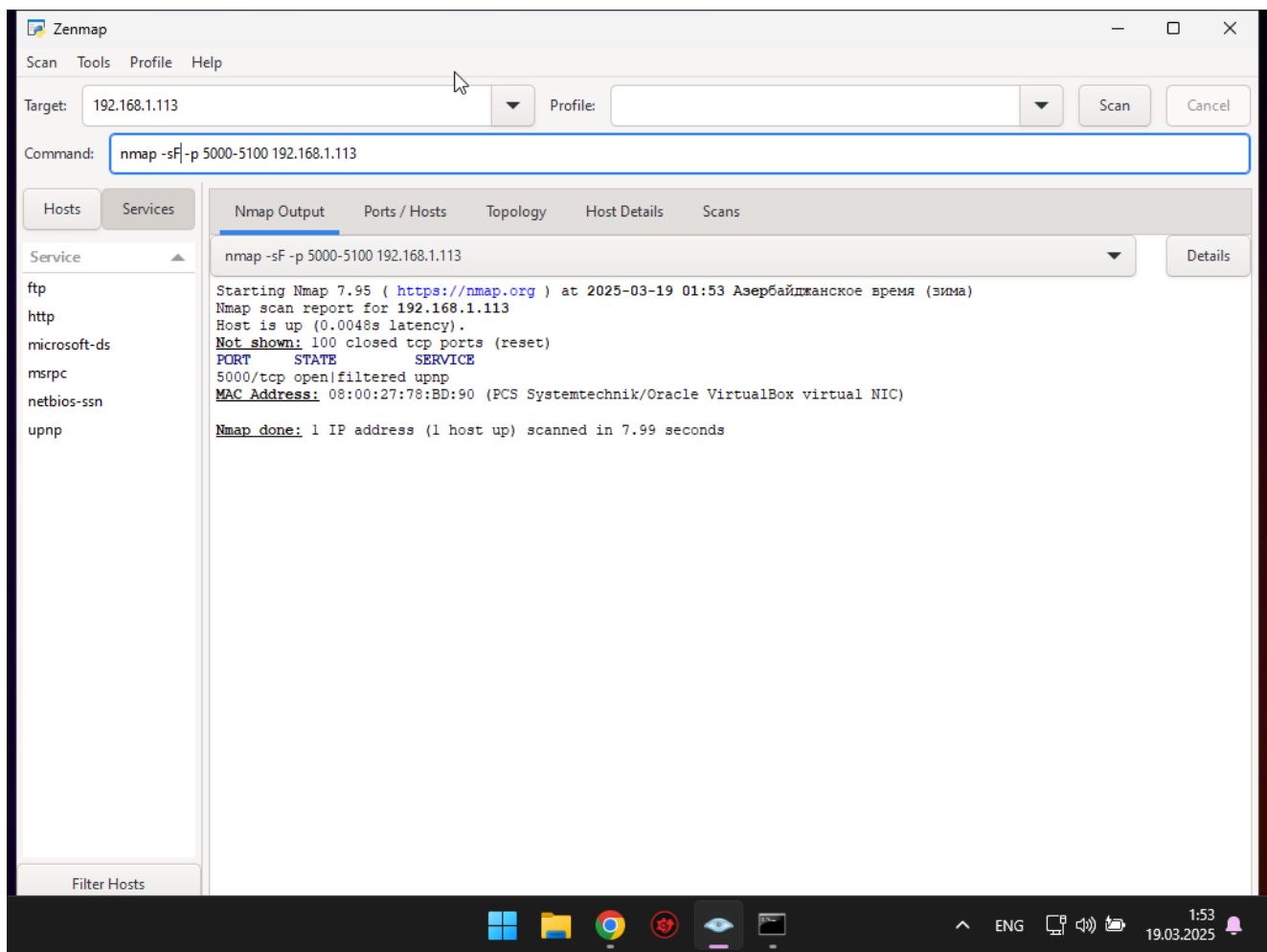
## TCP Connect Scan



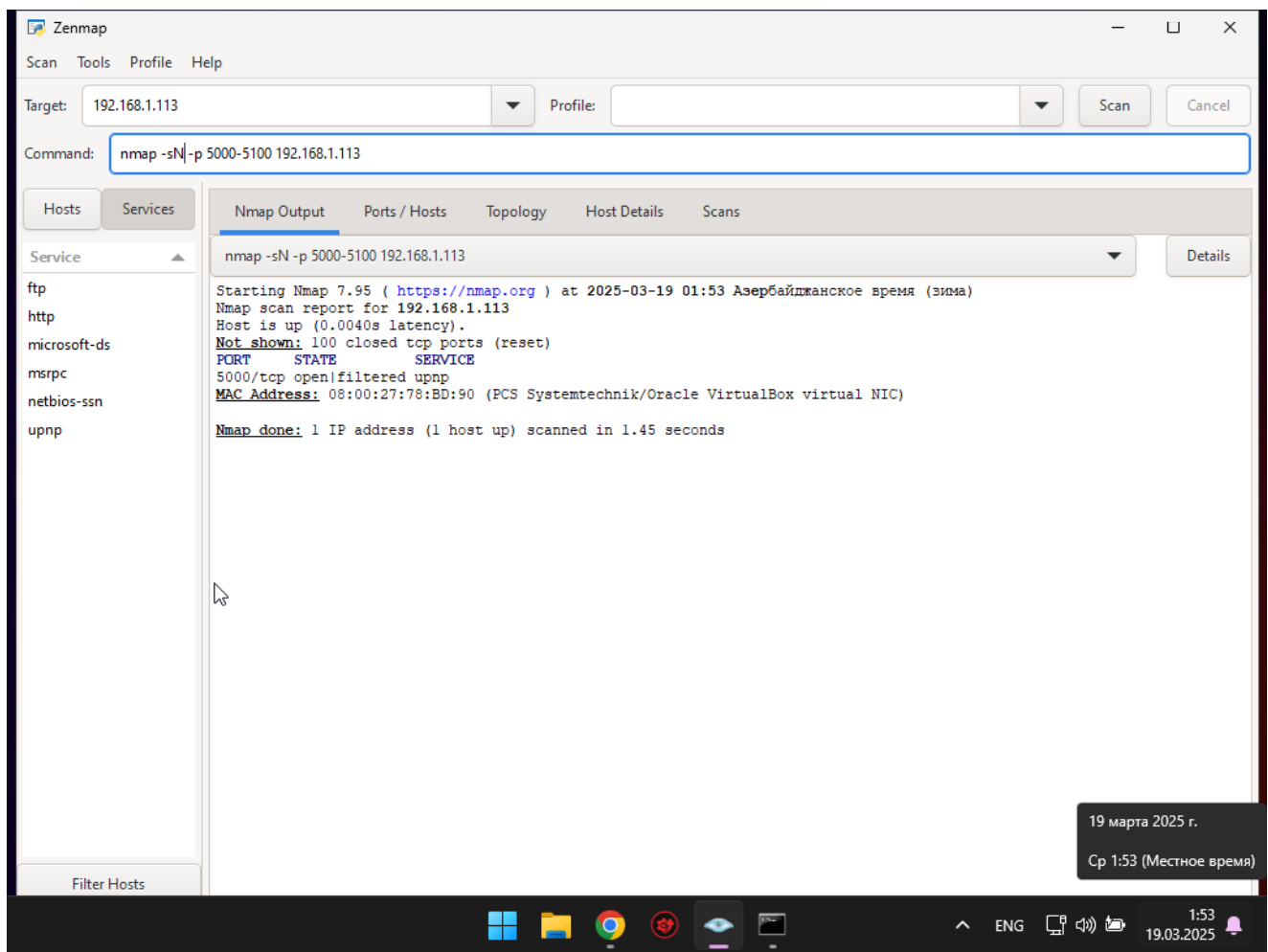
## UDP Scan



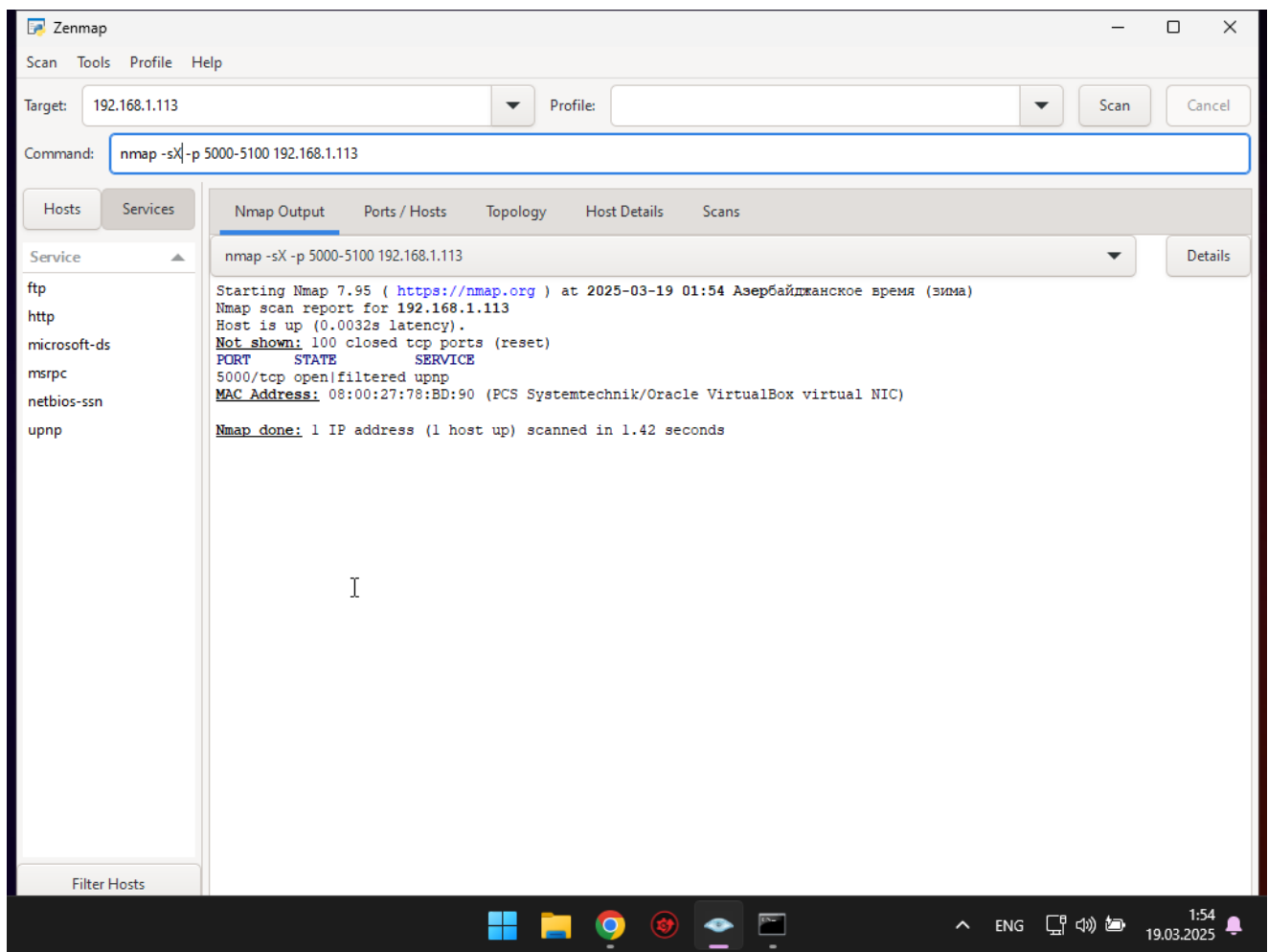
## TCP FIN Scan



## TCP NULL Scan

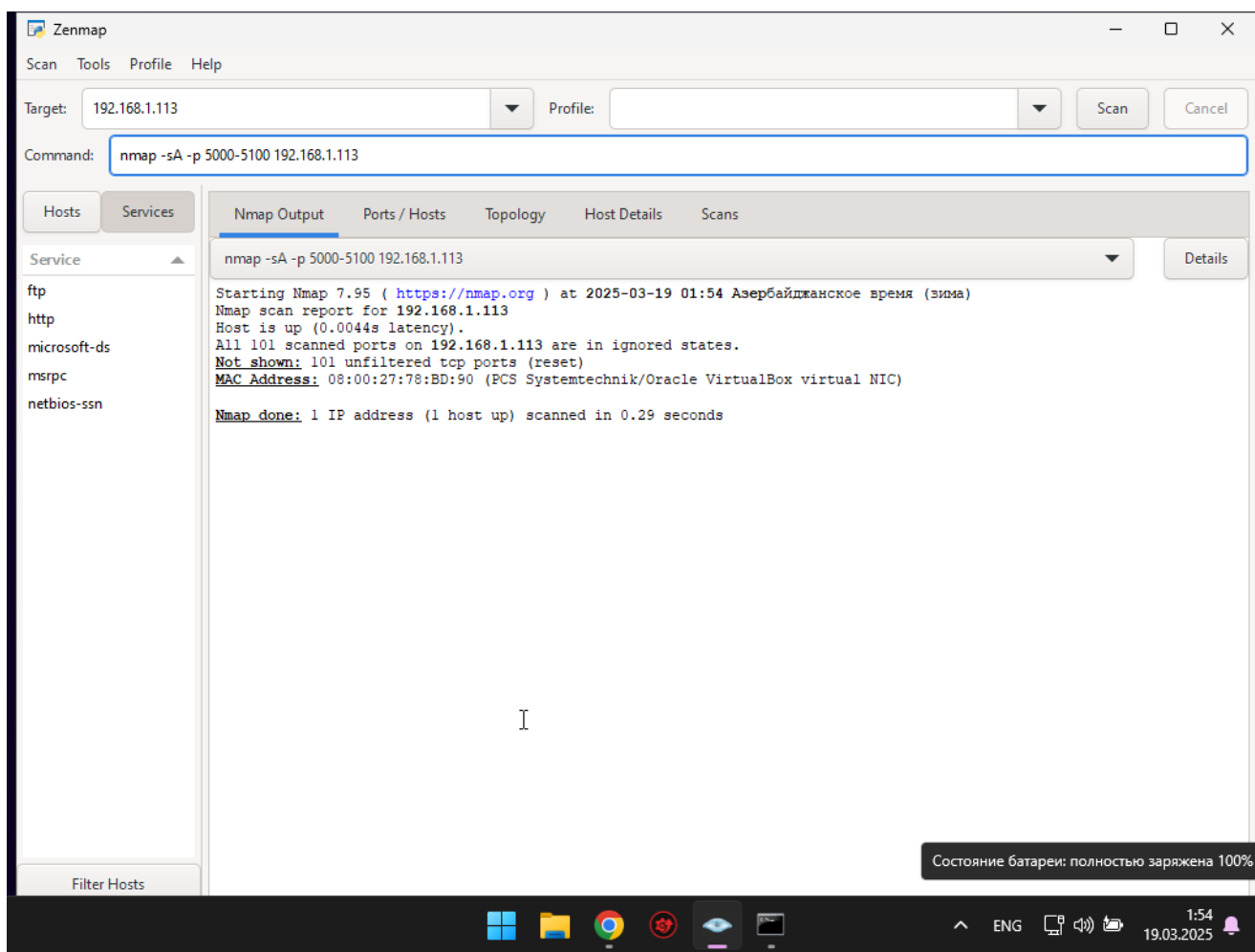


## TCP Xmas Scan



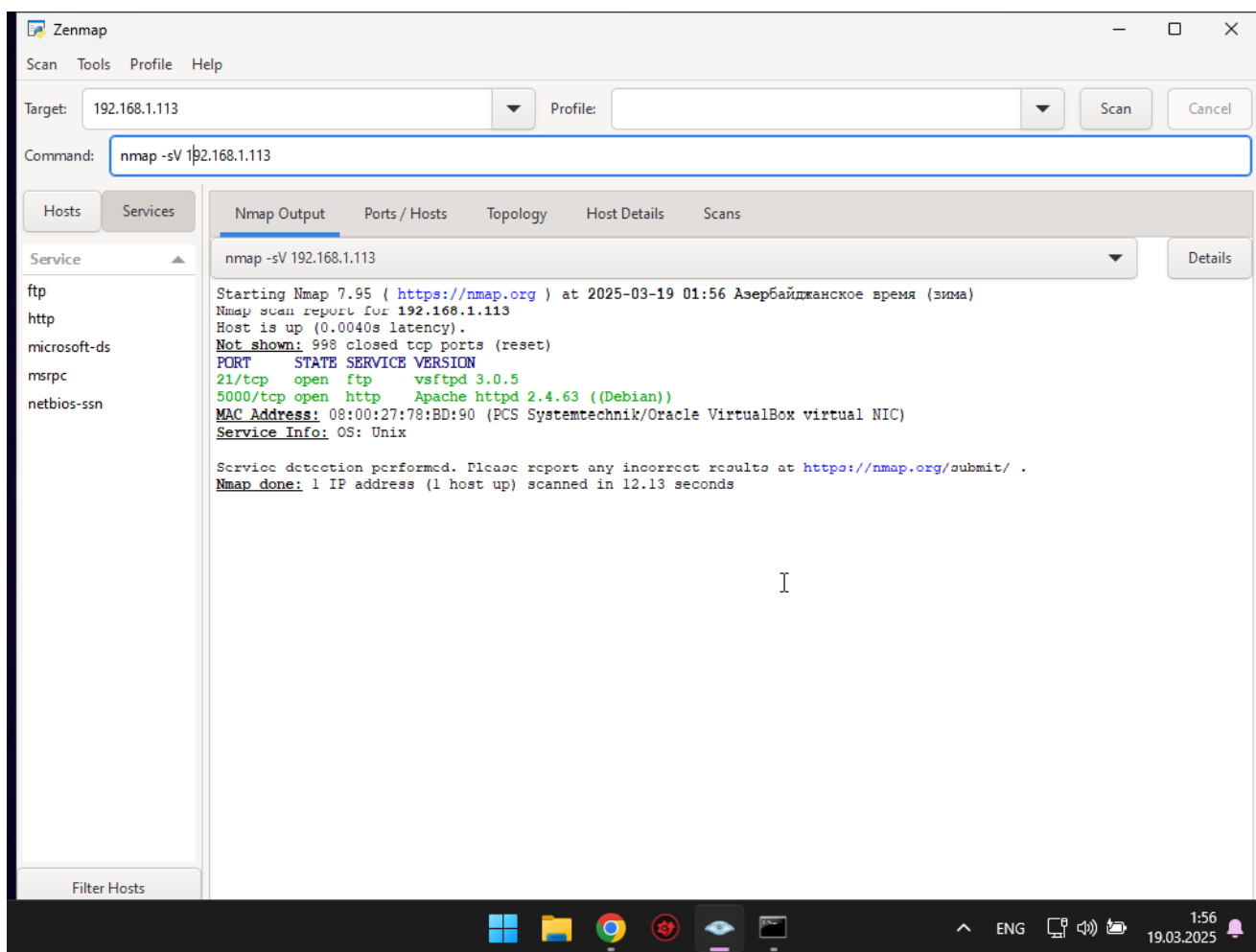
## TCP ACK Scan





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`

```
astepanov@kali: ~
File Actions Edit View Help

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

astepanov@kali:~$ psql --v
/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, --set=, --variable=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
-l ('one'), --single-transaction
                           execute as a single transaction (if non-interactive)
-?, --help[=options]      show this help, then exit
--help=commands           list backslash commands, then exit
--help=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-queries         echo commands 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
-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, --tuples-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
-Z, --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)

