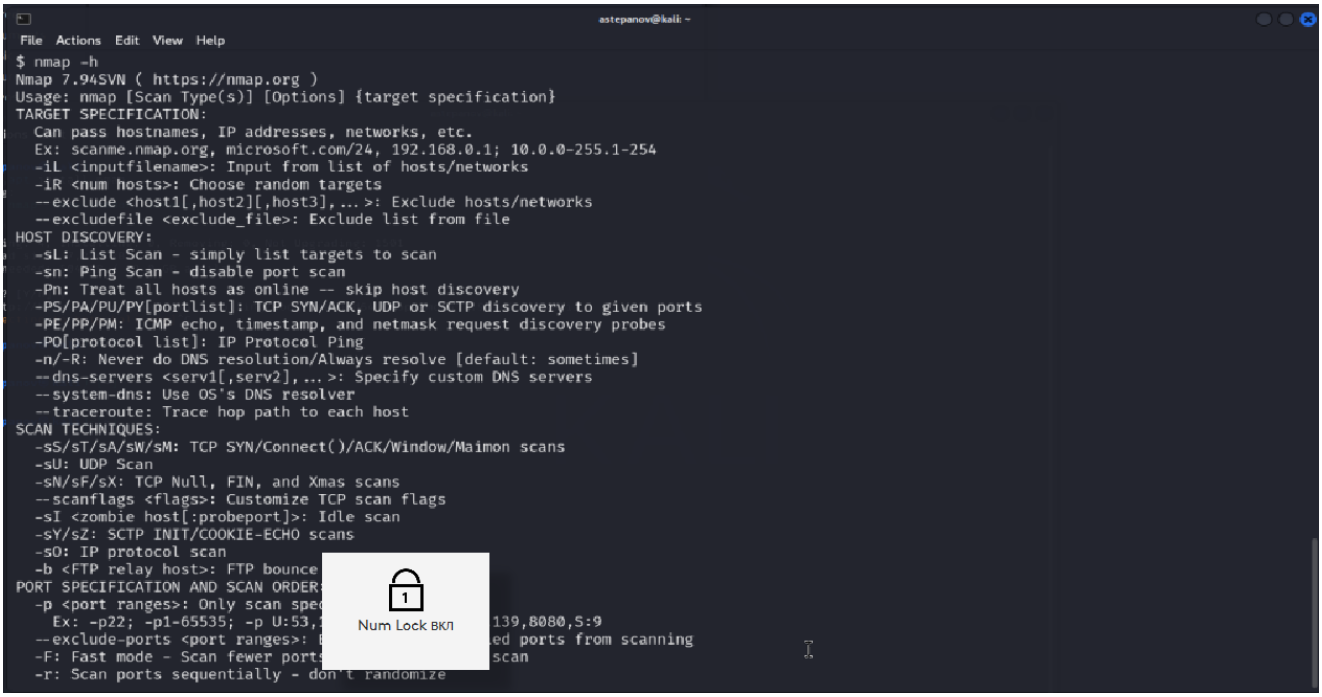
Модуль 2. Сканирование сетей (HW)

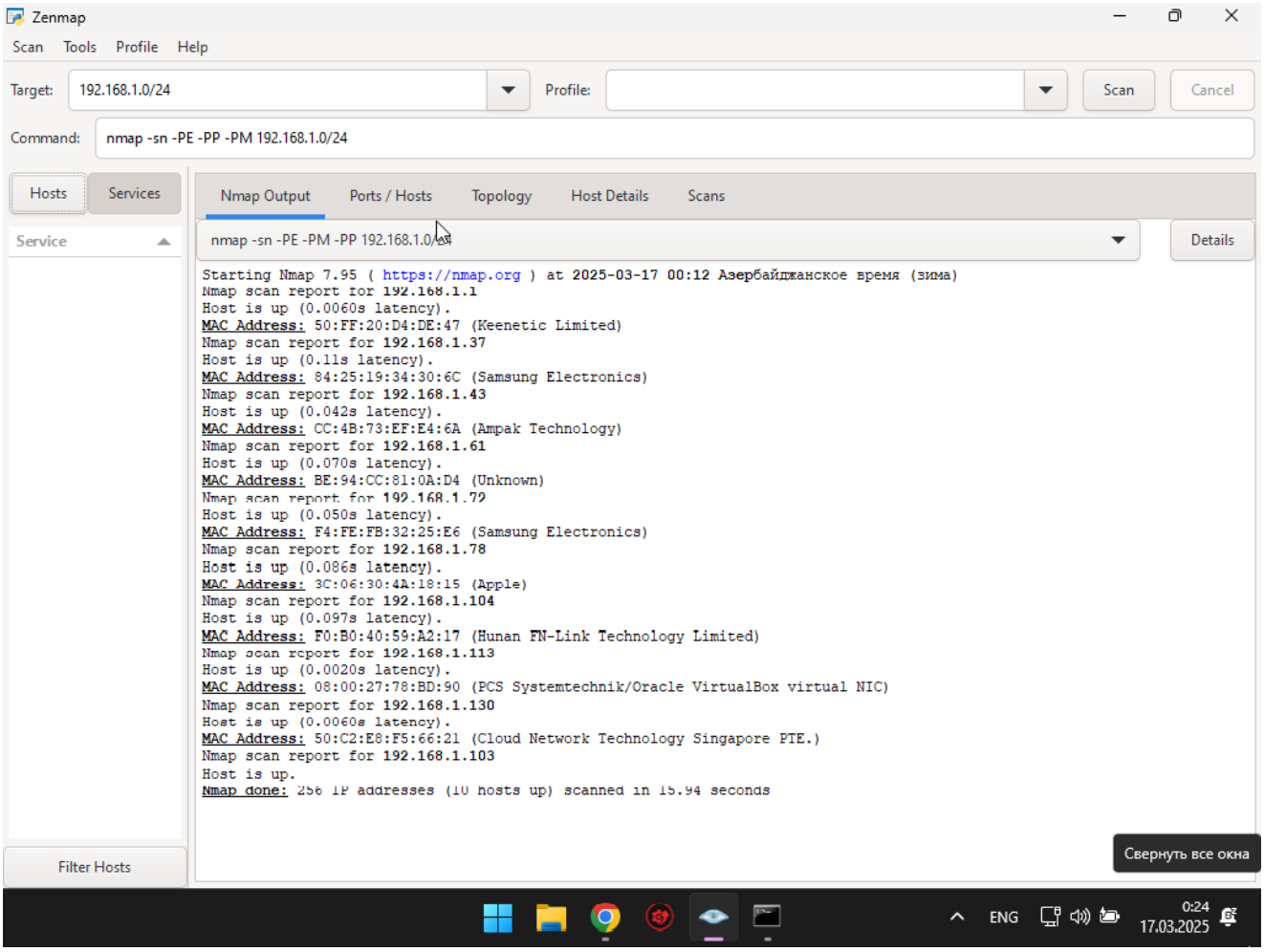
Лабораторная работа №2 (HW)

Для выполнения данной лабораторной работы пришлось устанавливать Windows на виртуальную машину