```
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 psql
Failed to start psql.service: Unit psql.service not found.

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

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

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

(astepanov@kali)-[~]
└─$ psql --version
Command 'psql' not found, did you mean:
  command 'pl' from deb gnustep-base-runtime
  command 'sql' from deb parallel
  command 'psql' from deb postgresql-client-common
  command 'pil' from deb picolisp
  command 'pdl' from deb pdl
  command 'pal' from deb pal
  command 'pst' from deb pst
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

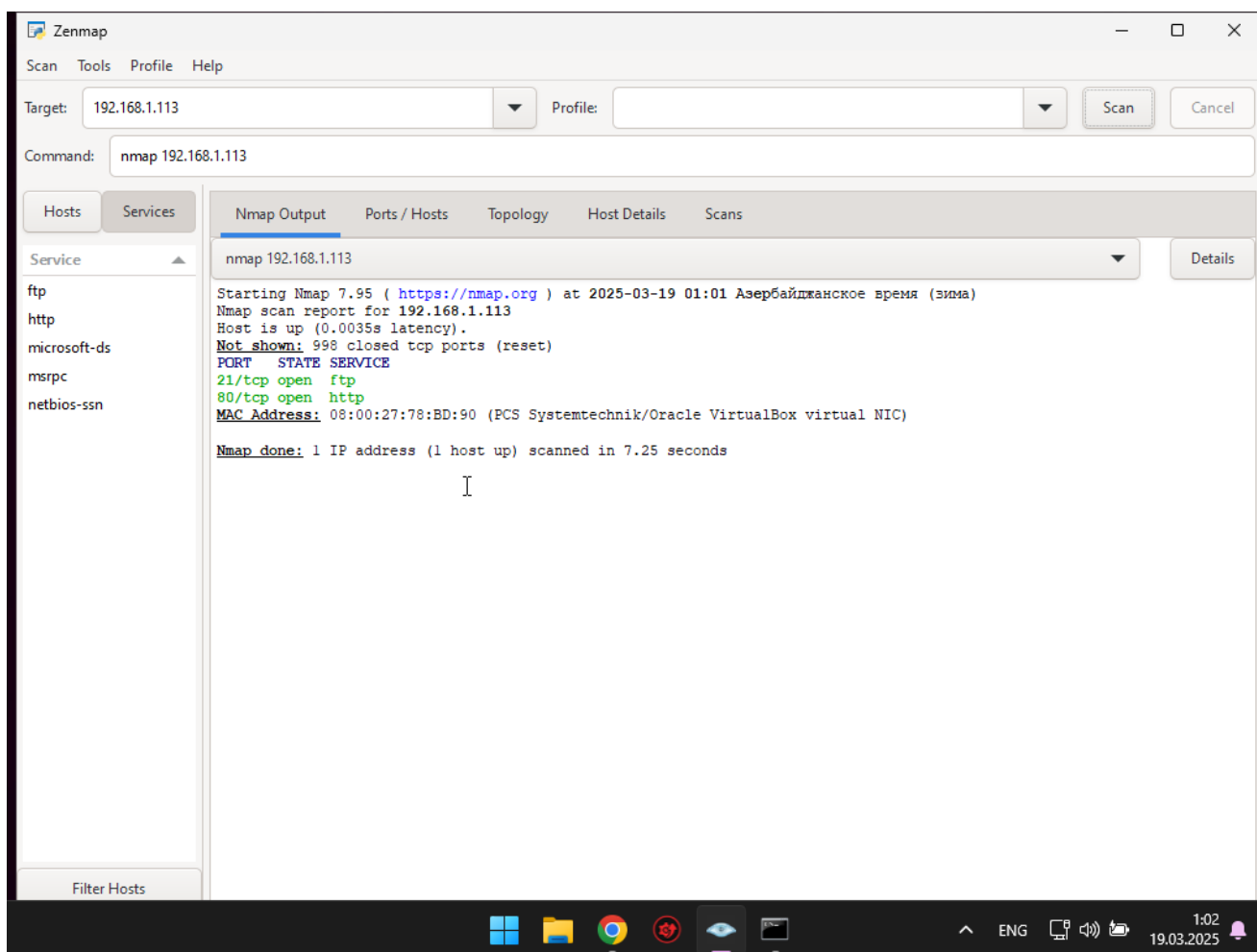
(astepanov@kali)-[~]
└─$ sudo systemctl status postgresql
● postgresql.service - PostgreSQL RDDBMS
   Loaded: loaded (/usr/lib/systemd/system/postgresql.service; disabled; preset: disabled)
   Active: active (exited) since Tue 2025-03-18 16:42:04 EDT; 5s ago
  Invocation: fcdee0043be48f88cc2bd245e4f73e6
    Process: 87783 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 87783 (code=exited, status=0/SUCCESS)
    Mem peak: 1.6M
       CPU: 11ms