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

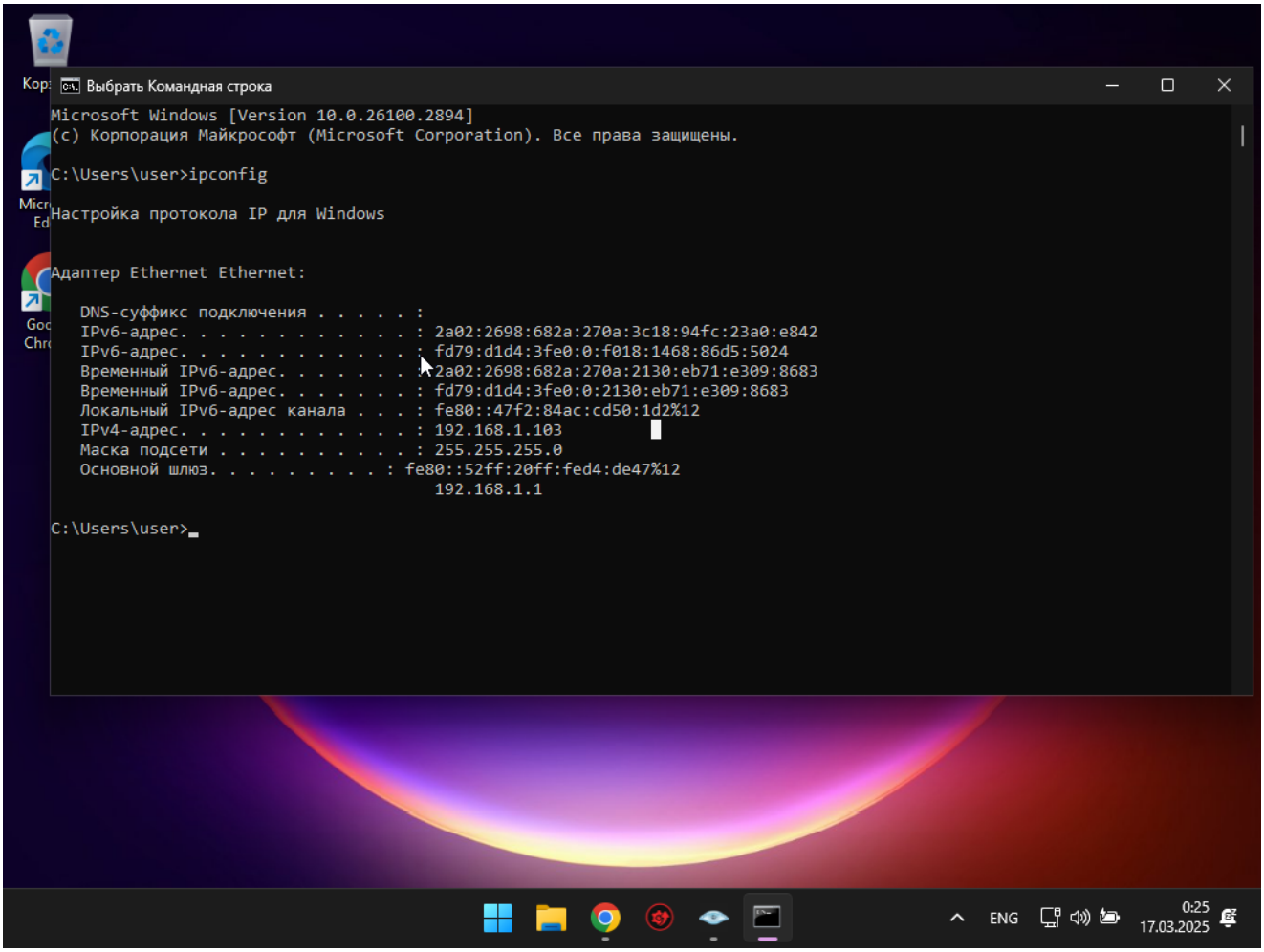


Шаг 2. Установите Nmap на Windows



Шаг 3. Узнайте IP-адрес на двух машинах

IP-адрес машины Windows - **192.168.1.103**

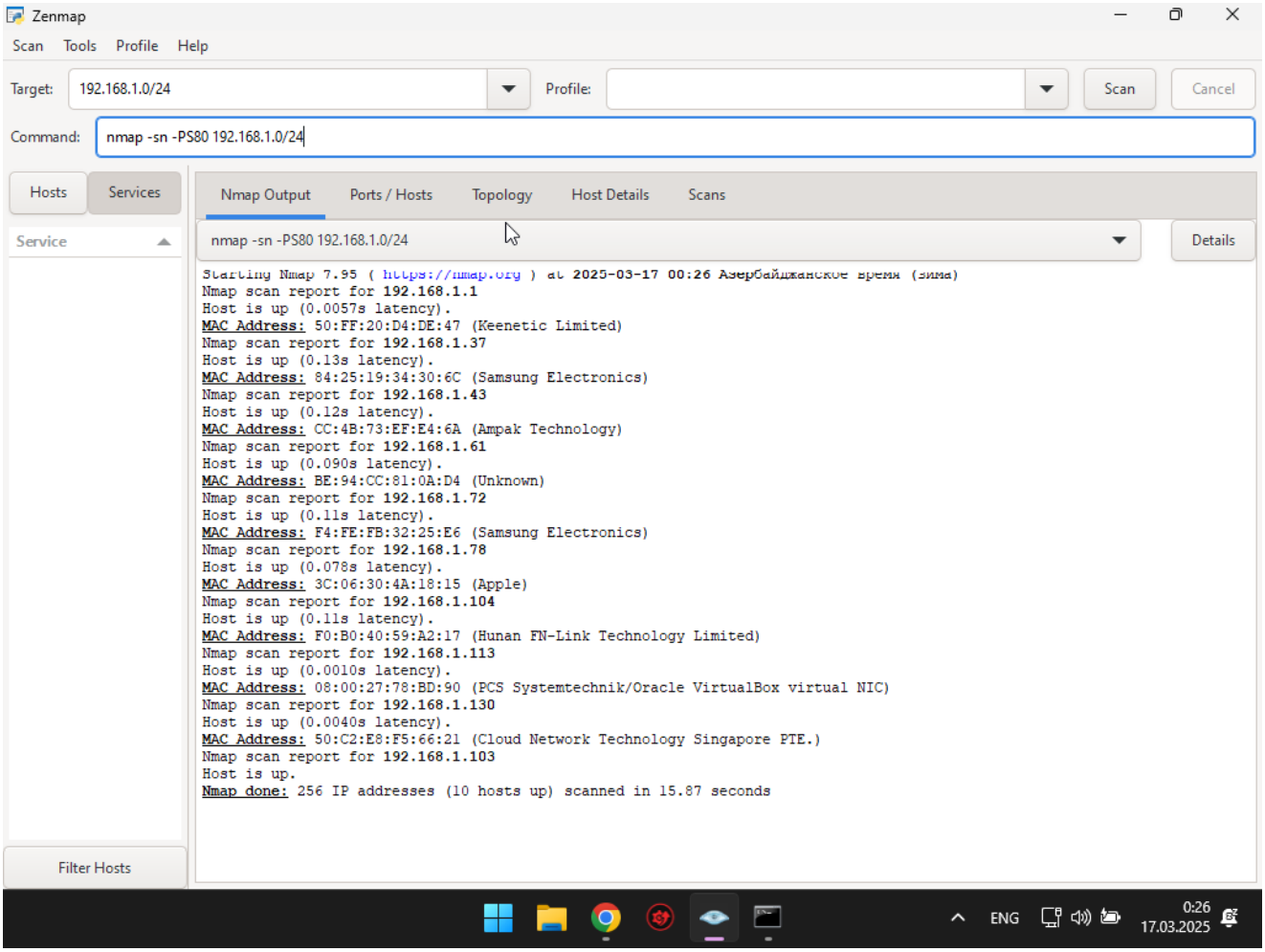


IP-адрес машины Kali Linux - **192.168.1.113**

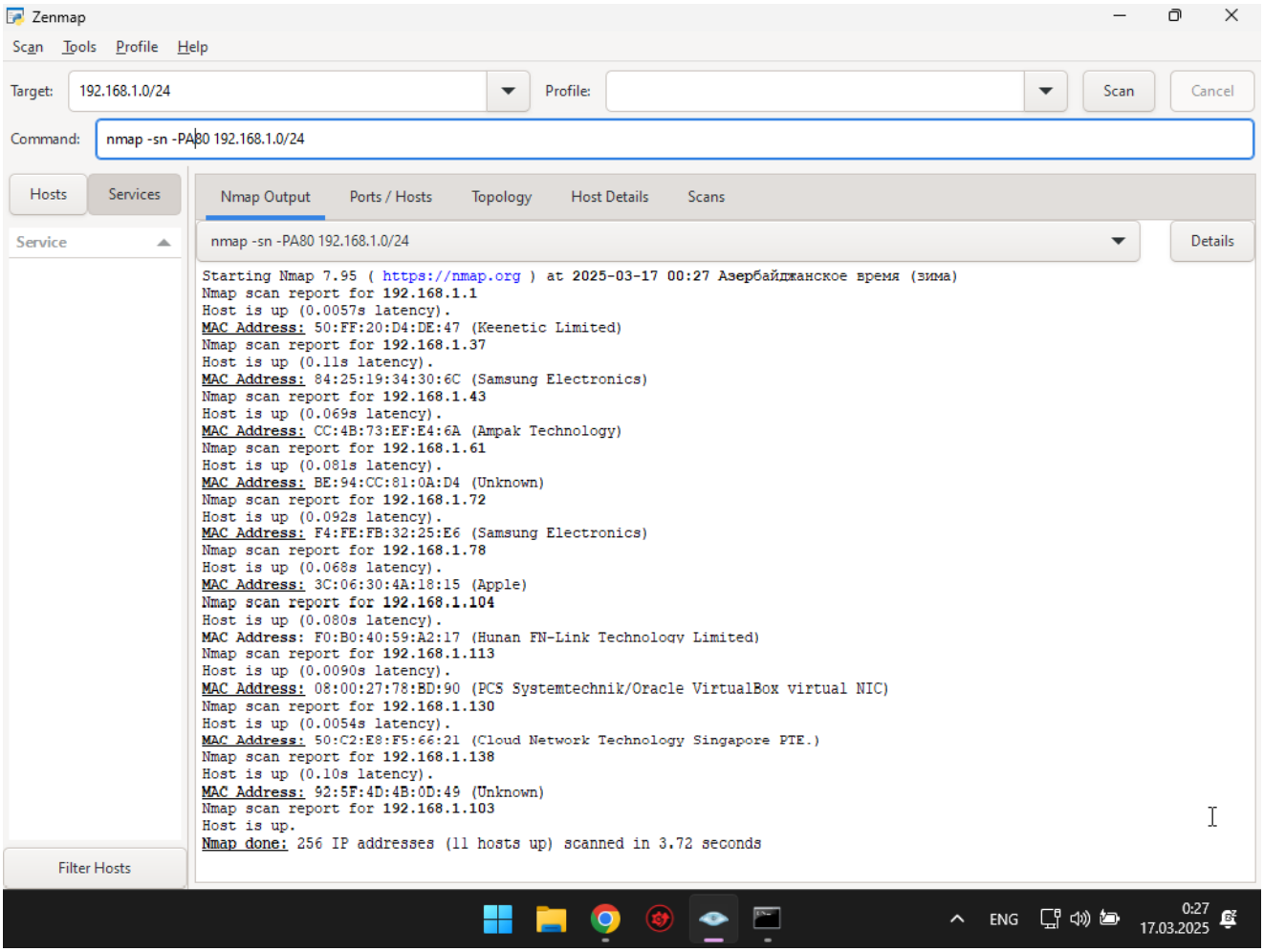
Шаг 4. Исследуем доступность сети

С машины Windows

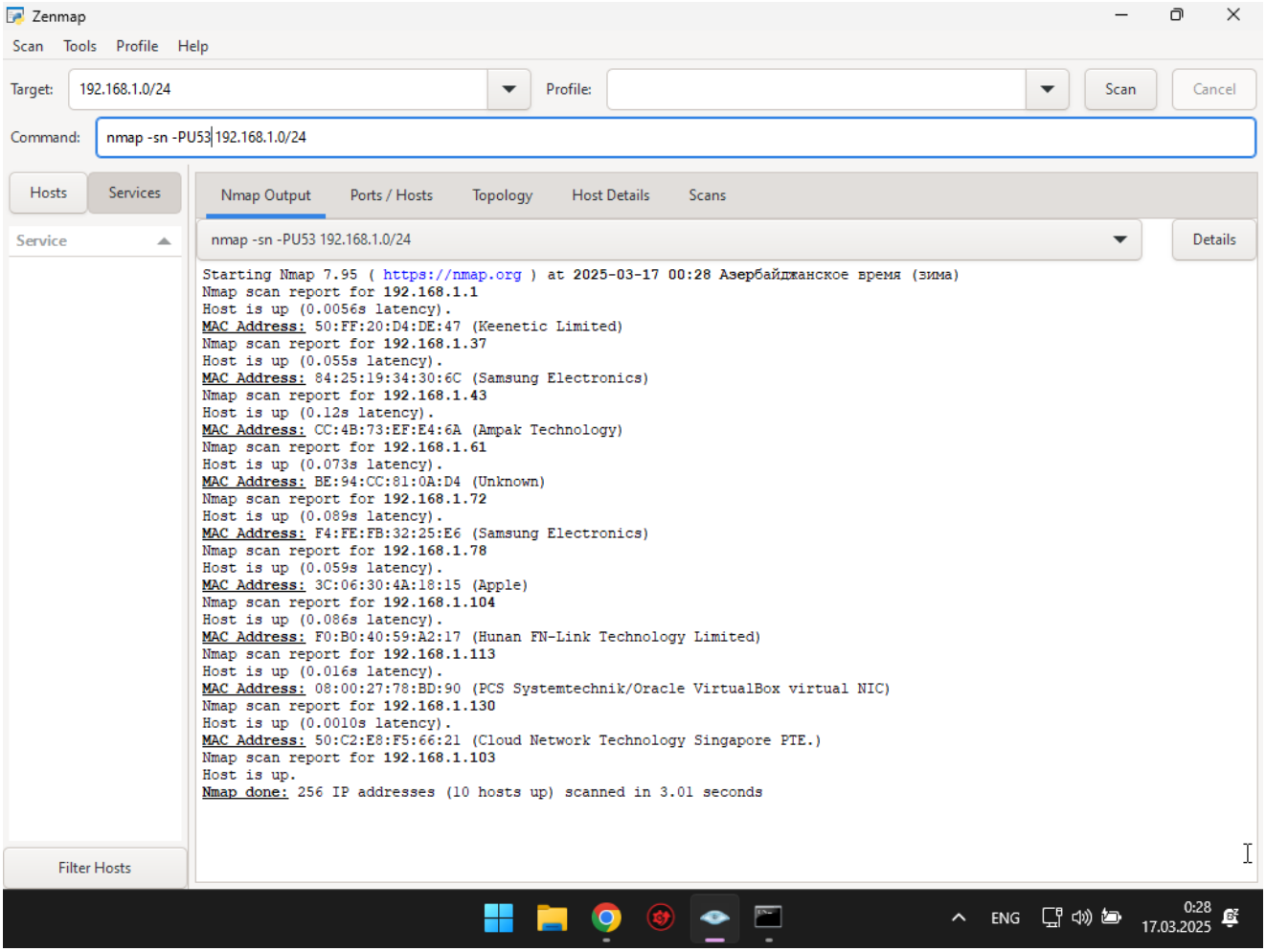
TCP SYN Ping



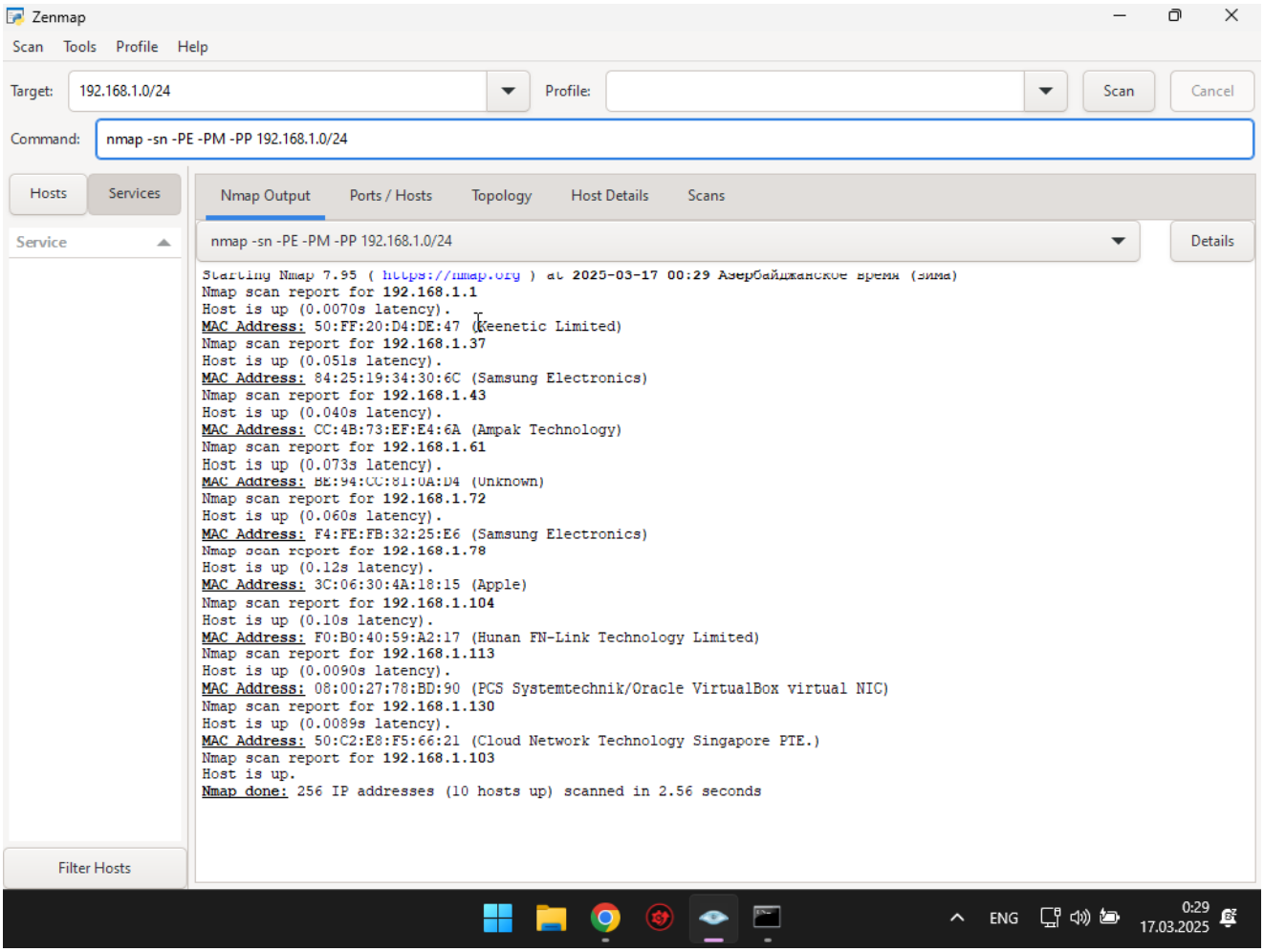
TCP ACK Ping


Zenmap
Scan Tools Profile Help
Target: 192.168.1.0/24
Profile:
Scan
Cancel
Command: nmap -sn -PA80 192.168.1.0/24
Hosts
Services
Service
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sn -PA80 192.168.1.0/24
Details
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

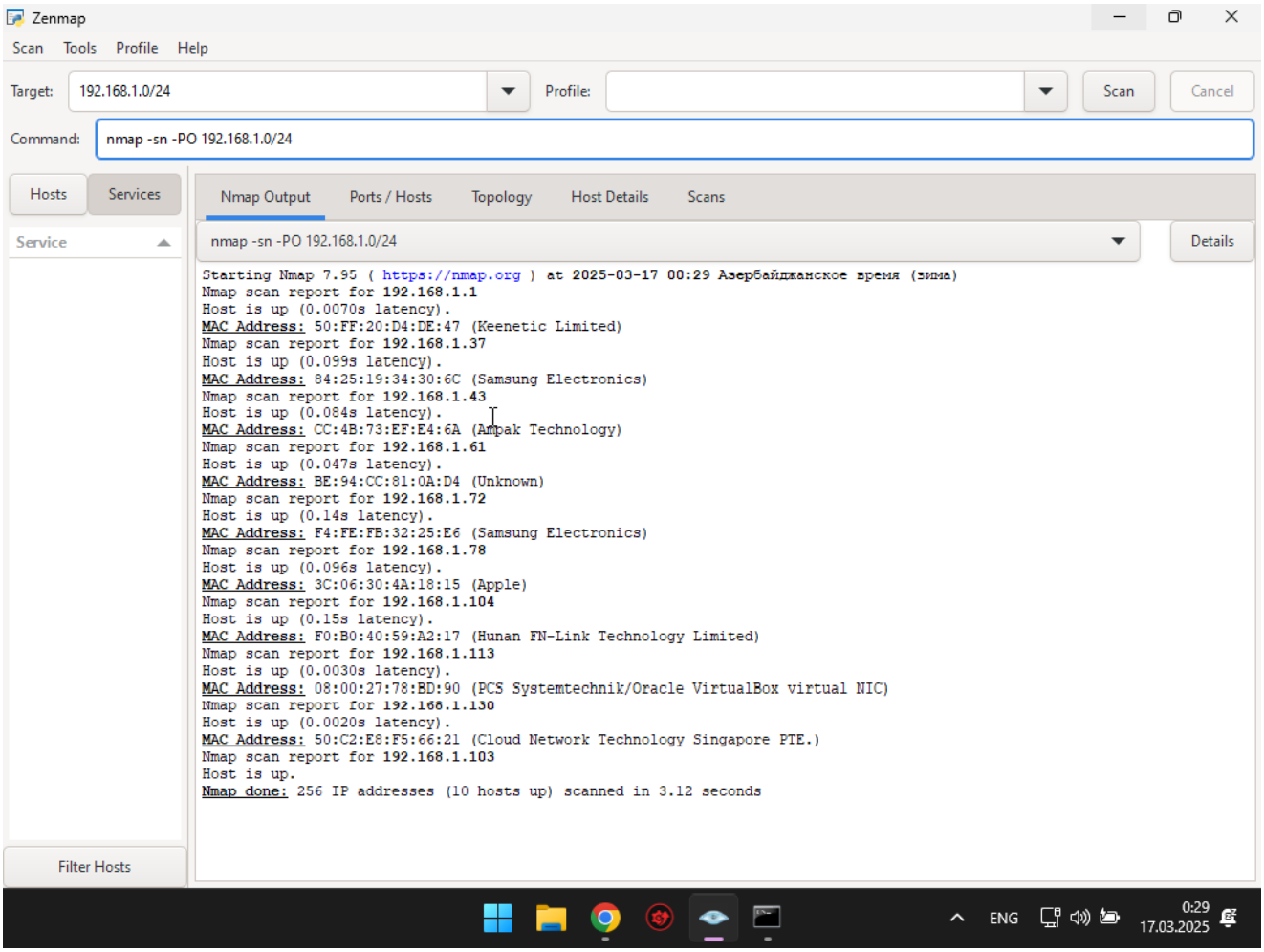
UDP Ping


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
ENG
0:28
17.03.2025

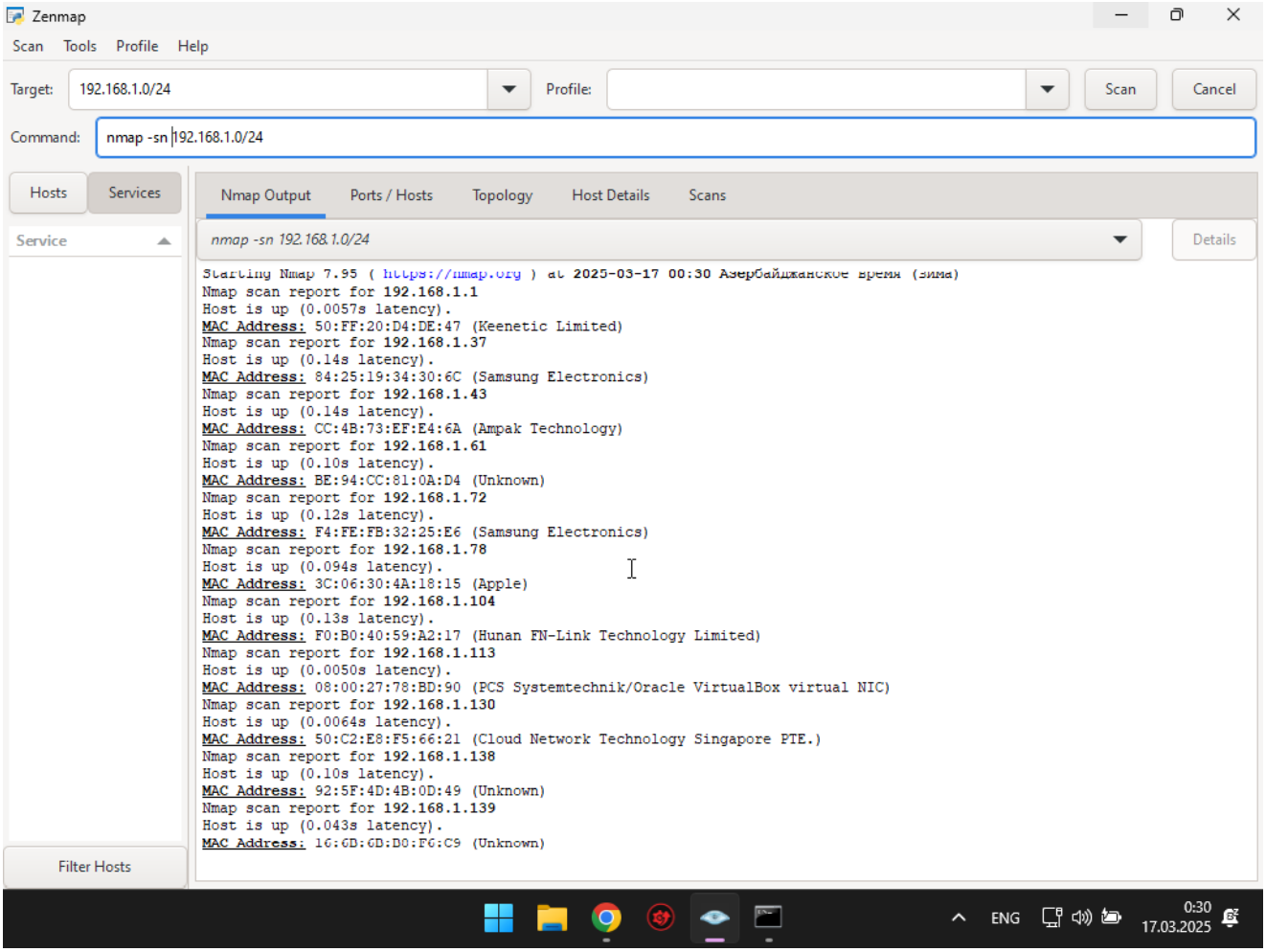
ICMP Ping Types



IP Protocol Ping



Обычный ping-скан

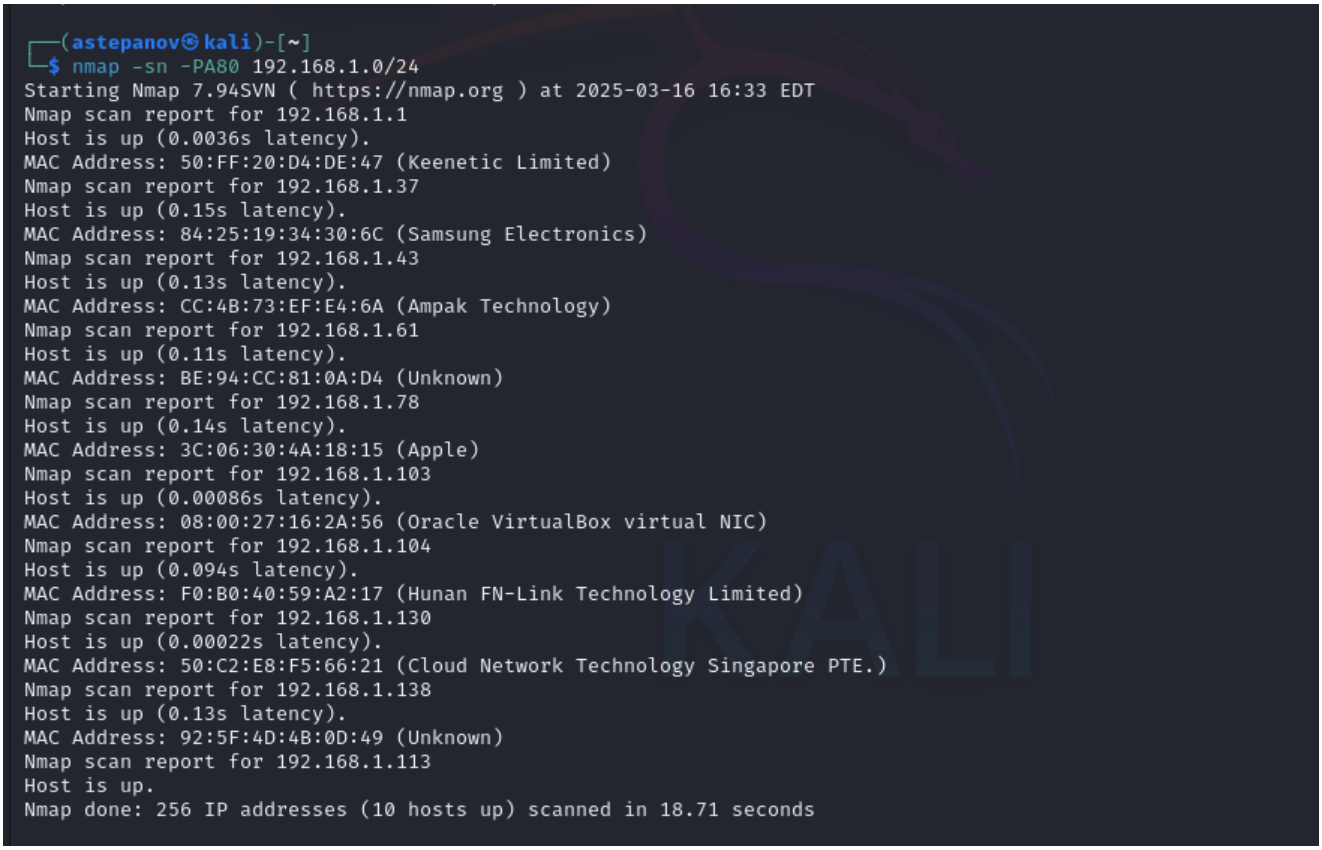


С машины Kali Linux

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

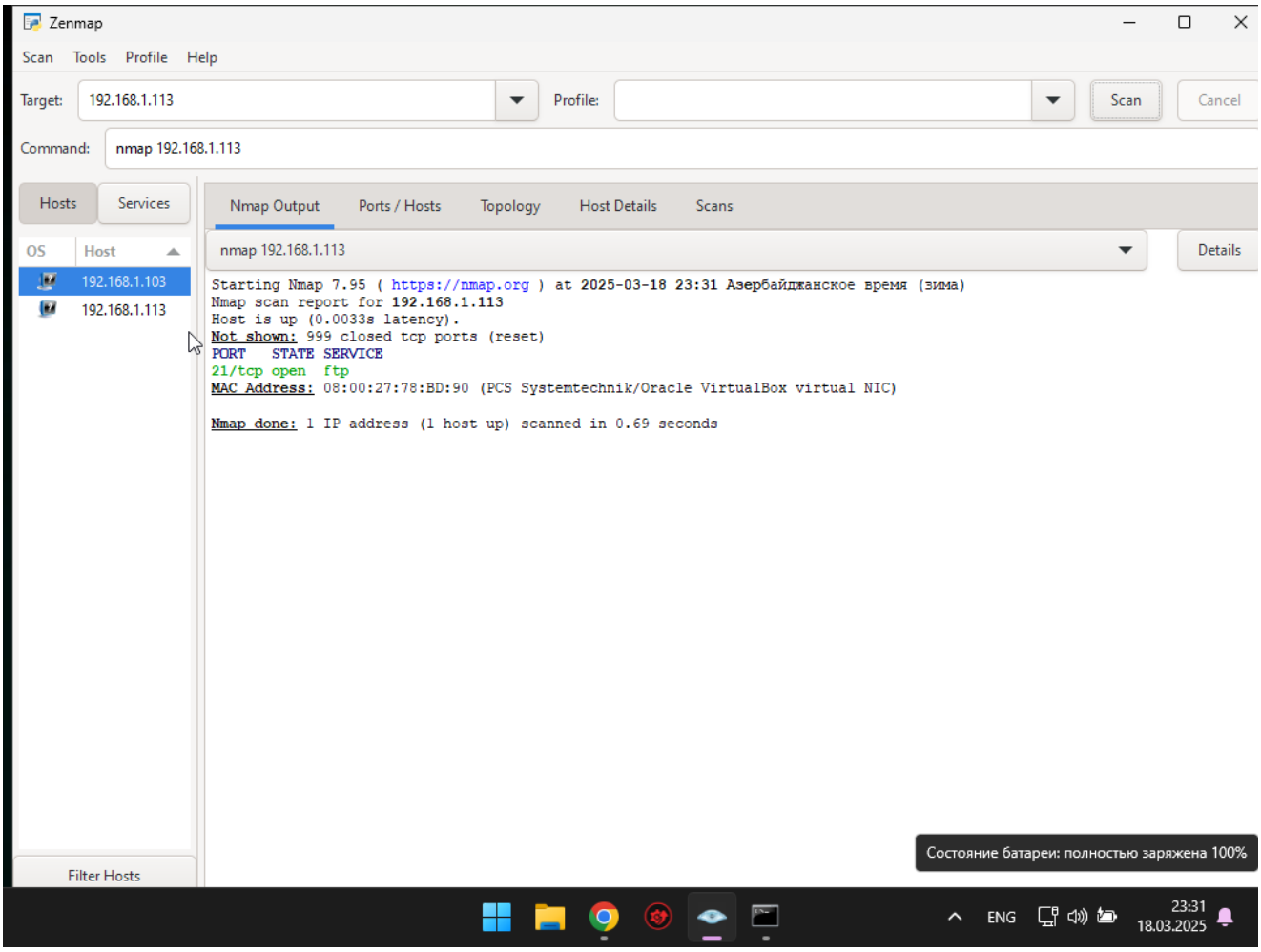
```
┌──(astepanov㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 16:39 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0035s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.16s latency).
MAC 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
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

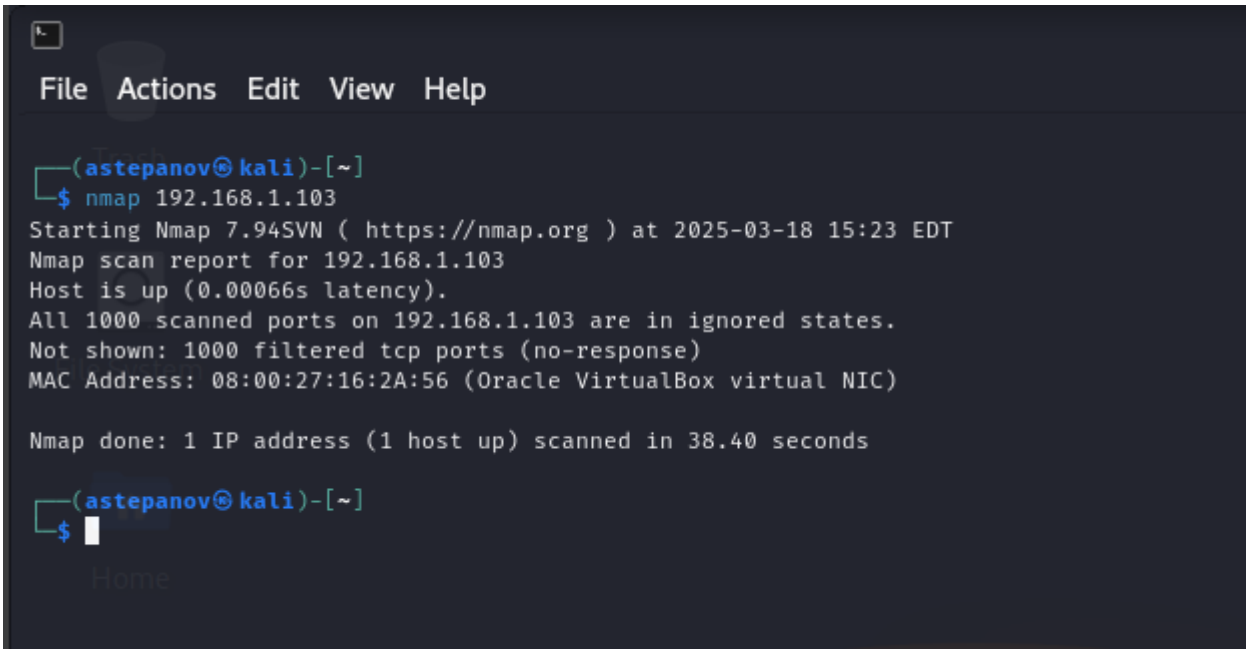
Сканирование с Windows



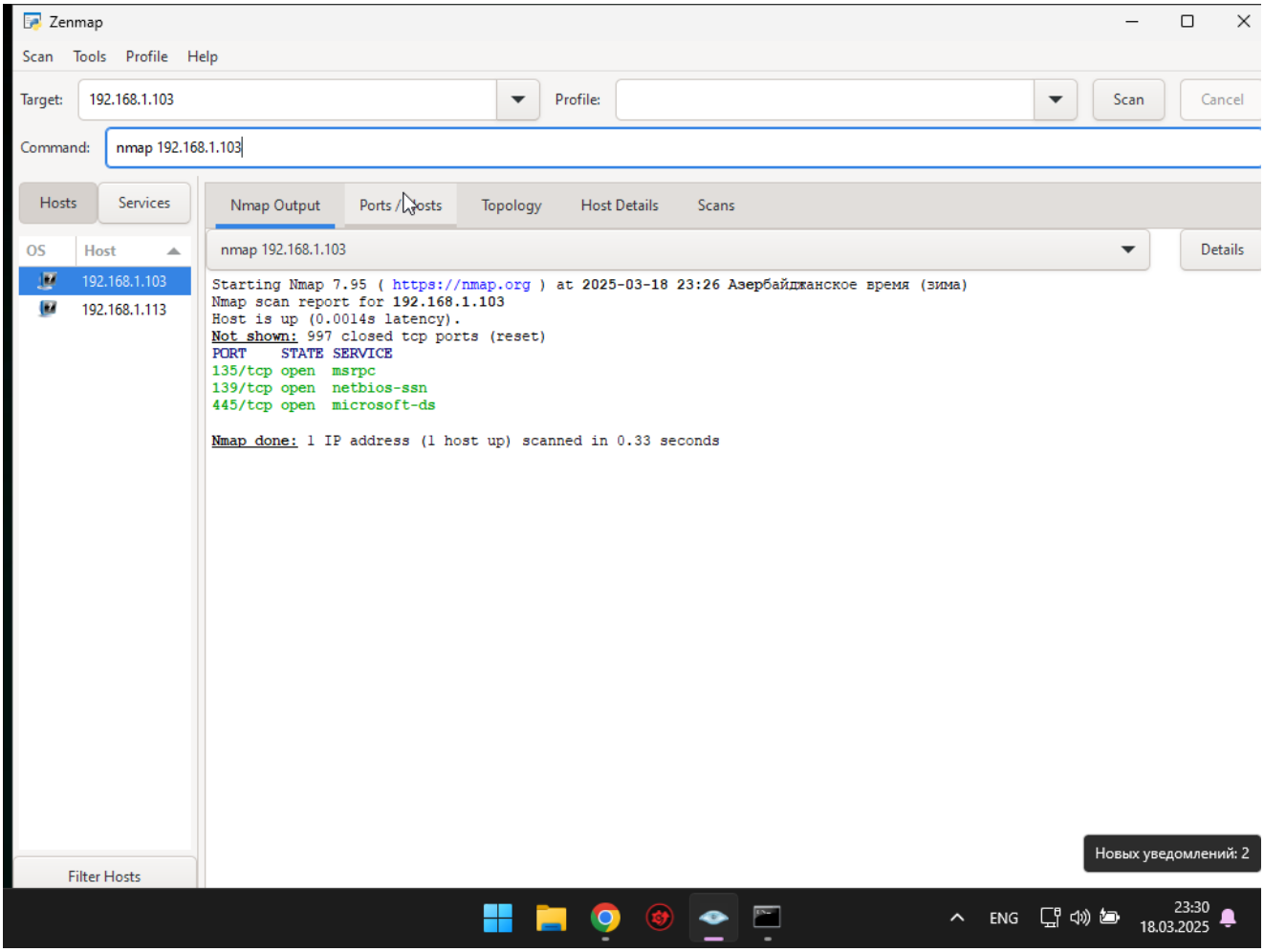
Видим, что на хосте Kali открыт 21-ый порт, порт управляющего соединения FTP, который был открыт в рамках предудыщей ЛР