Mar 18 16:42:04 kali systemd[1]: Starting postgresql.service - PostgreSQL RDDBMS ...
Mar 18 16:42:04 kali systemd[1]: Finished postgresql.service - PostgreSQL RDDBMS.

(astepanov@kali)-[~]
└─$
```

Запускаем сервис postgresql

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

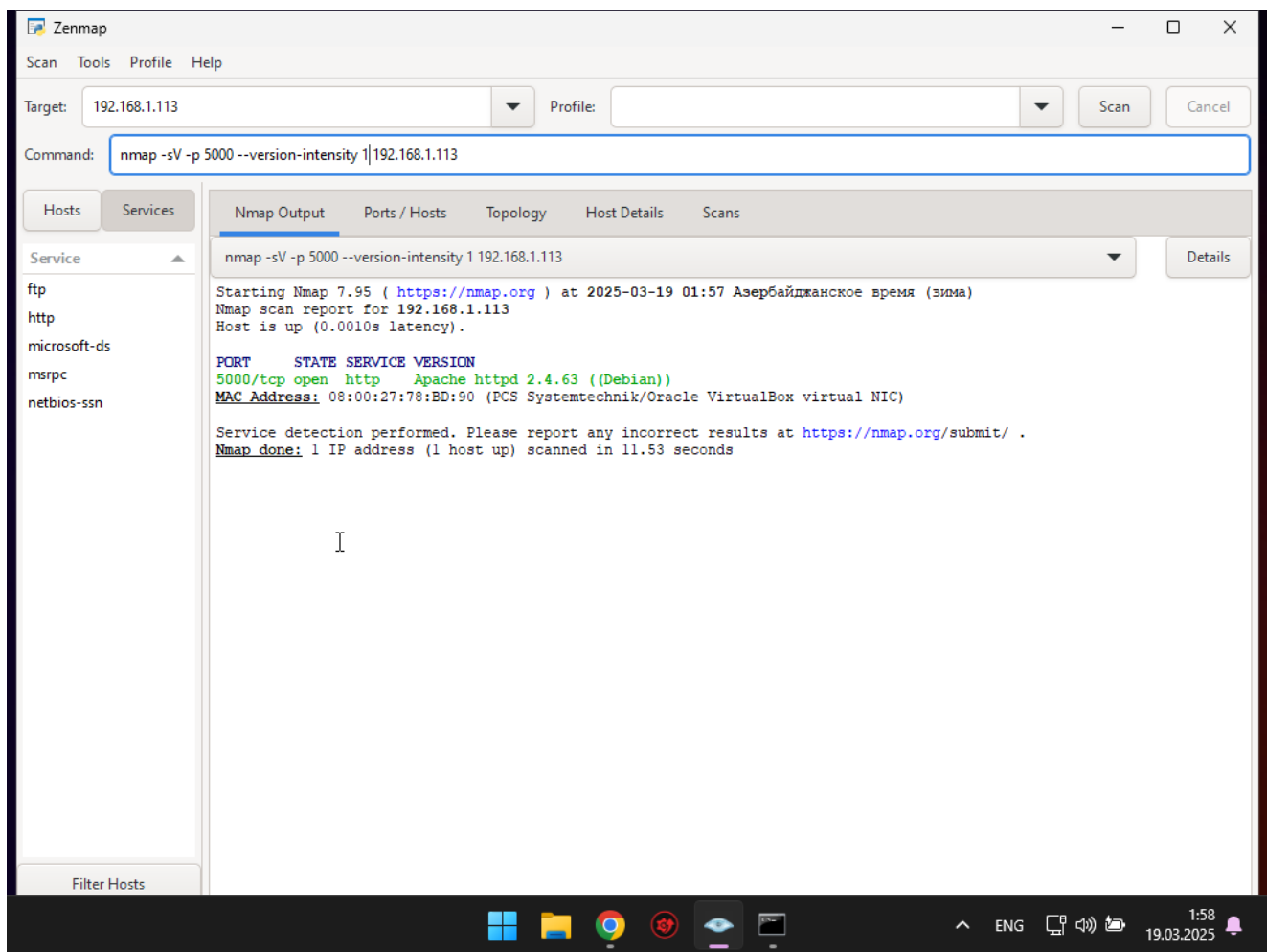


Результат сканирования не изменился. Видимо в задании предполагалось, что после запуска сервиса pgsql должен появиться порт pg, однако это требует дополнительной настройки сервиса, т.к. по умолчанию pg слушает только localhost.

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 не настроен и его порт не виден результаты отражены для порта 5000

### Интенсивность 1



## Интенсивность 2

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113 Profile: Scan Cancel

Command: nmap -sV -p 5000 --version-intensity 2 192.168.1.113

Hosts Services

Service

ftp  
http  
microsoft-ds  
msrpc  
netbios-ssn

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV -p 5000 --version-intensity 2 192.168.1.113

Details

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-03-19 01:59 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 18.04 seconds

Английский (США)  
США

Чтобы переключить методы ввода, нажмите клавиши  
WINDOWS+ПРОБЕЛ.

ENG

2:00  
19.03.2025

## Интенсивность 3

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113 Profile: Scan Cancel

Command: `nmap -sV -p 5000 --version-intensity 3 192.168.1.113`

Hosts Services

Service

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

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV -p 5000 --version-intensity 3 192.168.1.113 Details

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-03-19 02:00 Азербайджанское время (зима)  
Nmap scan report for 192.168.1.113  
Host is up (0.0020s 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 11.54 seconds

Свернуть все окна

2:01 19.03.2025



## Интенсивность 4

The screenshot shows the Zenmap application window. At the top, there is a menu bar with 'Scan', 'Tools', 'Profile', and 'Help'. Below the menu, the 'Target' field contains '192.168.1.113' and the 'Profile' field is empty. The 'Command' field contains 'nmap -sV -p 5000 --version-intensity 4 192.168.1.113'. On the left side, there is a 'Hosts' tab and a 'Services' tab. The 'Services' tab is active, showing a list of services: ftp, http, microsoft-ds, msrpc, and netbios-ssn. The main area displays the Nmap output for the scan. The output includes the command used, the starting time, the scan report for 192.168.1.113, and the results of the service detection. The results show that port 5000/tcp is open and running the http service (Apache httpd 2.4.63 (Debian)). The MAC address is 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC). The scan was completed in 11.55 seconds.

Target: 192.168.1.113 Profile: Scan Cancel

Command: nmap -sV -p 5000 --version-intensity 4 192.168.1.113

Hosts Services

Service

ftp  
http  
microsoft-ds  
msrpc  
netbios-ssn

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV -p 5000 --version-intensity 4 192.168.1.113 Details

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

2:01  
19.03.2025

## Интенсивность 5

The screenshot displays the Zenmap application window. At the top, the 'Target' field is set to '192.168.1.113' and the 'Command' field contains 'nmap -sV -p 5000 --version-intensity 5 192.168.1.113'. The 'Scan' button is visible. Below the command field, the 'Hosts' and 'Services' tabs are active. The 'Services' tab shows a list of services: ftp, http, microsoft-ds, msrpc, and netbios-ssn. The 'Nmap Output' tab is selected, displaying the following scan results:

```
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 Windows taskbar at the bottom shows the date and time as 19.03.2025, 2:01, and the language is set to ENG.

## Интенсивность 6

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113 Profile: Scan Cancel

Command: `nmap -sV -p 5000 --version-intensity 6 192.168.1.113`

Hosts Services

Service

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

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV -p 5000 --version-intensity 6 192.168.1.113 Details

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 (0.0011s 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

2:02  
19.03.2025

## Интенсивность 7

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113 Profile: Scan Cancel

Command: nmap -sV -p 5000 --version-intensity 7 192.168.1.113

Hosts Services

Service

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

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV -p 5000 --version-intensity 7 192.168.1.113 Details