Сканирование с Kali Linux

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

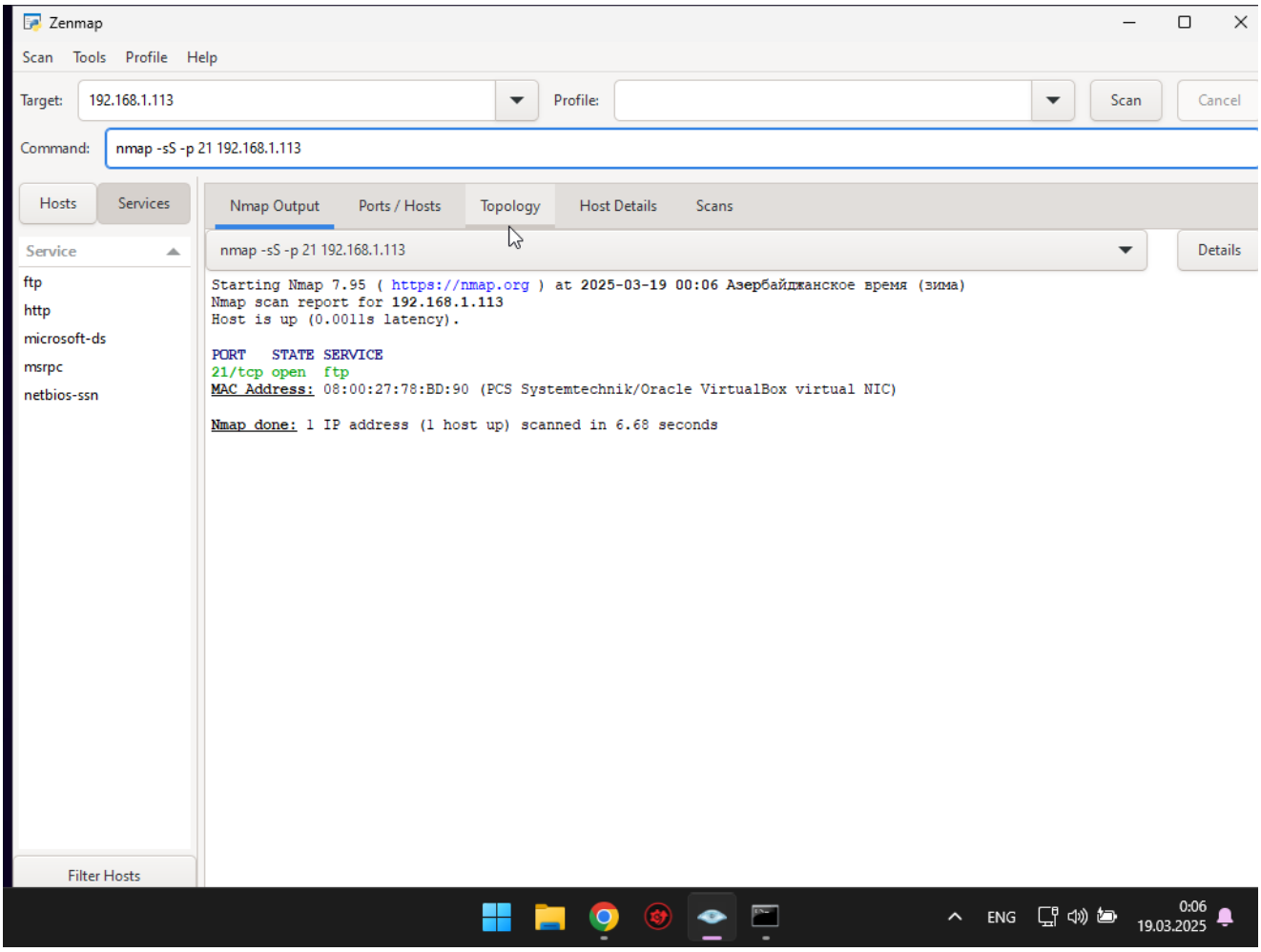


Хотя если Windows-хост будет сканировать сам себя, то результат покажет наличие открытых tcp-портов:



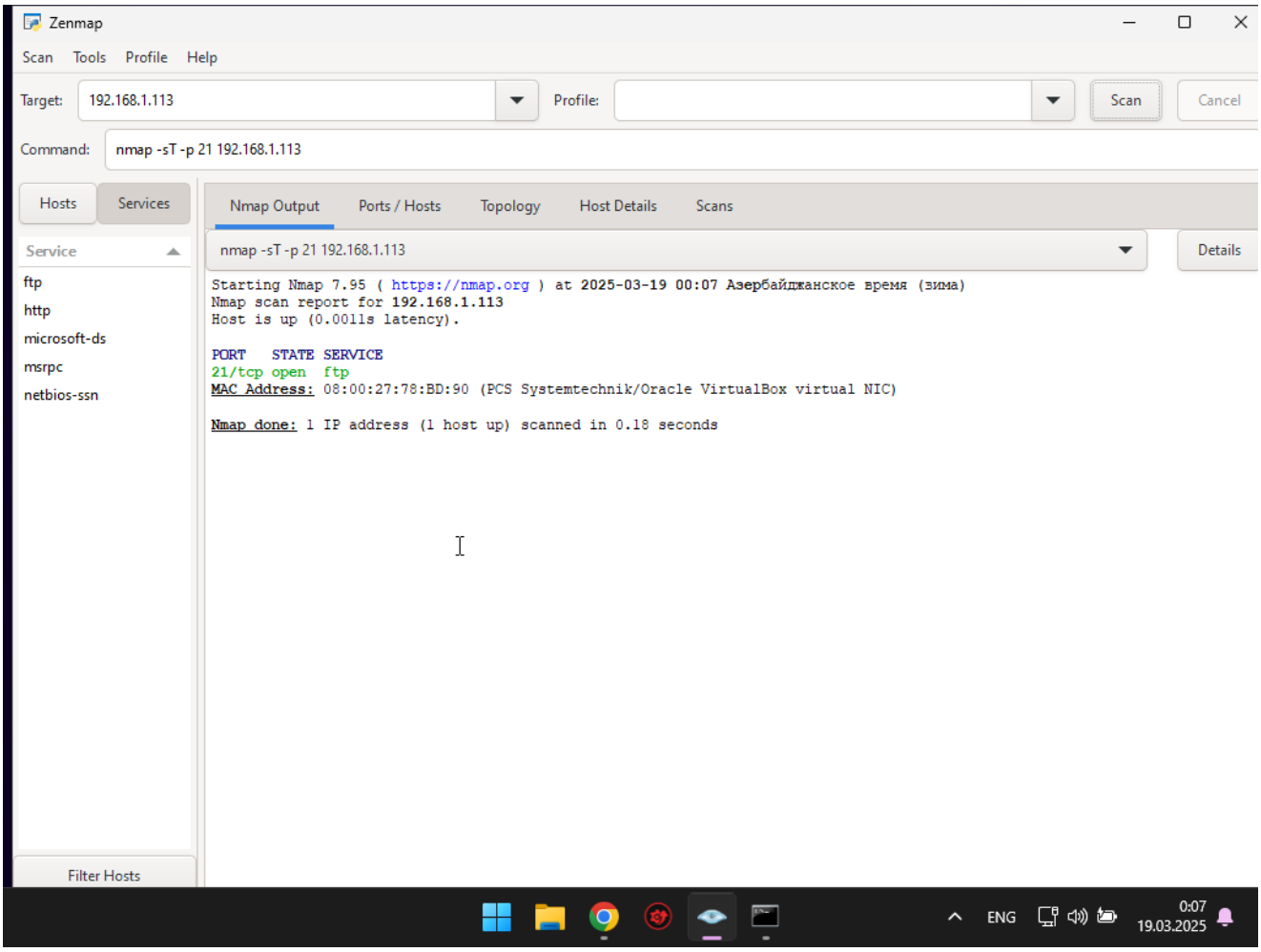
Шаг 6. Выберите какой-нибудь порт, полученный в пункте 4 (видимо речь про п.5, так что берем 21-ый), и просканируйте его с помощью методов TCP SYN Scan, TCP Connect Scan, UDP Scan, TCP FIN Scan, TCP NULL Scan, TCP Xmas Scan и TCP ACK Scan. Сделайте скриншот каждого результата.

TCP SYN Scan



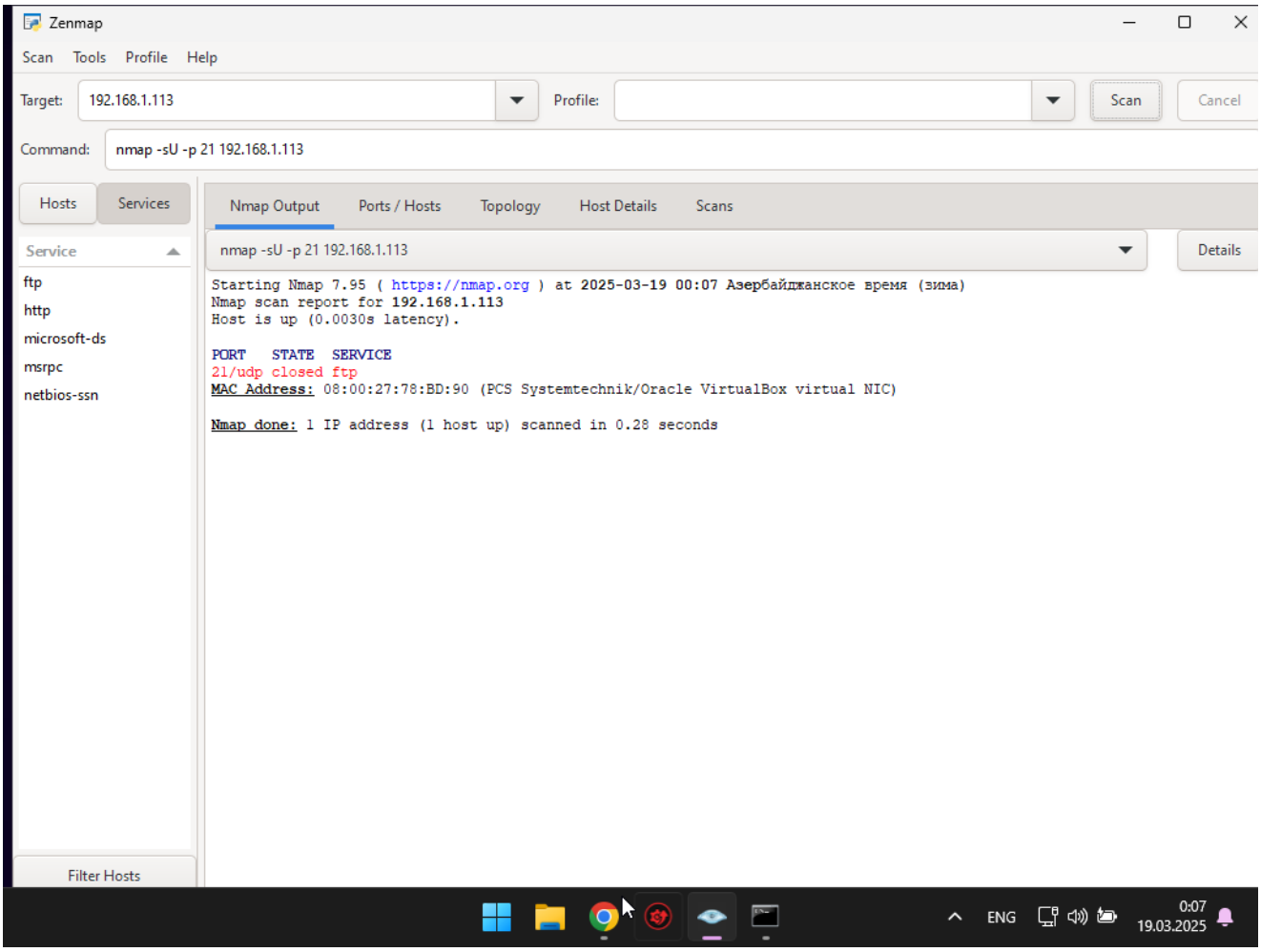
Порт открыт

TCP Connect Scan



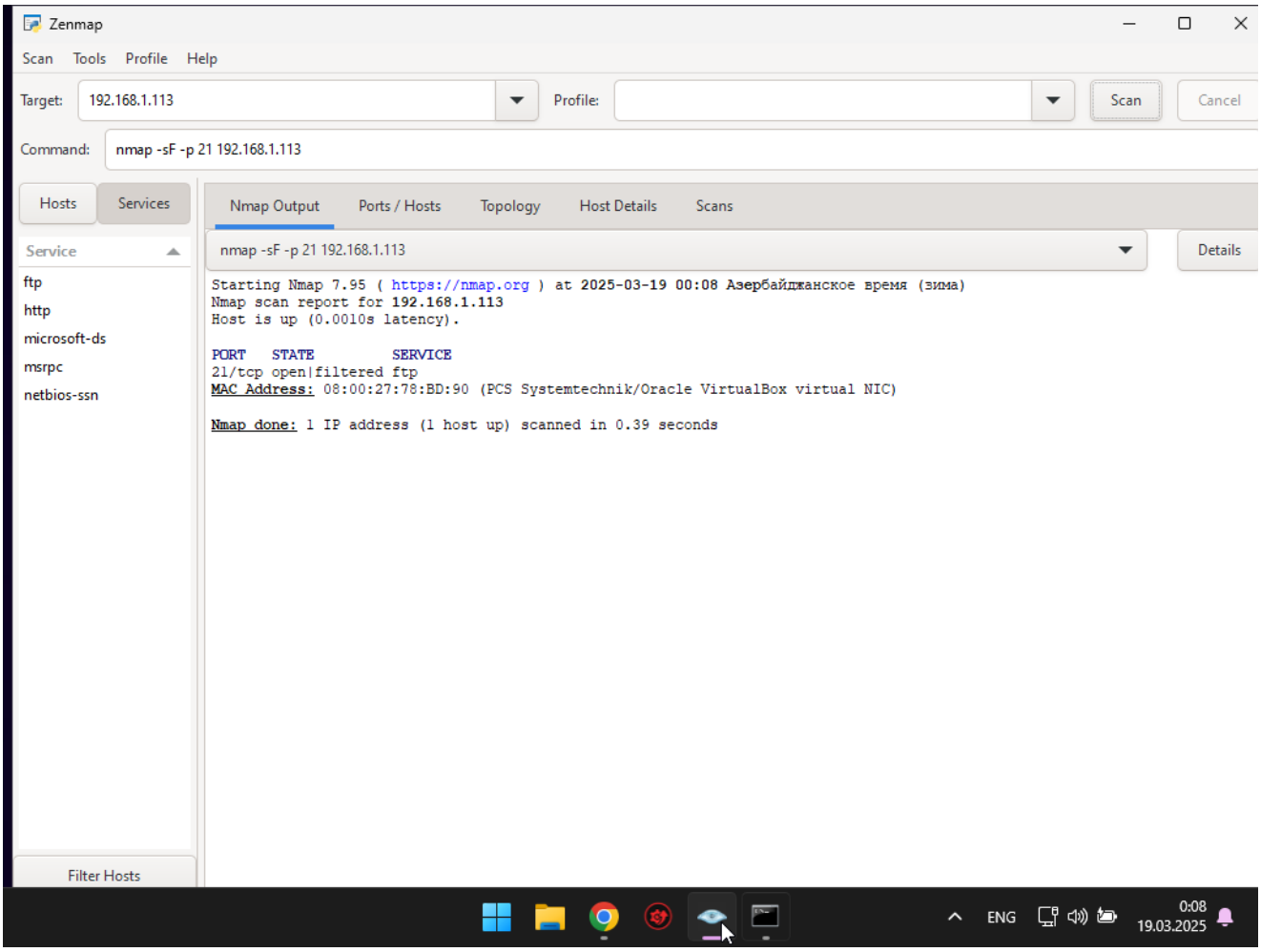
Порт открыт

UDP Scan



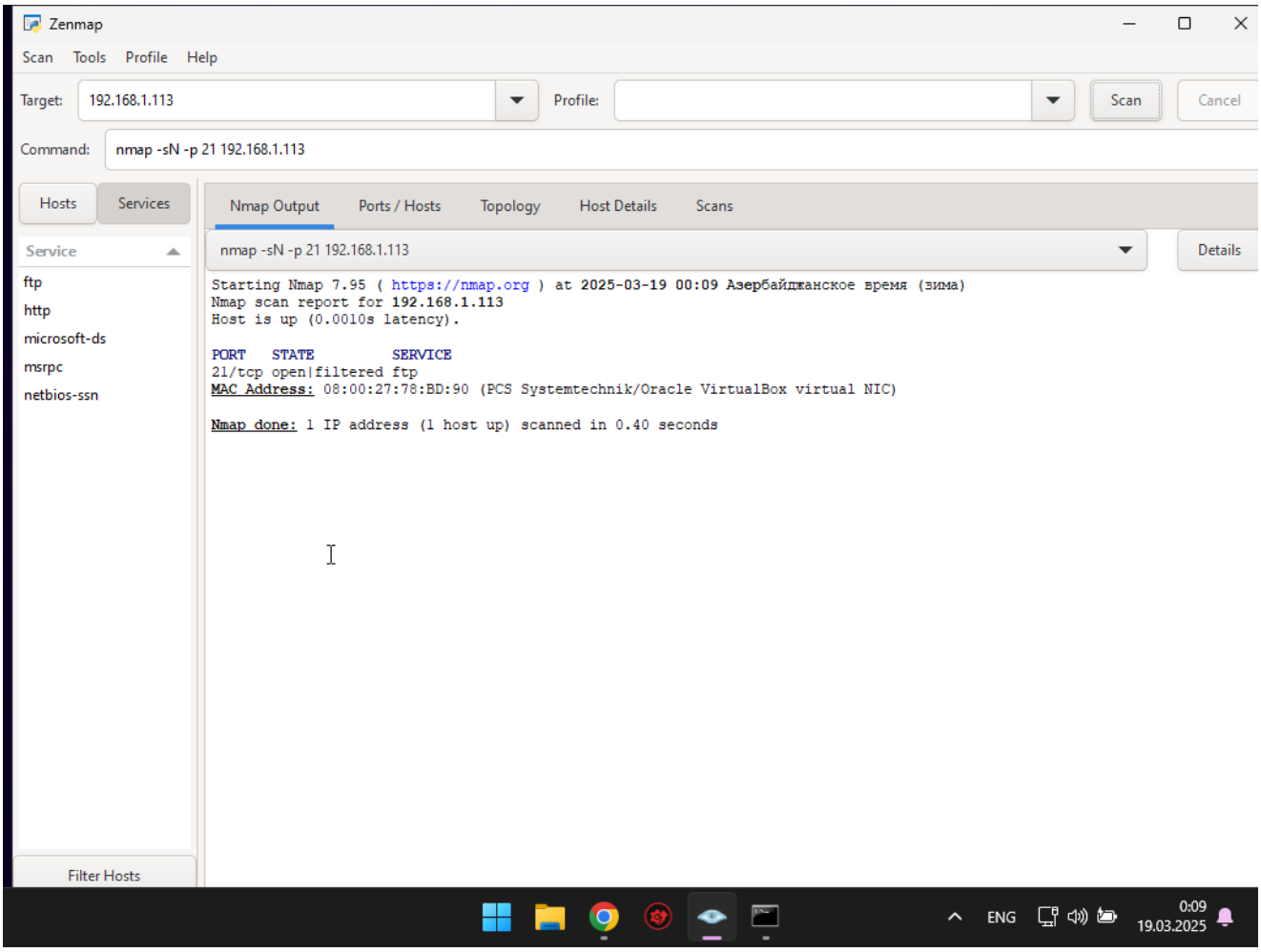
Порт закрыт. Видимо, потому что это не UDP порт

TCP FIN Scan



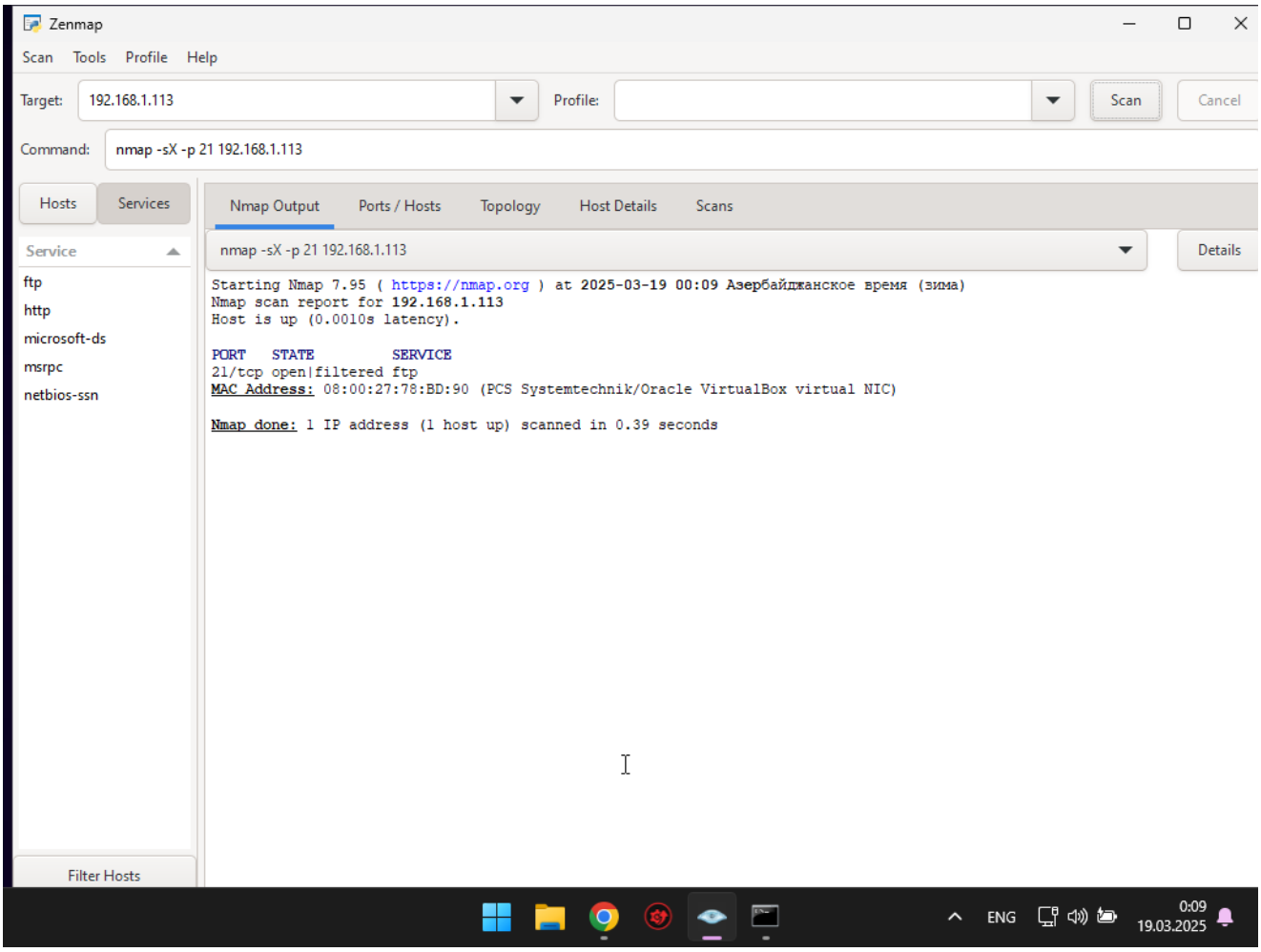
Порт открыт и не отвечает на нестандартные TCP-пакеты.

TCP NULL Scan



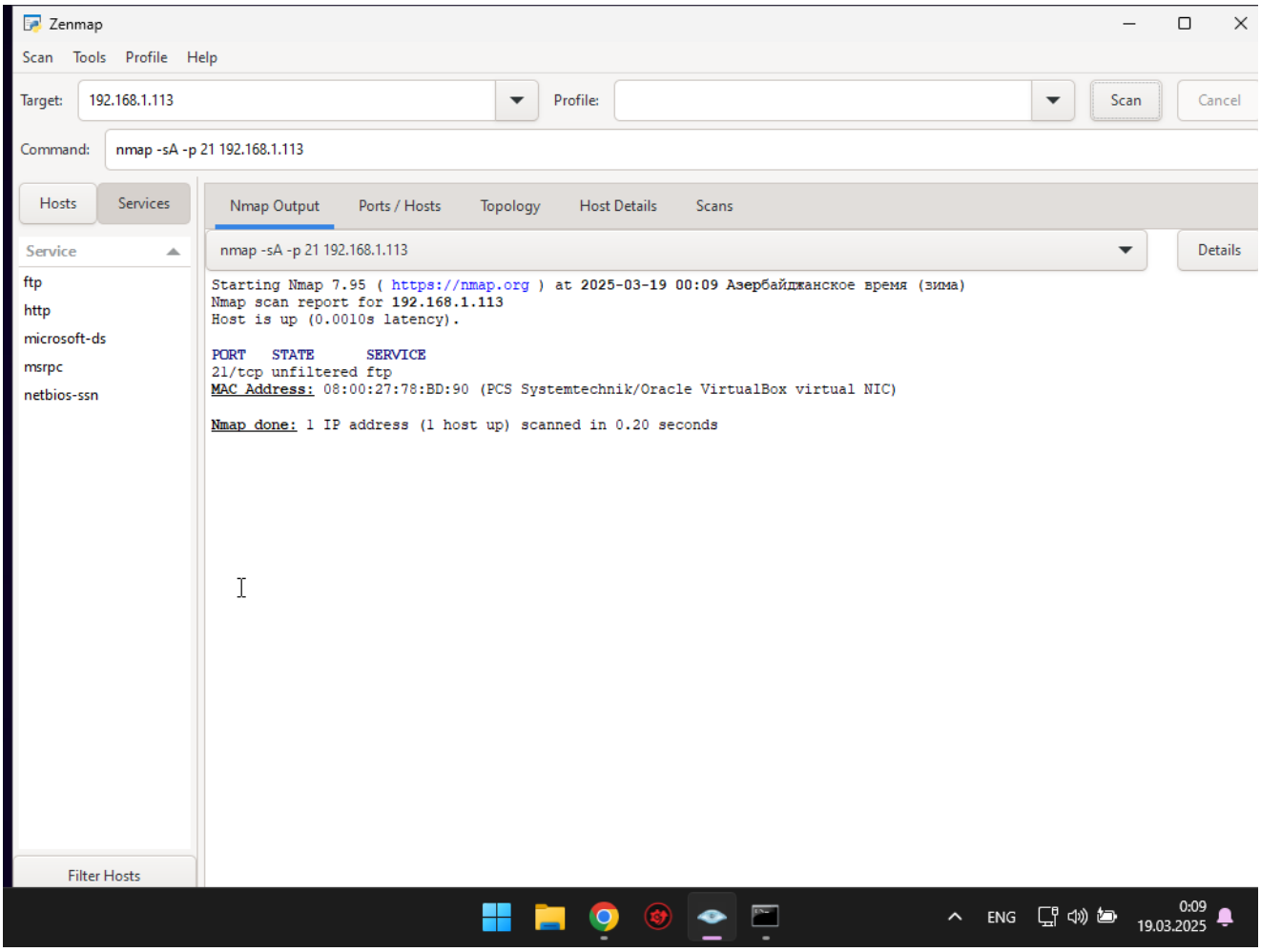
Порт открыт и не отвечает на нестандартные TCP-пакеты.

TCP Xmas Scan



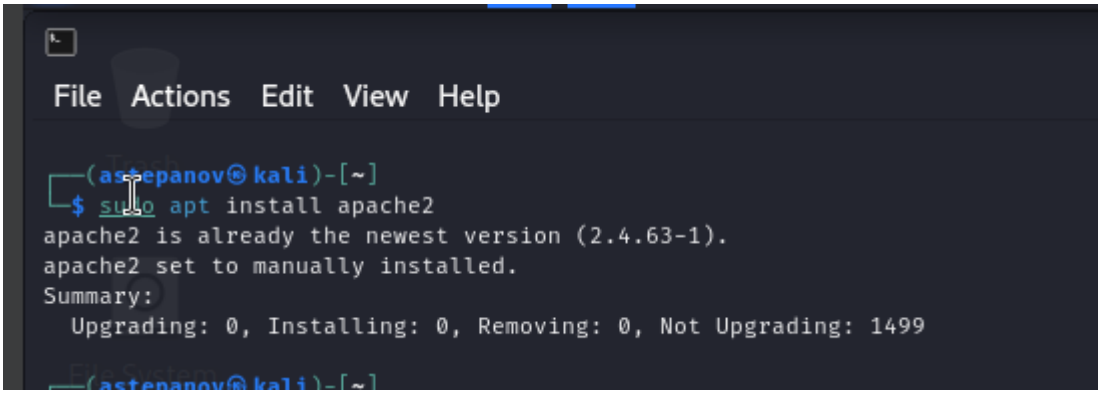
Порт открыт и не отвечает на нестандартные TCP-пакеты.

TCP ACK Scan



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



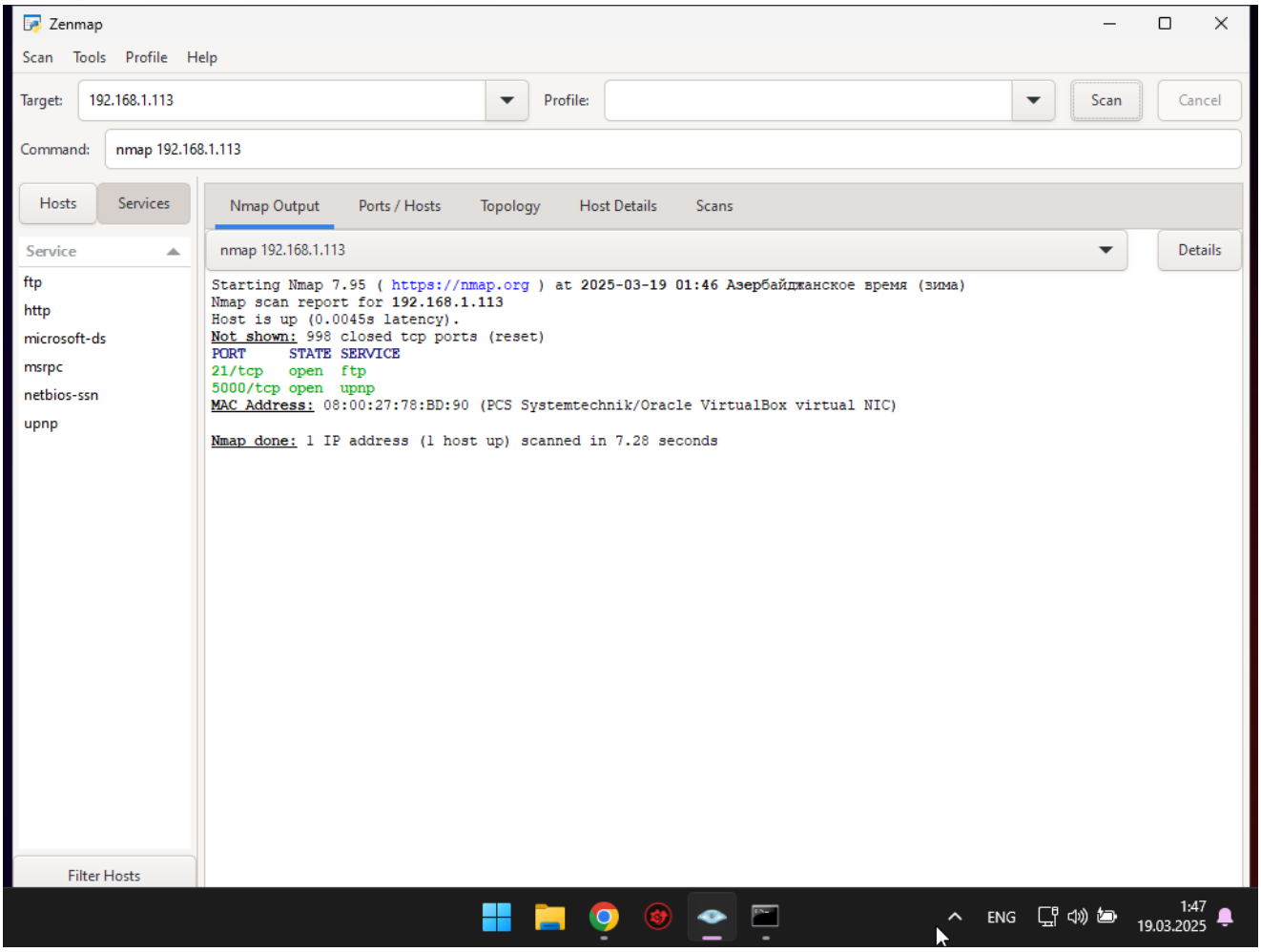
Шаг 8. Настройка и запуск веб-сервера Apache2

Прописываем слушать 5000 порт в конфиге

Перезапускаем сервер для того, чтобы подхватился конфиг

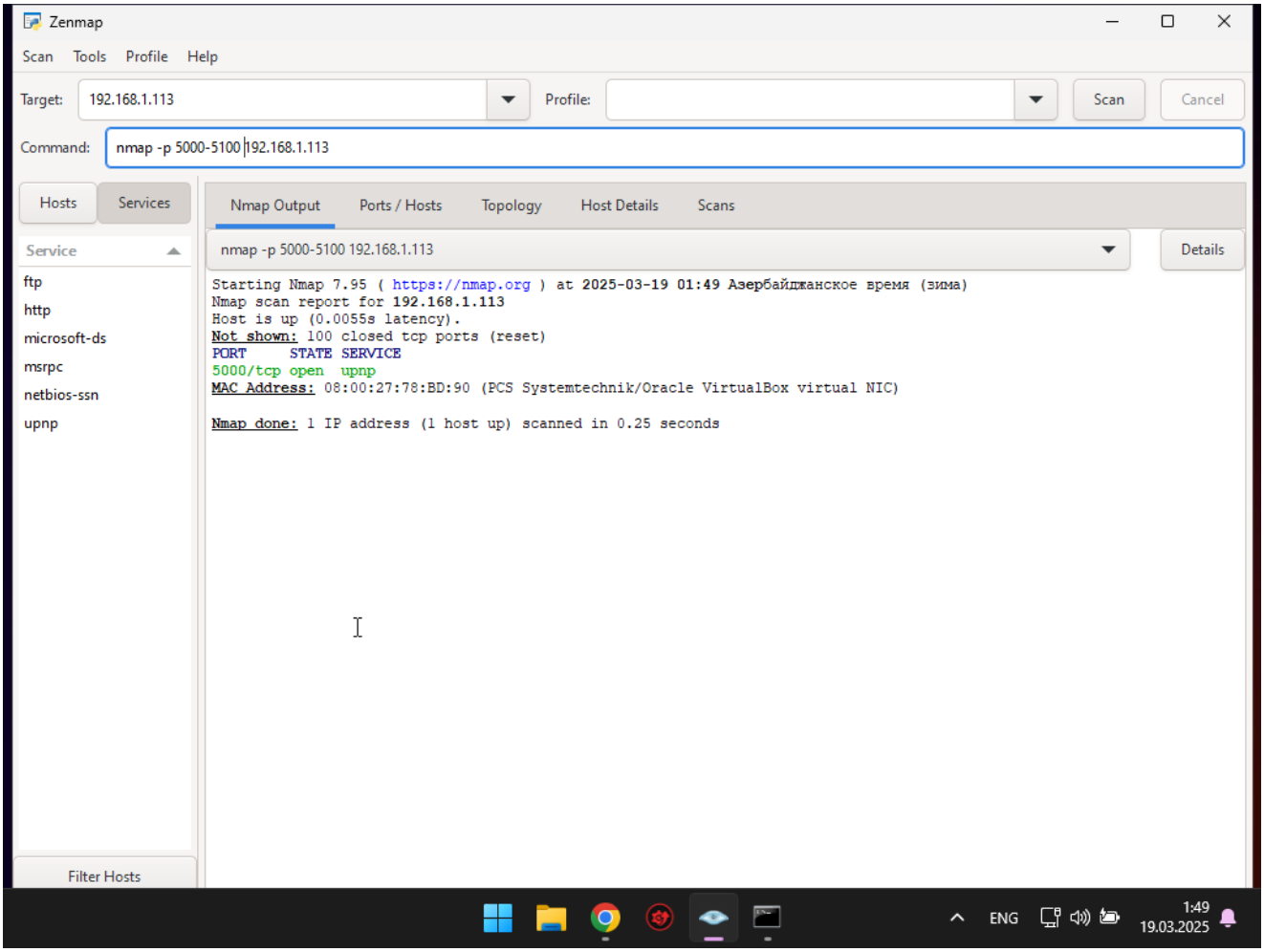
Шаг 9. С Windows повторите команду из пункта 4 (видимо речь про п.5). Появился ли ранее указанный порт?

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 соответвуют пункам из задания, поэтому остается только догадываться, что имелось ввиду, видимо речь снова про 5000-ый порт)

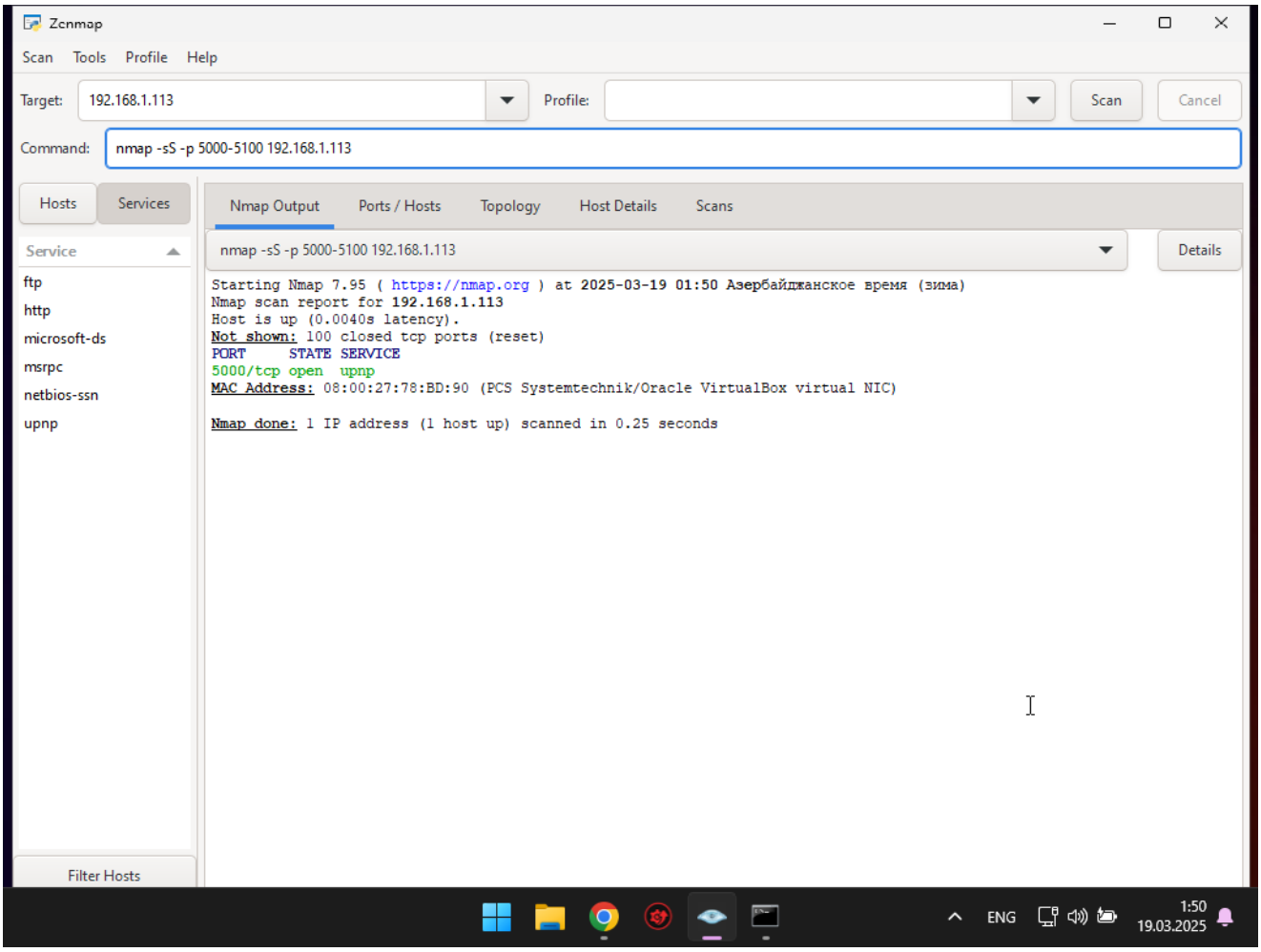
Сканируем дианазон портов 5000-5100