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

Windows taskbar: 2:02 19.03.2025

## Интенсивность 8

The screenshot displays the Zenmap application window. At the top, the 'Target' field is set to '192.168.1.113' and the 'Command' field contains 'nmap -sV -p 5000 --version-intensity 8 192.168.1.113'. The 'Scan' button is visible. Below the command field, there are tabs for 'Hosts', 'Services', 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Services' tab is selected, showing a list of services on the left: ftp, http, microsoft-ds, msrpc, and netbios-ssn. The 'Nmap Output' tab is also visible, showing the scan results for the target IP. The output text is as follows:

```
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 Windows taskbar at the bottom shows the system clock as 2:02 on 19.03.2025, along with various system icons and the language set to ENG.

## Интенсивность 9

Zenmap

Scan Tools Profile Help

Target: 192.168.1.113 Profile: Scan Cancel

Command: nmap -sV -p 5000 --version-intensity 9 192.168.1.113

Hosts Services

Service

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

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV -p 5000 --version-intensity 9 192.168.1.113 Details

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-03-19 02:03 Азербайджанское время (зима)  
Nmap scan report for 192.168.1.113  
Host is up (0.0011s latency).

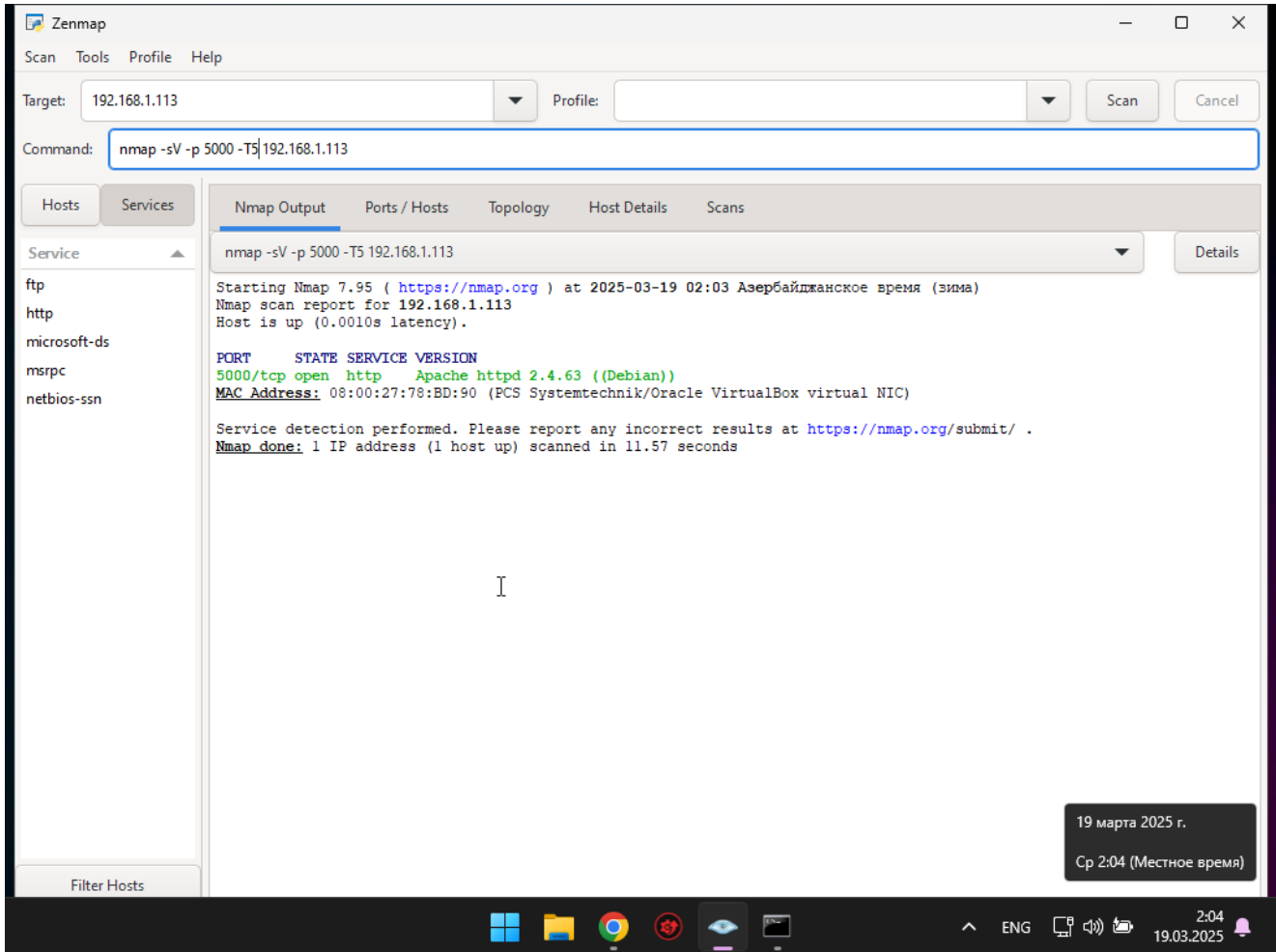
PORT	STATE	SERVICE	VERSION
5000/tcp	open	http	Apache httpd 2.4.63 ((Debian))

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 11.62 seconds

2:03  
19.03.2025

## 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

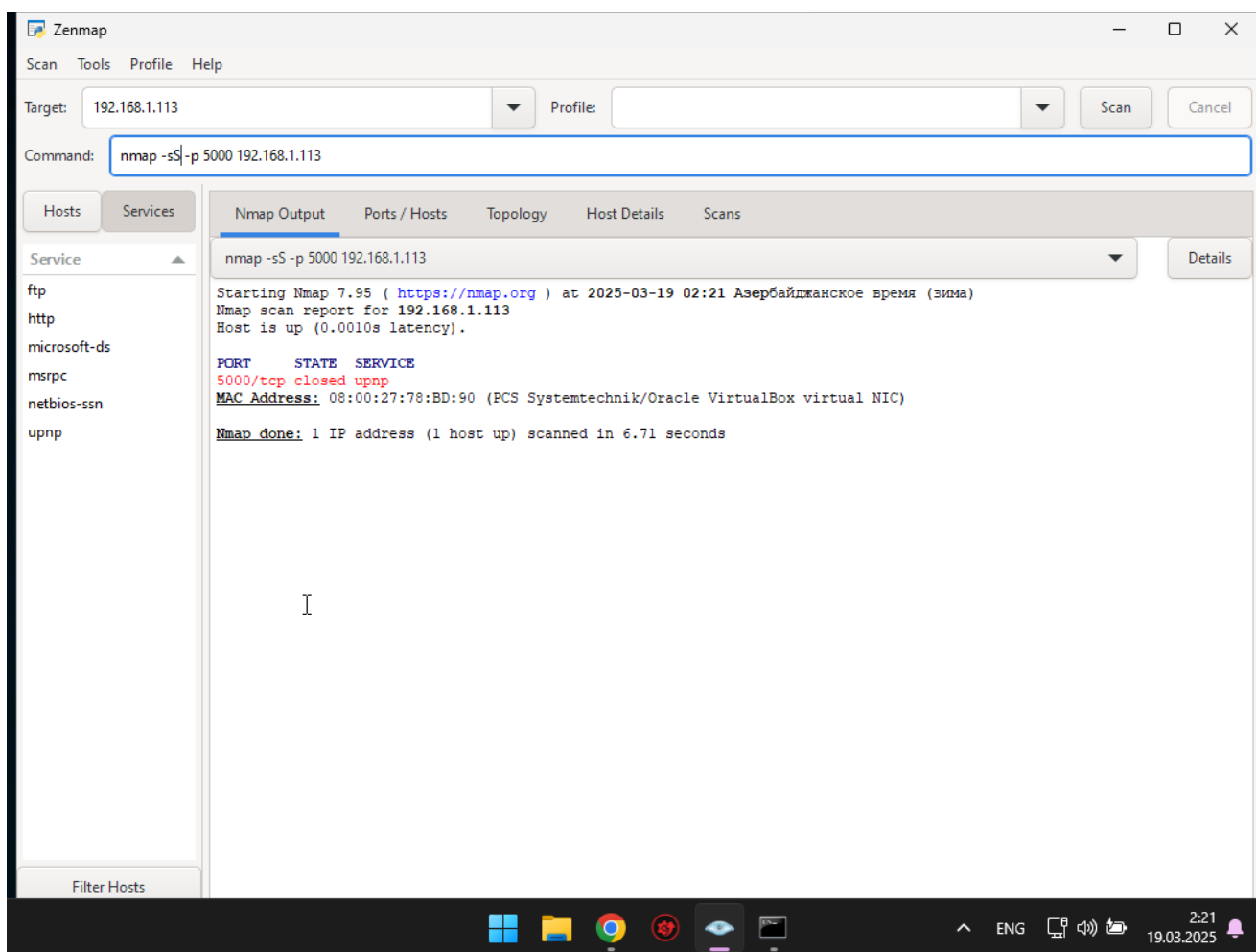
```
sudo: iptables: command not found

(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.

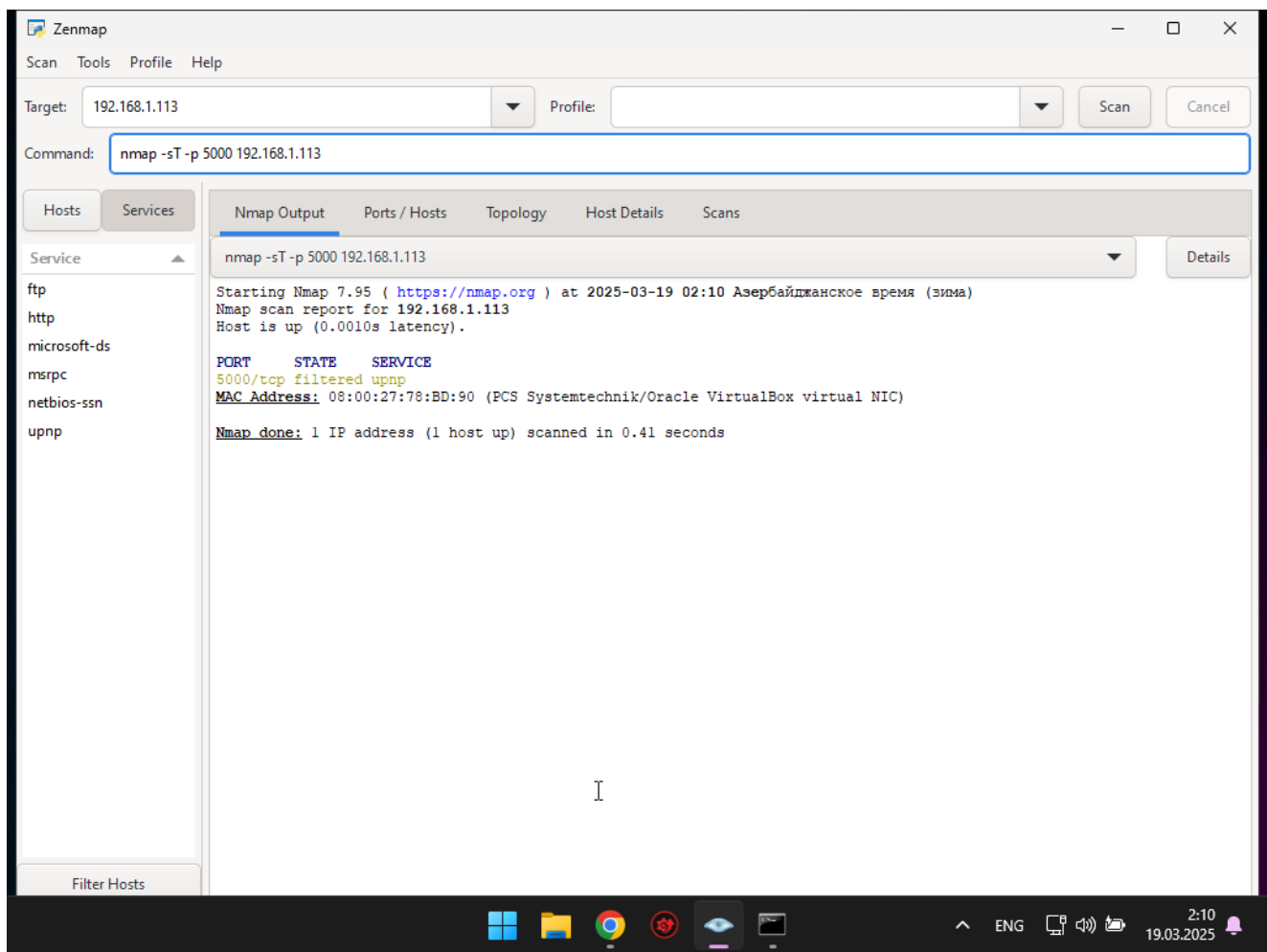
### TCP SYN Scan



REJECT отправляет ответ RST, nmap считает порт закрытым.