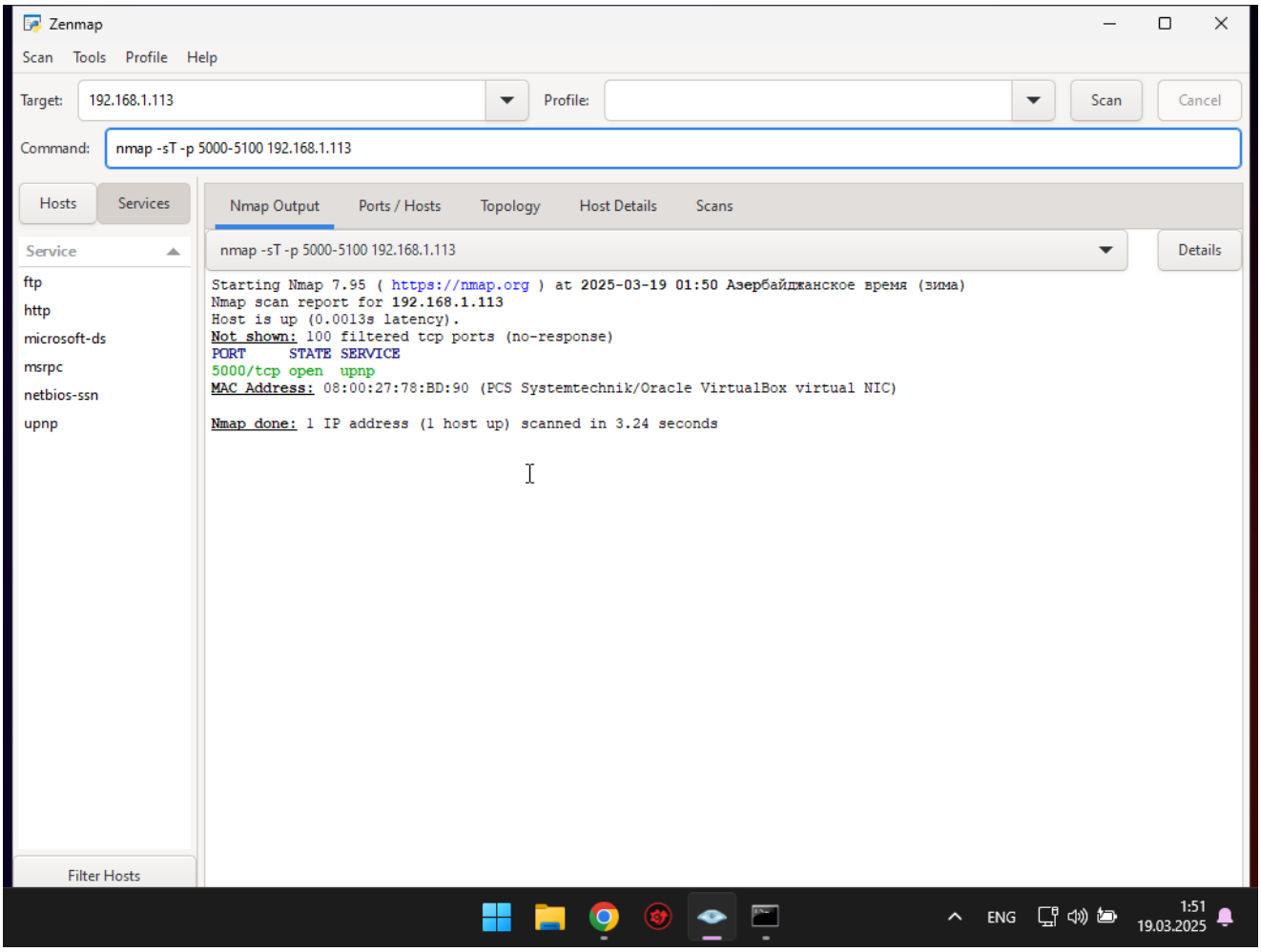
В общем-то, результат довольно очевидный - видим открытый 5000-ый порт

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

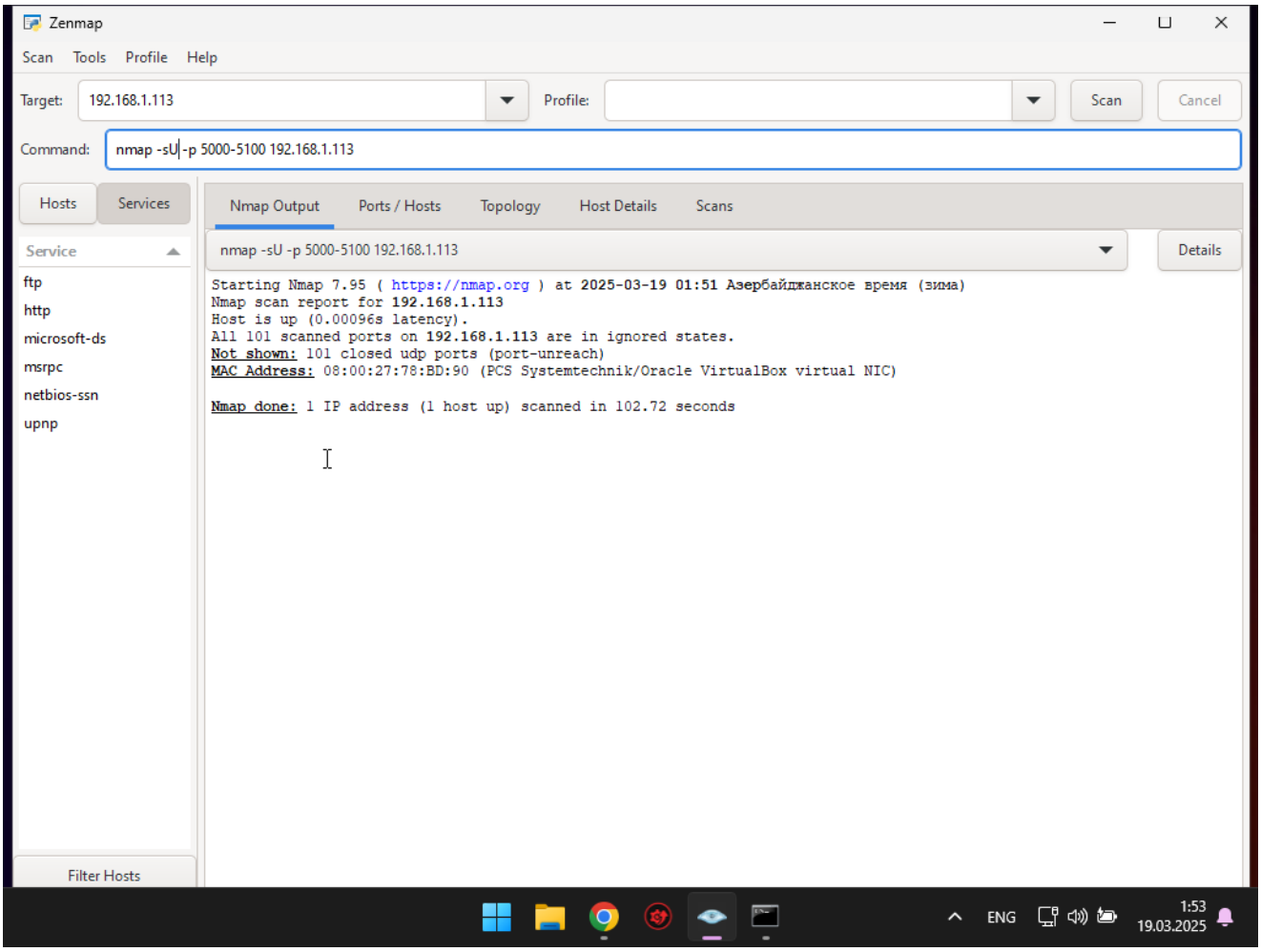
TCP SYN Scan



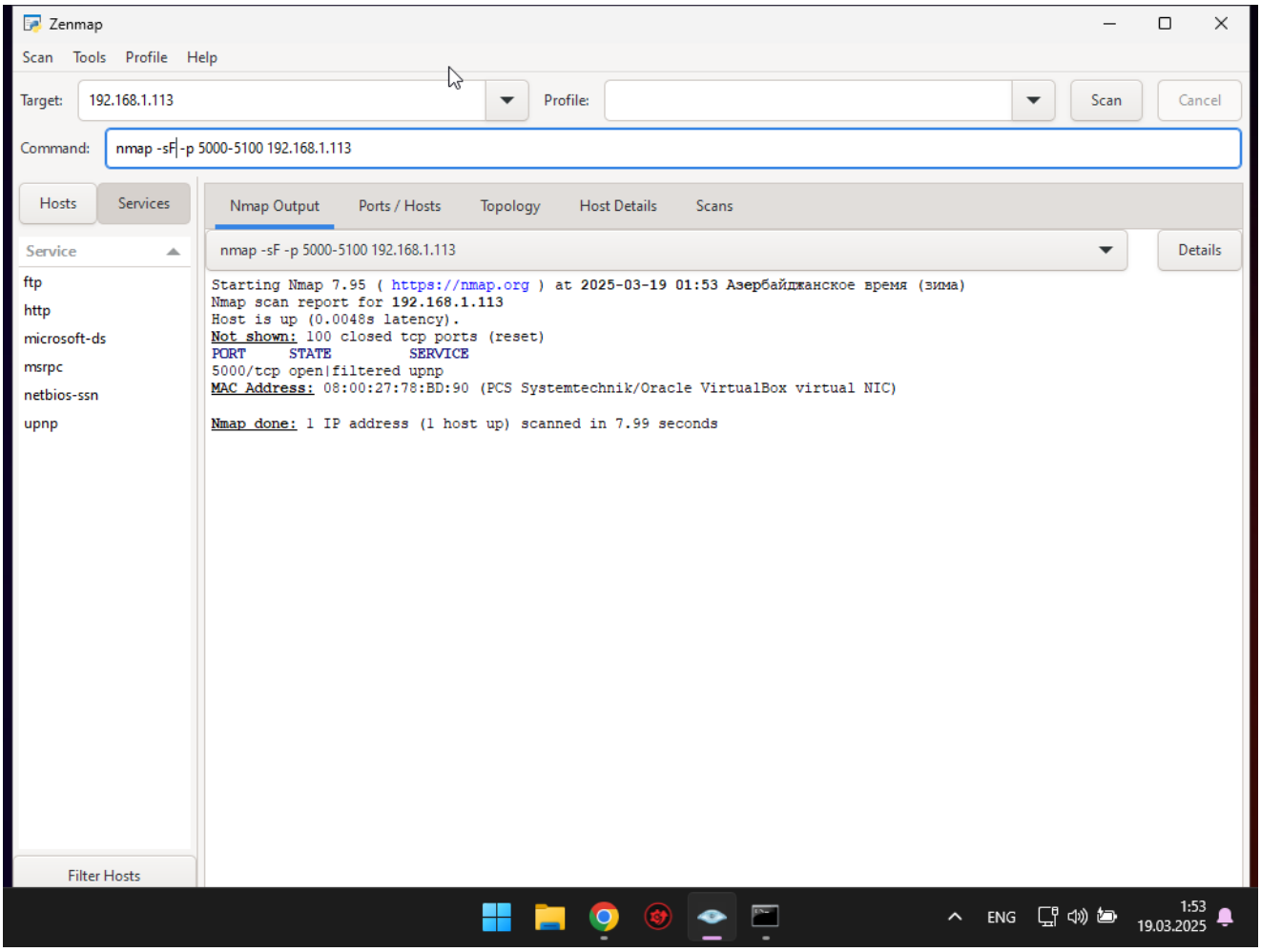
TCP Connect Scan


Zenmap
Scan Tools Profile Help
Target: 192.168.1.113
Profile:
Scan
Cancel
Command: nmap -sT -p 5000-5100 192.168.1.113
Hosts
Services
Service
ftp
http
microsoft-ds
msrpc
netbios-ssn
upnp
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sT -p 5000-5100 192.168.1.113
Details
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 (0.0013s latency).
Not shown: 100 filtered tcp ports (no-response)
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 3.24 seconds
ENG
1:51
19.03.2025

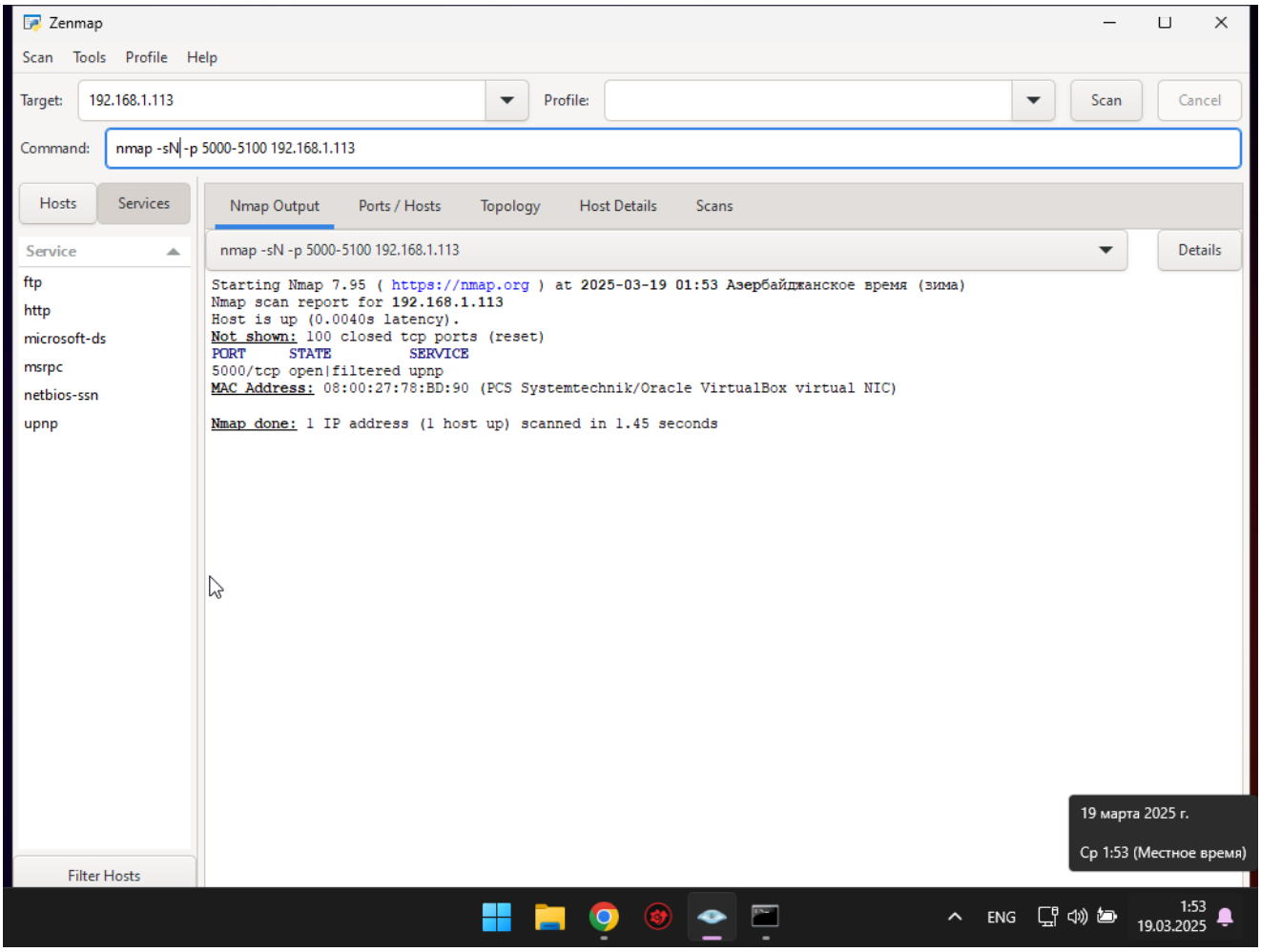
UDP Scan


Zenmap
Scan Tools Profile Help
Target: 192.168.1.113
Profile:
Scan
Cancel