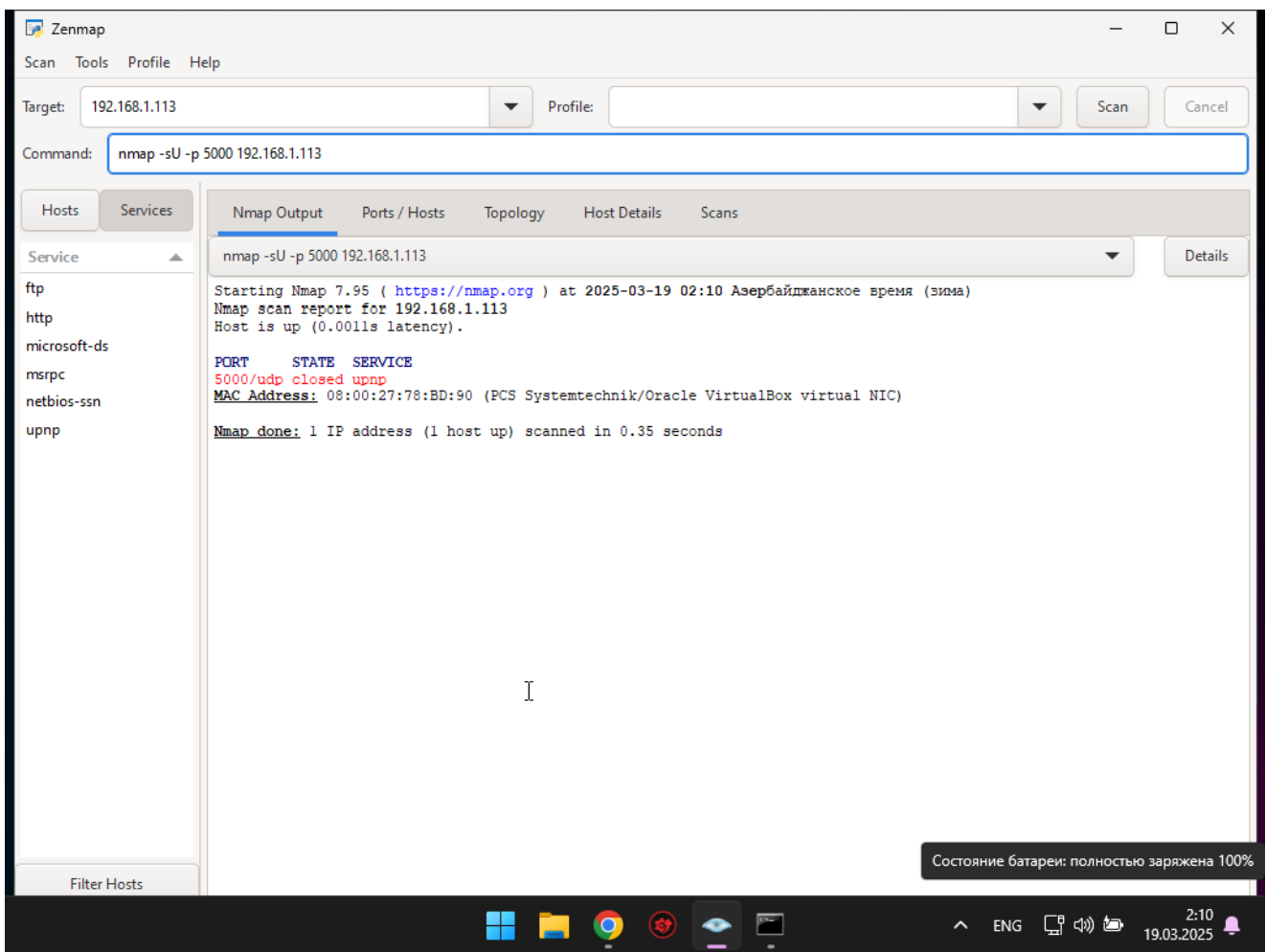
## TCP Connect Scan





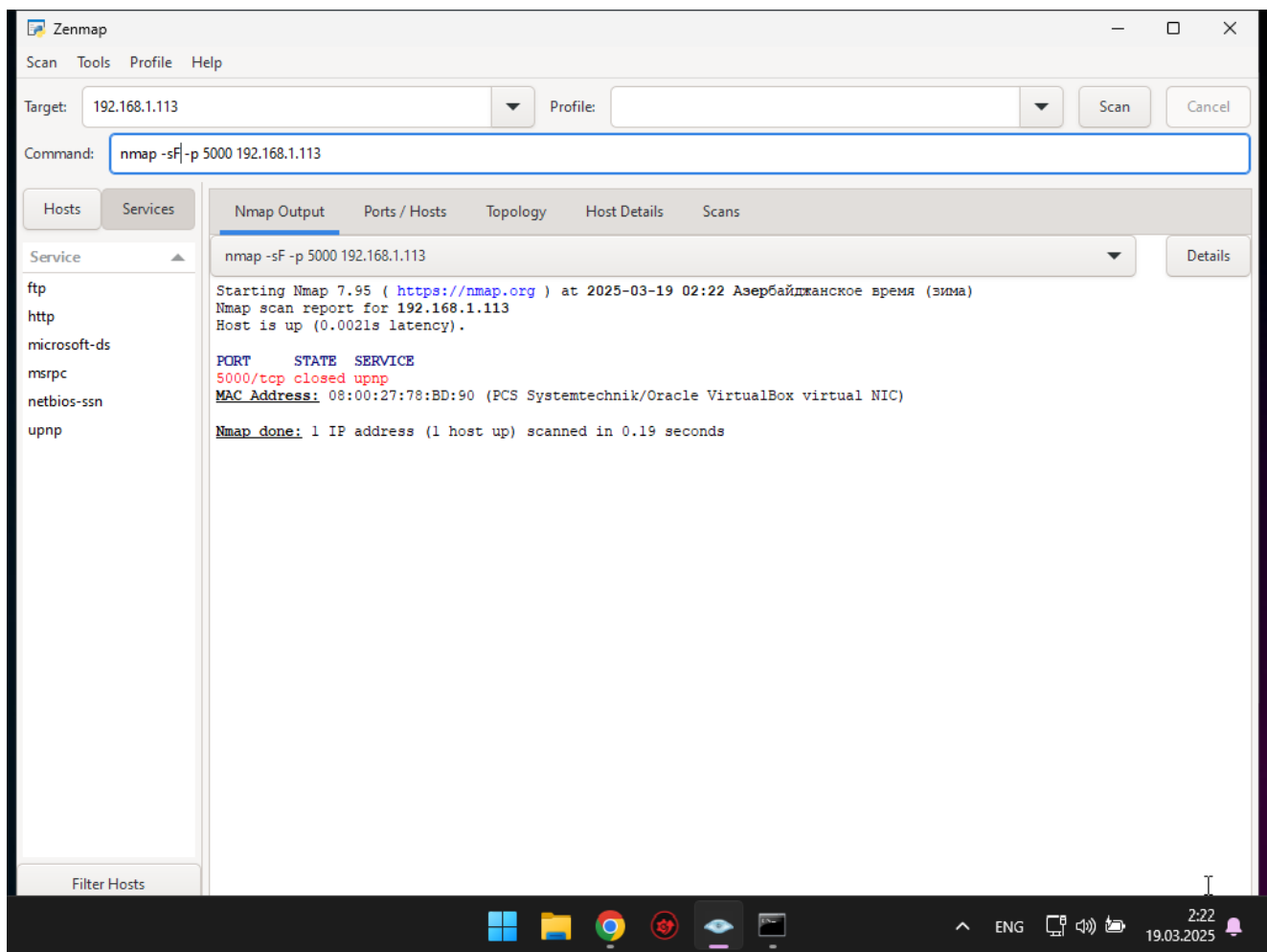
Порт показывается как filtered

## UDP Scan



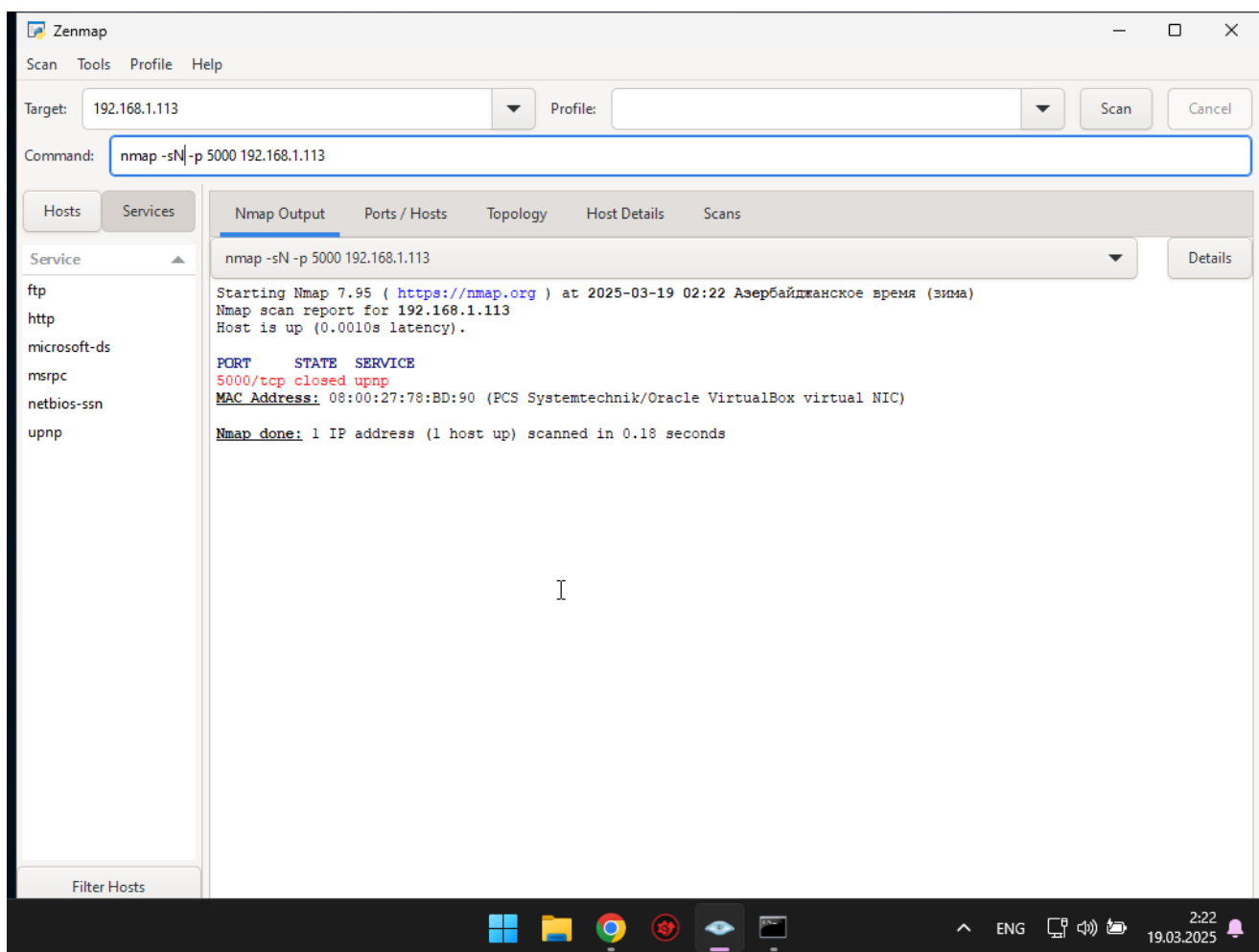
Порт показывается как closed

## TCP FIN Scan



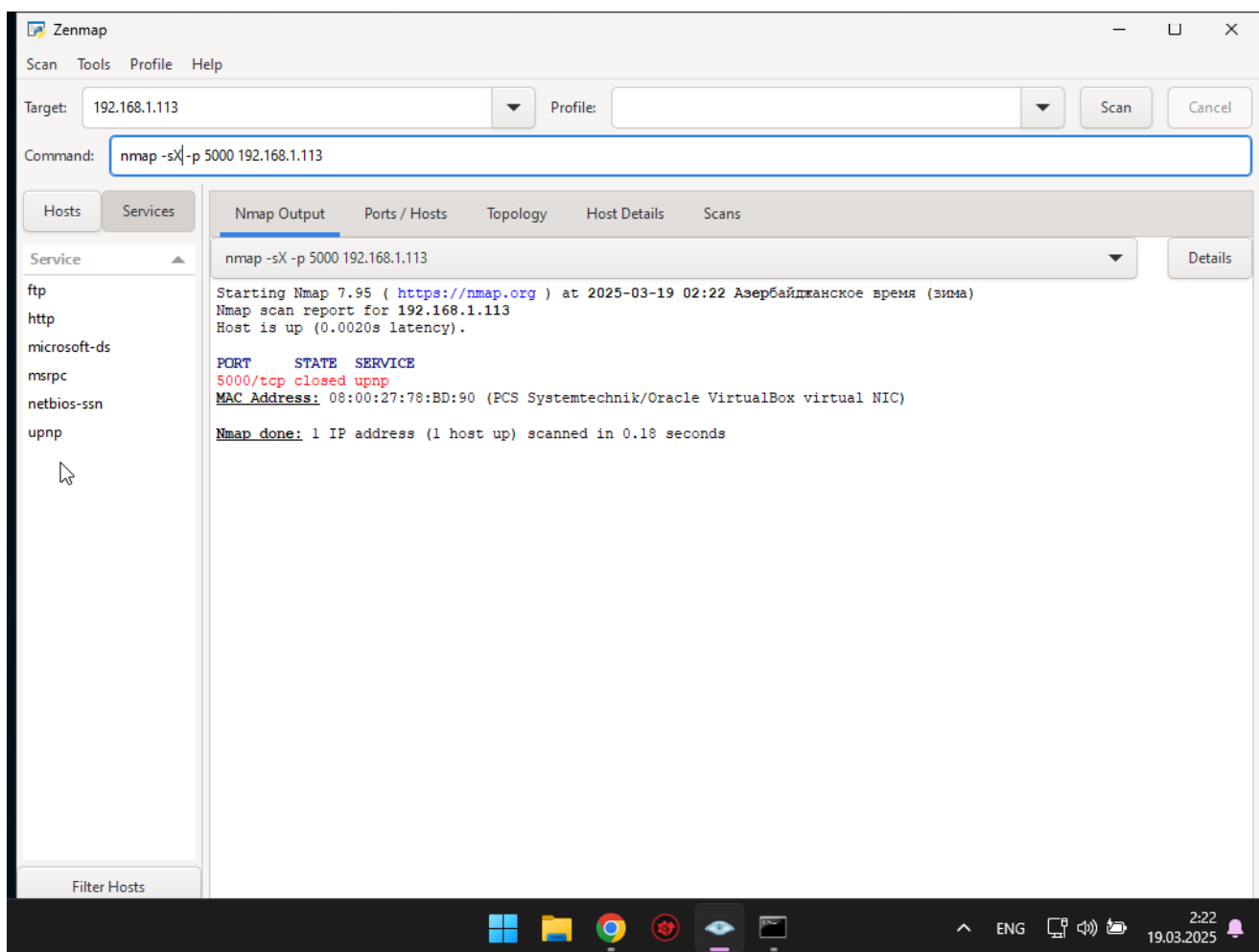
Порт показывается как closed

## TCP NULL Scan



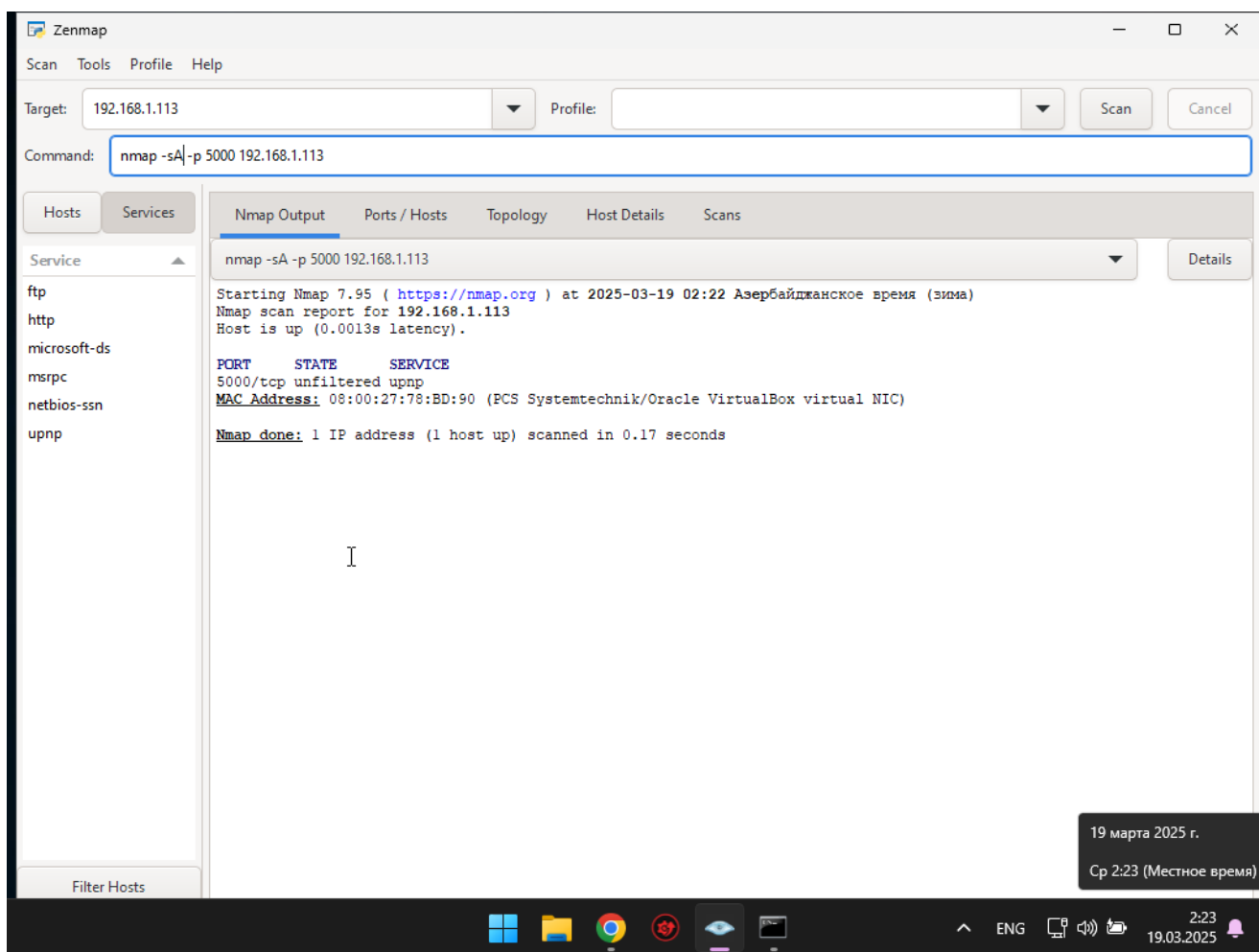