Command: nmap -sU -p 5000-5100 192.168.1.113
Hosts
Services
Service
ftp
http
microsoft-ds
msrpc
netbios-ssn
upnp
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sU -p 5000-5100 192.168.1.113
Details
Starting Nmap 7.95 (https://nmap.org) at 2025-03-19 01:51 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.00096s latency).
All 101 scanned ports on 192.168.1.113 are in ignored states.
Not shown: 101 closed udp ports (port-unreach)
MAC Address: 08:00:27:78:BD:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 102.72 seconds
ENG
1:53
19.03.2025

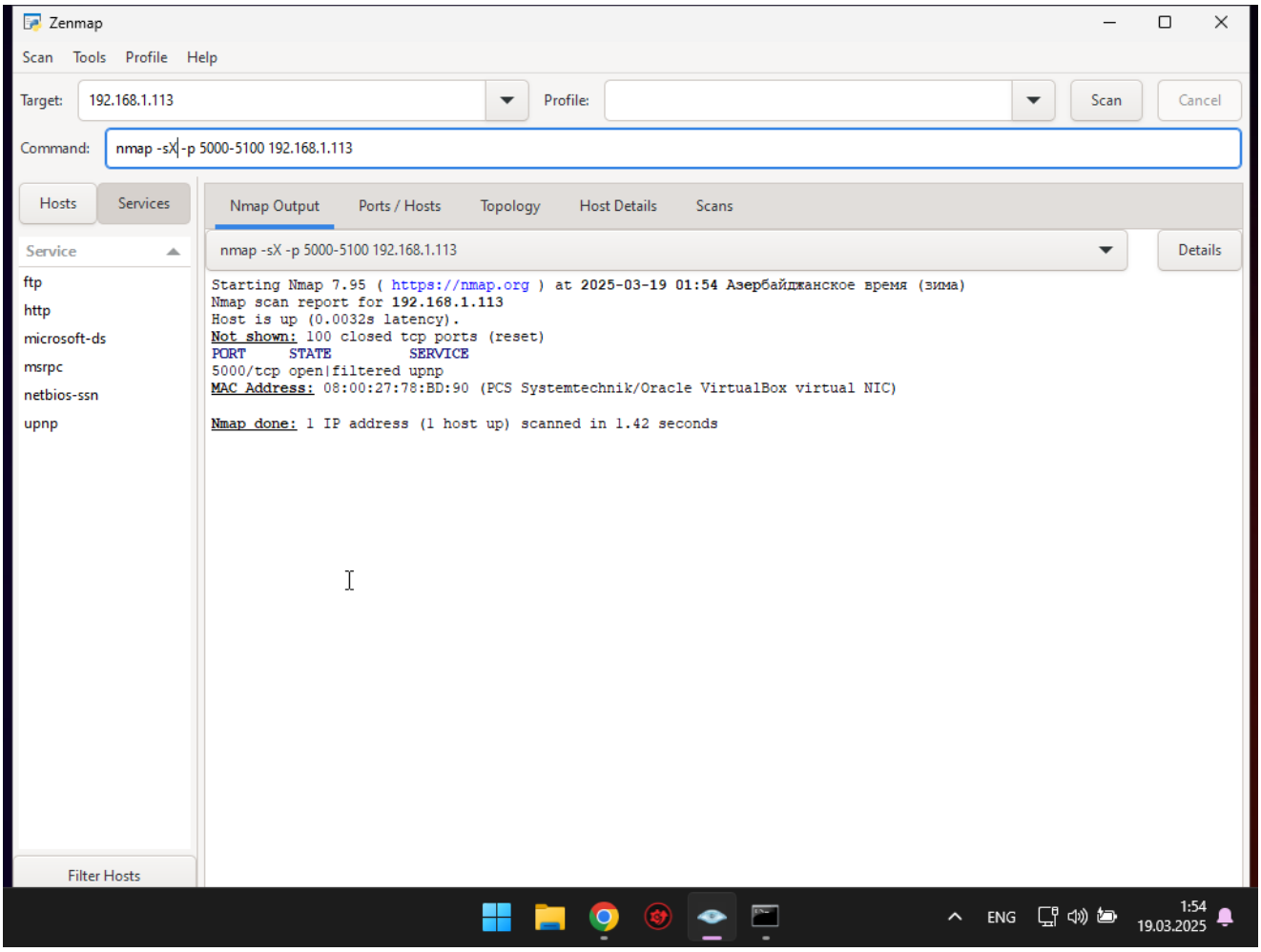
TCP FIN Scan



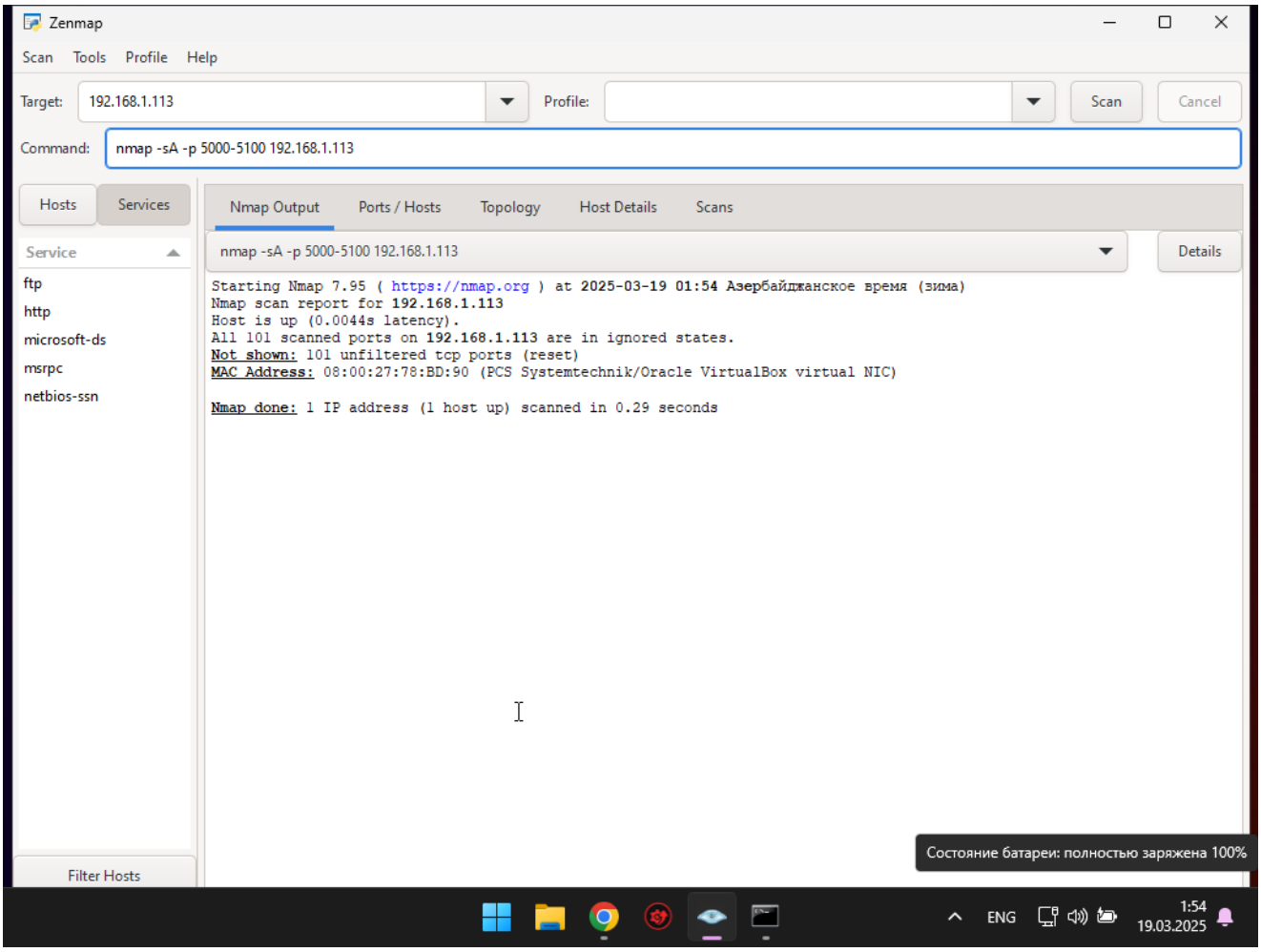
TCP NULL Scan



TCP Xmas Scan

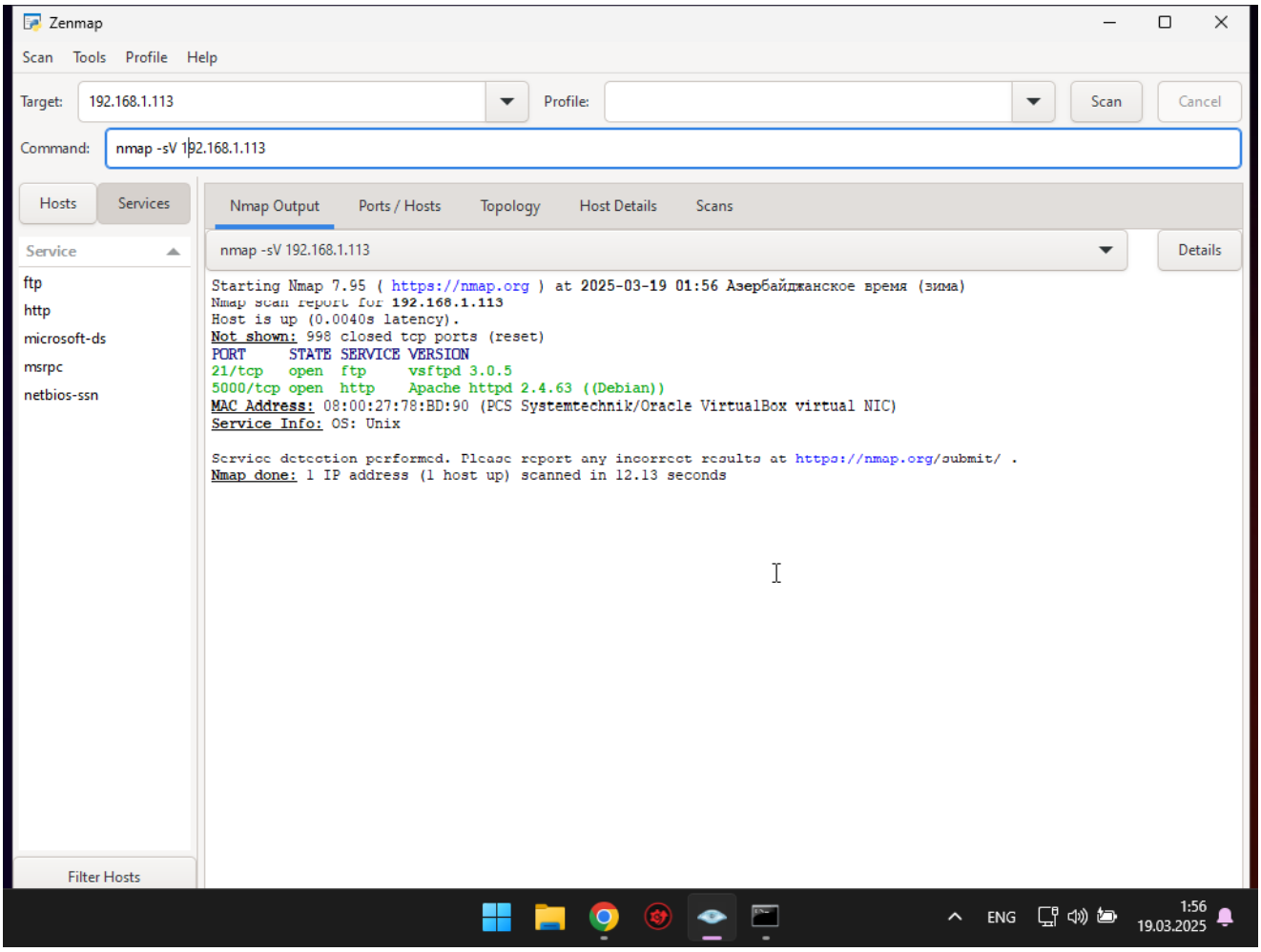

Zenmap
Scan Tools Profile Help
Target: 192.168.1.113
Profile:
Scan
Cancel
Command: nmap -sX -p 5000-5100 192.168.1.113
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Service