Порт показывается как closed

## TCP Xmas Scan



Порт показывается как closed

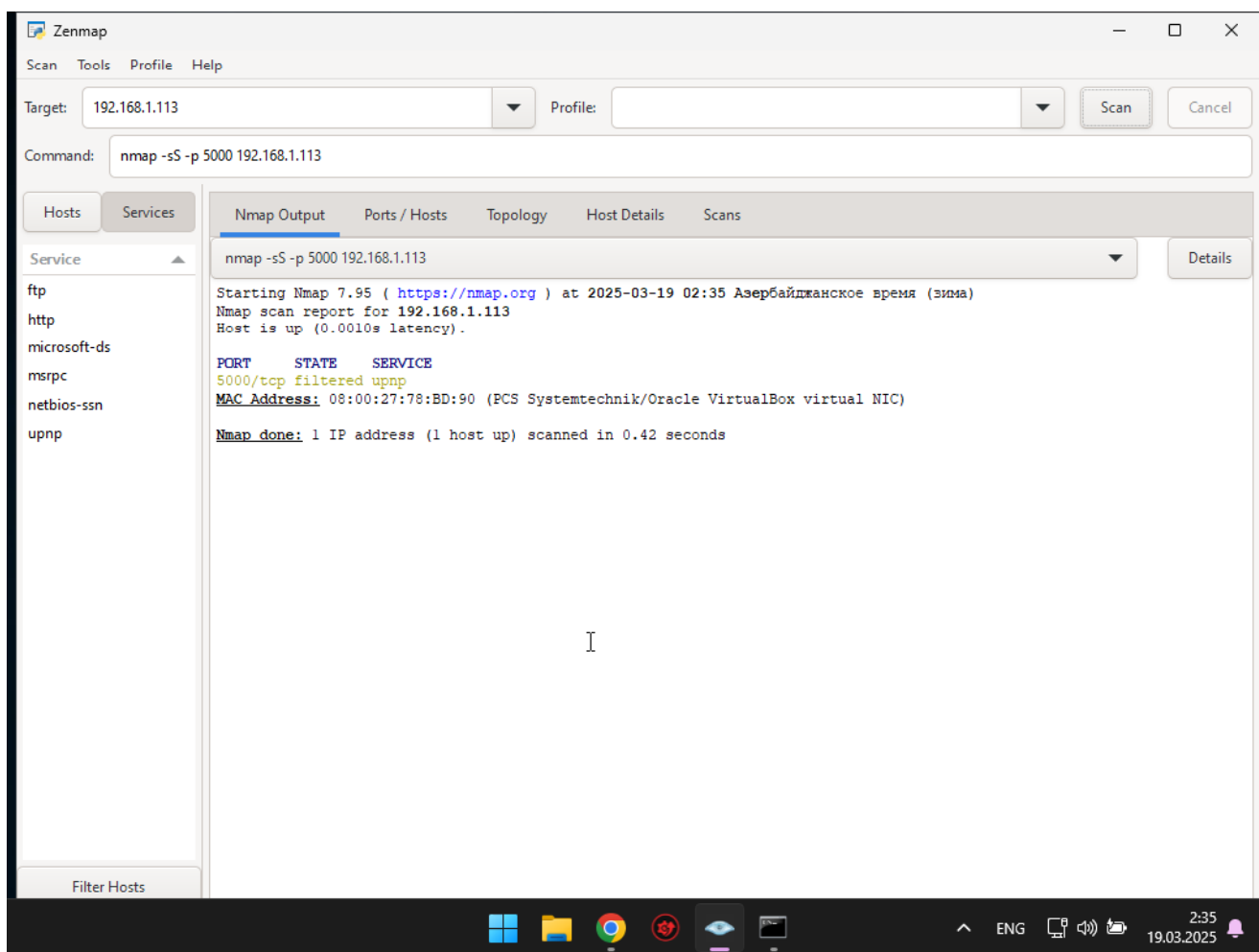
## TCP ACK Scan



Порт показывается как unfiltered

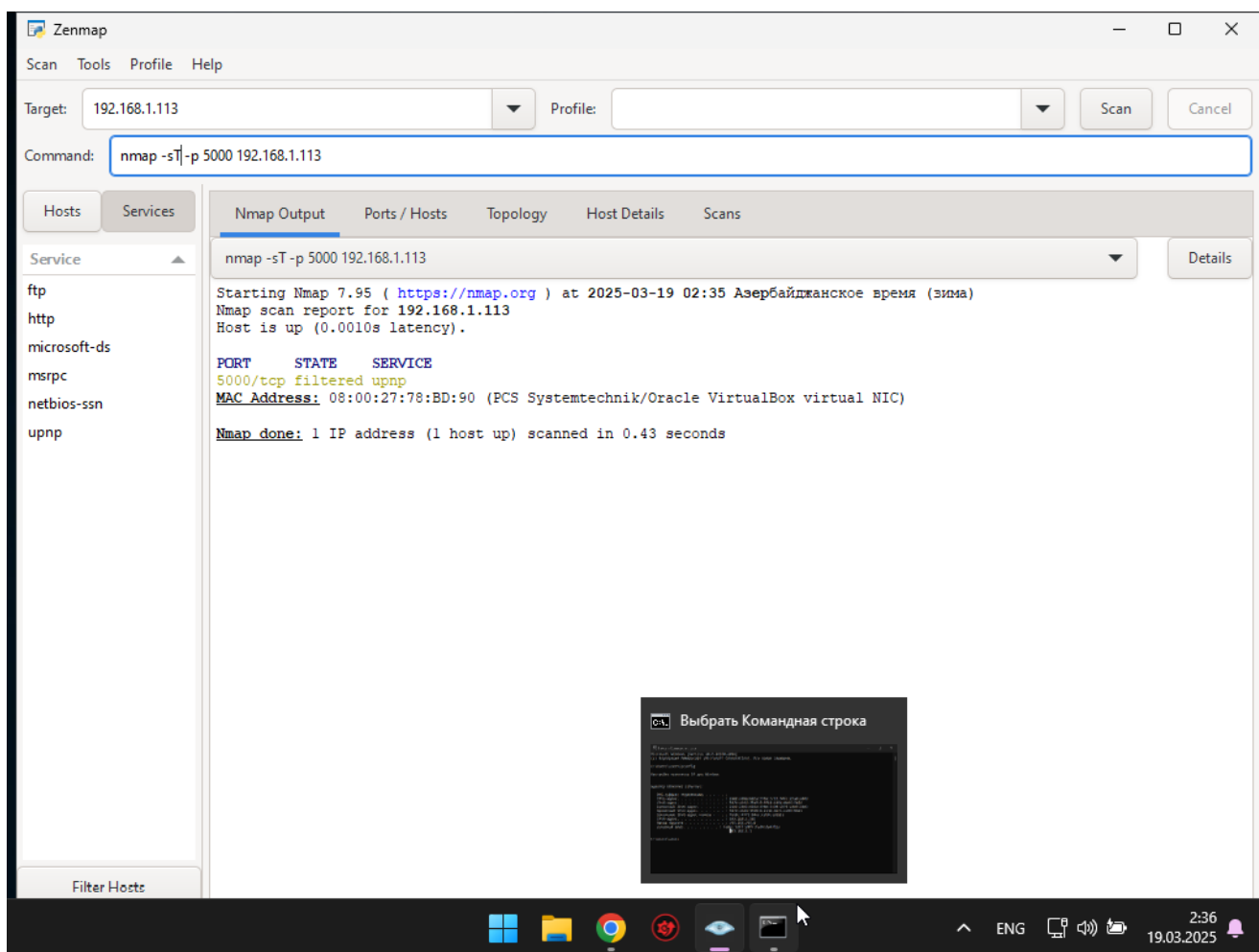
Шаг 16. Удалите правило из пункта 13 (14) и добавьте аналогичное, но с политикой DROP. Повторите пункт 14 (15). Сравните результаты с пунктом 14 (15).

### TCP SYN Scan



Порт показывается как filtered

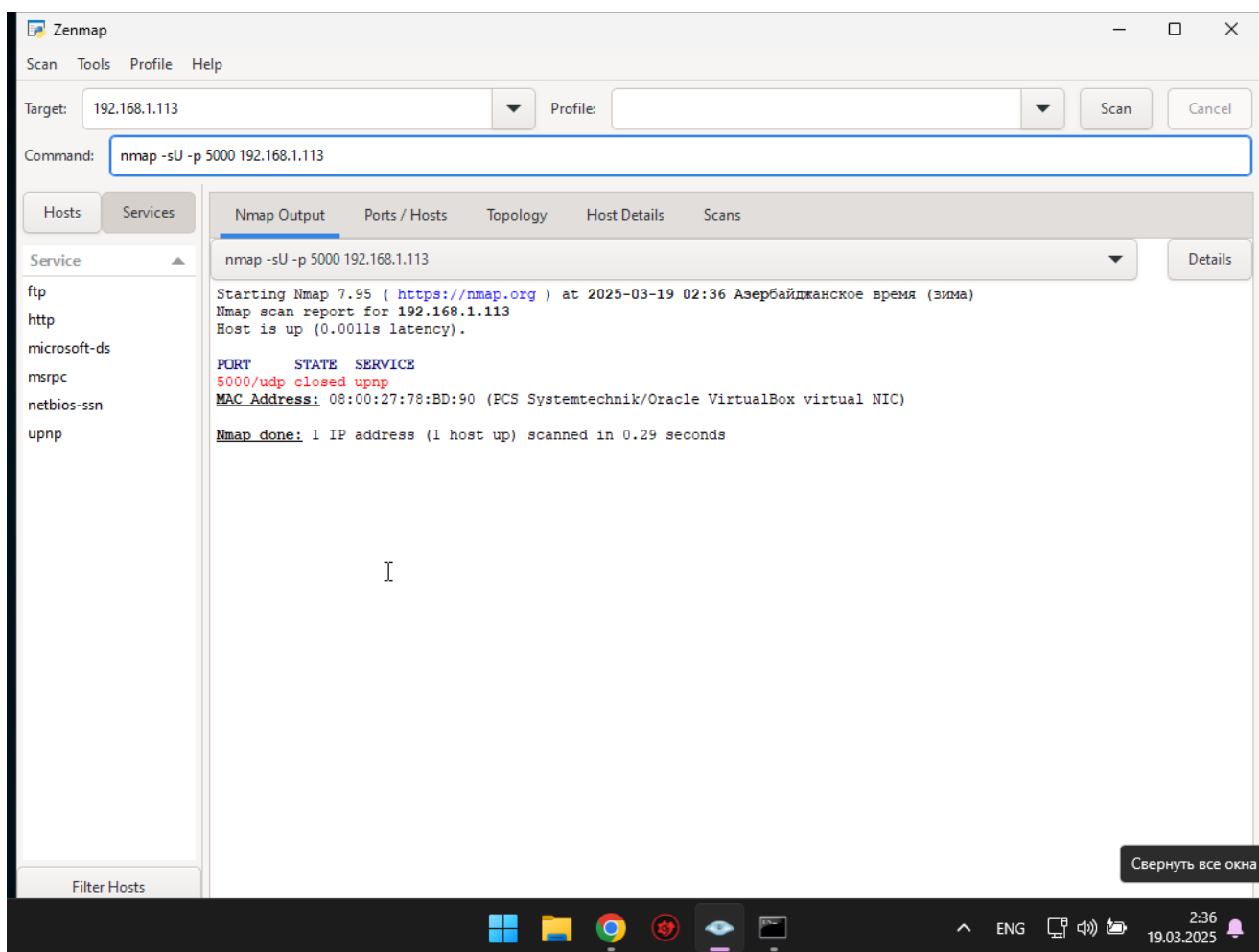
## TCP Connect Scan



Порт показывается как filtered

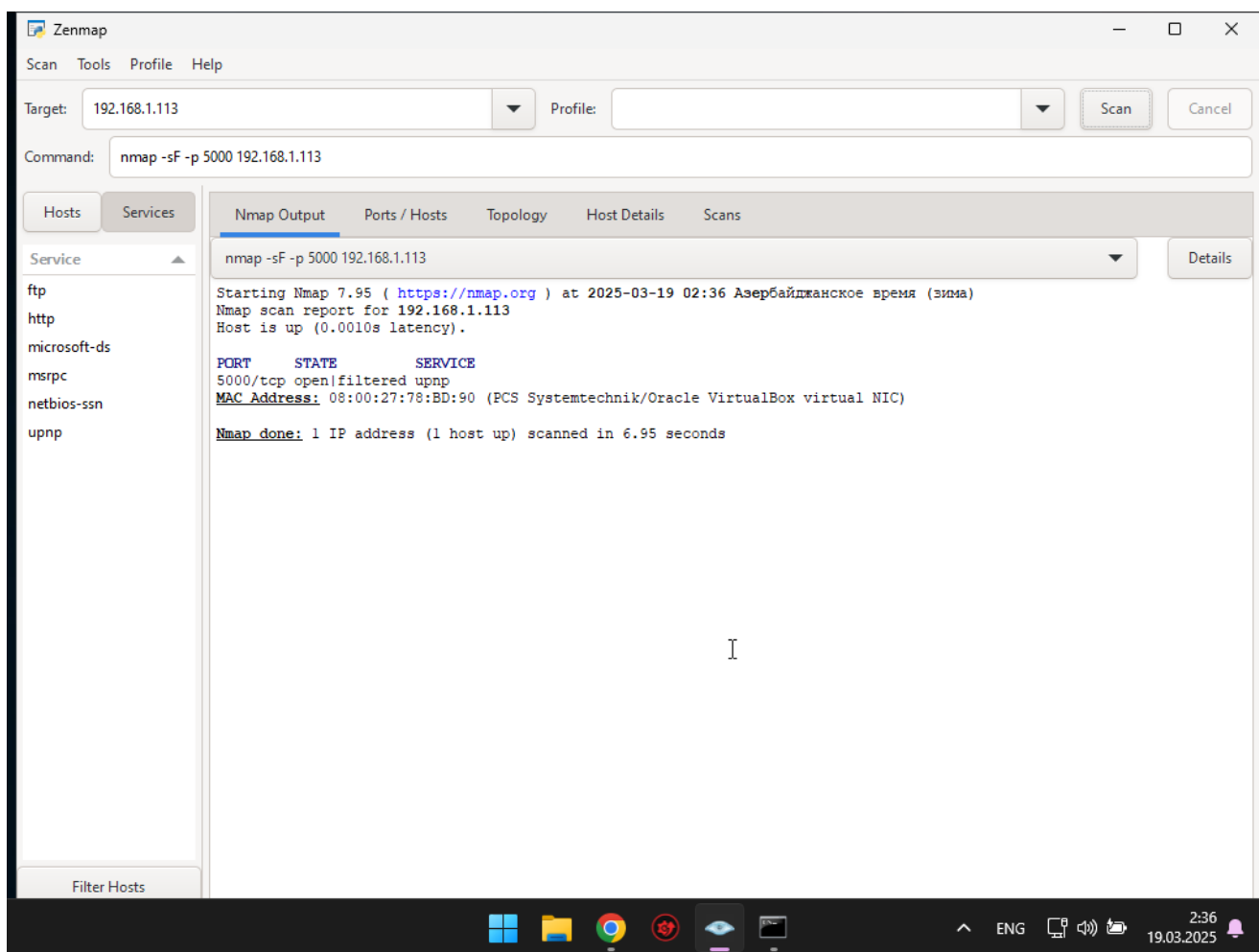
## UDP Scan





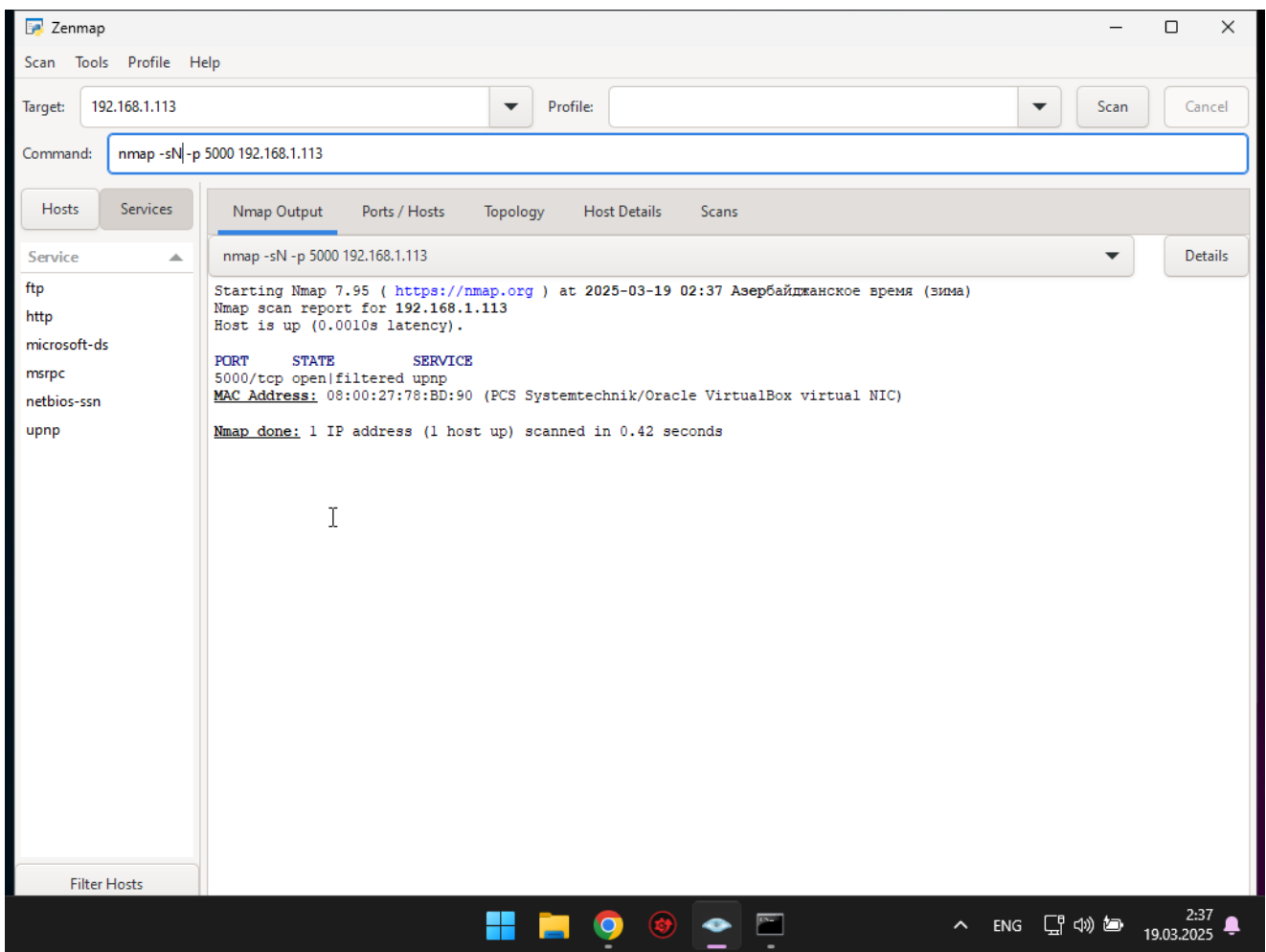
Порт показывается как closed

## TCP FIN Scan



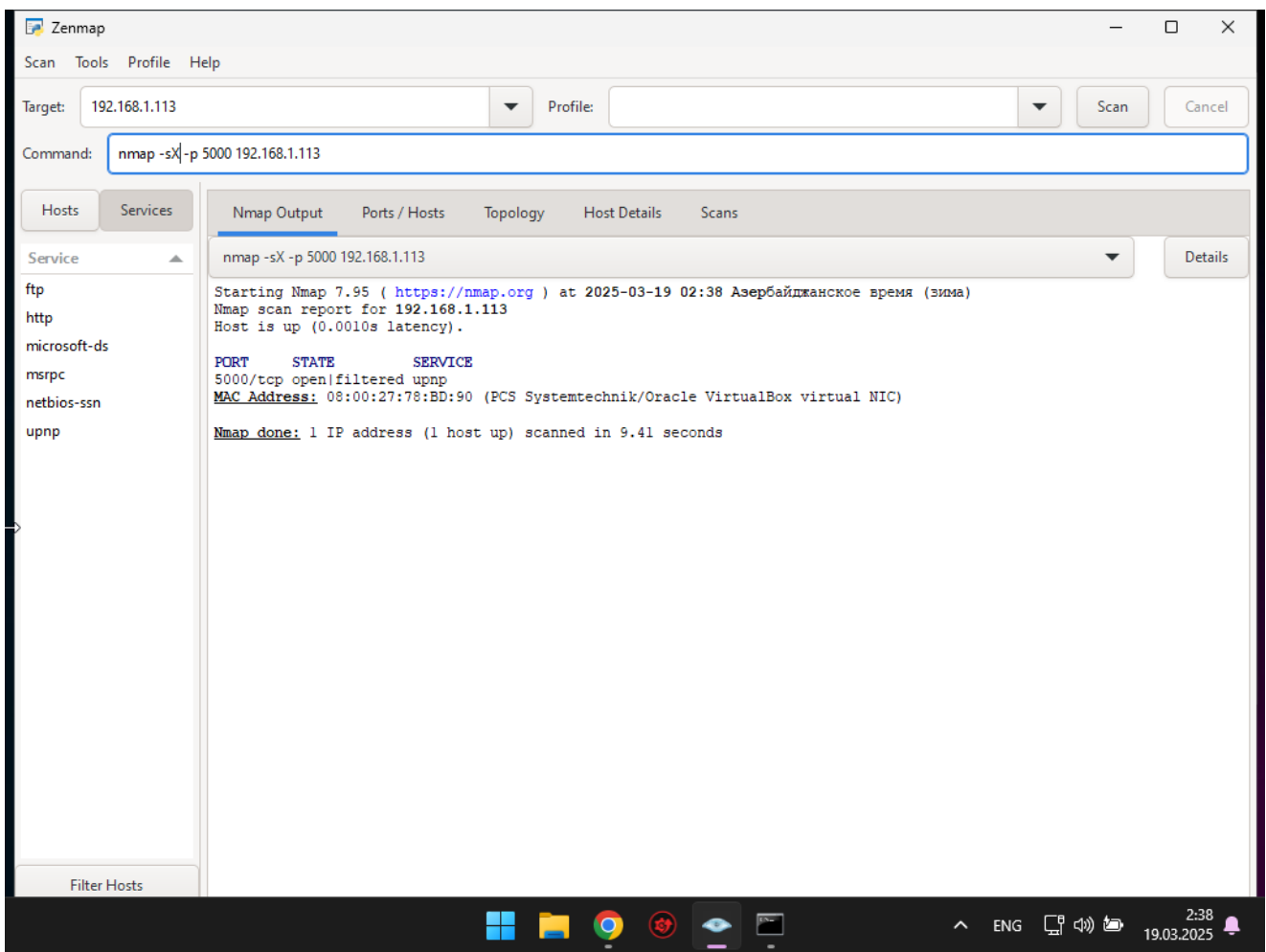
Порт показывается как open|filtered

## TCP NULL Scan



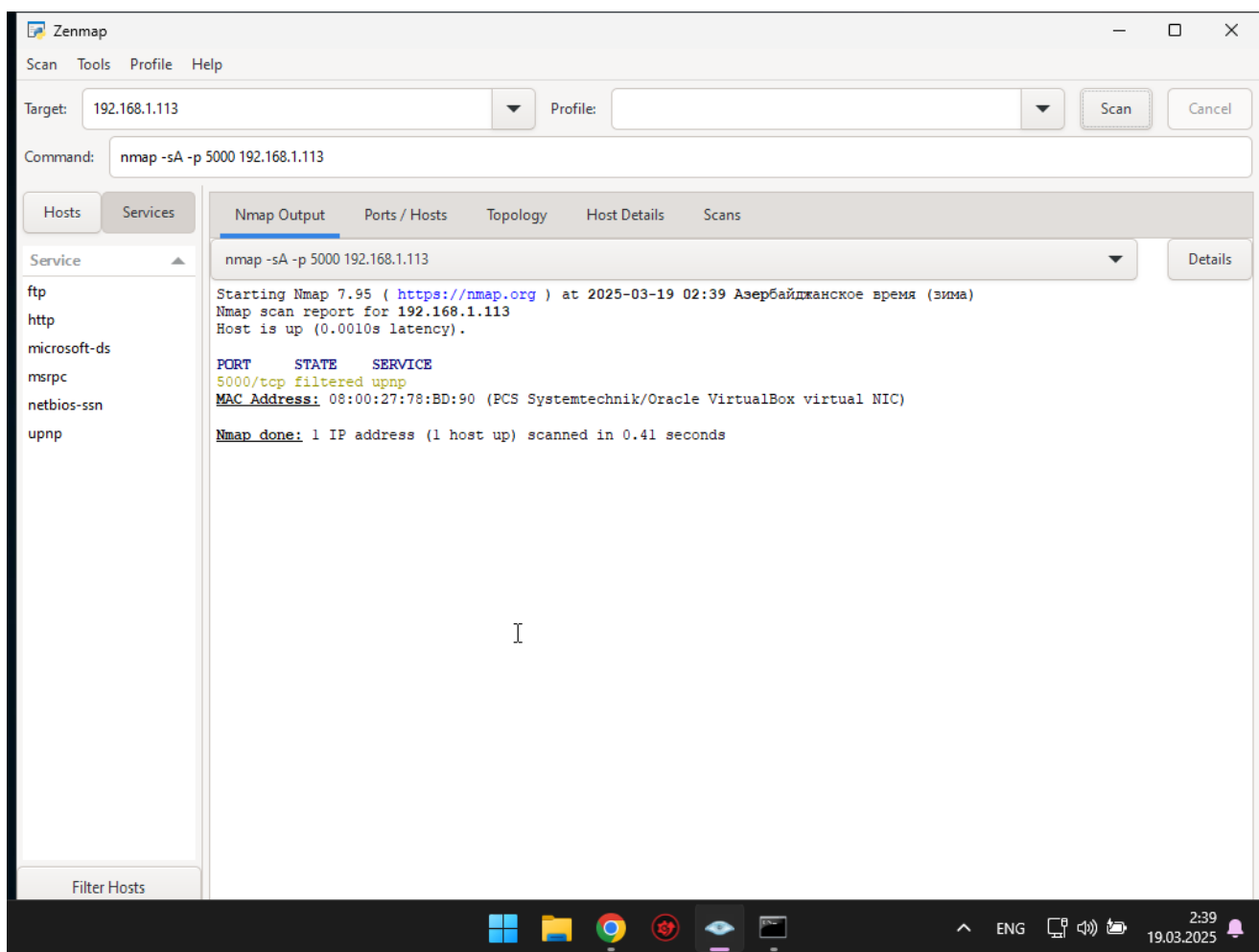
Порт показывается как open|filtered

## TCP Xmas Scan



Порт показывается как open|filtered

## TCP ACK Scan



Порт показывается как filtered