nmap -sX -p 5000-5100 192.168.1.113
Details
ftp
http
microsoft-ds
msrpc
netbios-ssn
upnp
Starting Nmap 7.95 (https://nmap.org) at 2025-03-19 01:54 Азербайджанское время (зима)
Nmap scan report for 192.168.1.113
Host is up (0.0032s latency).
Not shown: 100 closed tcp ports (reset)
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 1.42 seconds
Filter Hosts
ENG
1:54
19.03.2025

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.



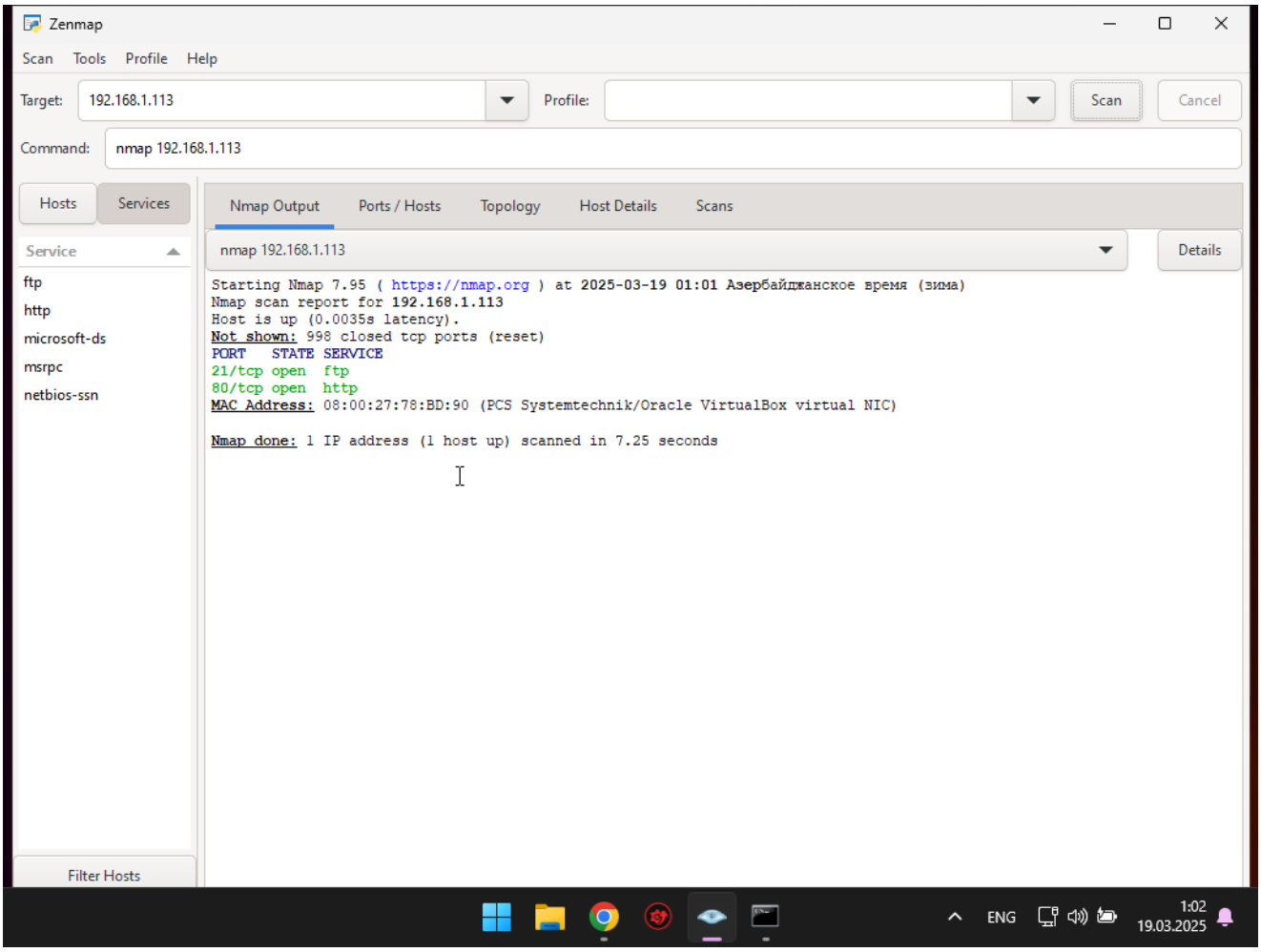
В результате сканирования мы видим не только открытые порты, но и версии сервисов, запущенных на них.
Видим, что на 21-ом порту запущен ftp-сервис vsftpd v.3.0.5, а на 5000-ом порту - веб-сервер Apache 2.4.63 Debian версия

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

Проверяем наличие psql (Postgresql предустановлена на Kali)

Запускаем сервис postgresql

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

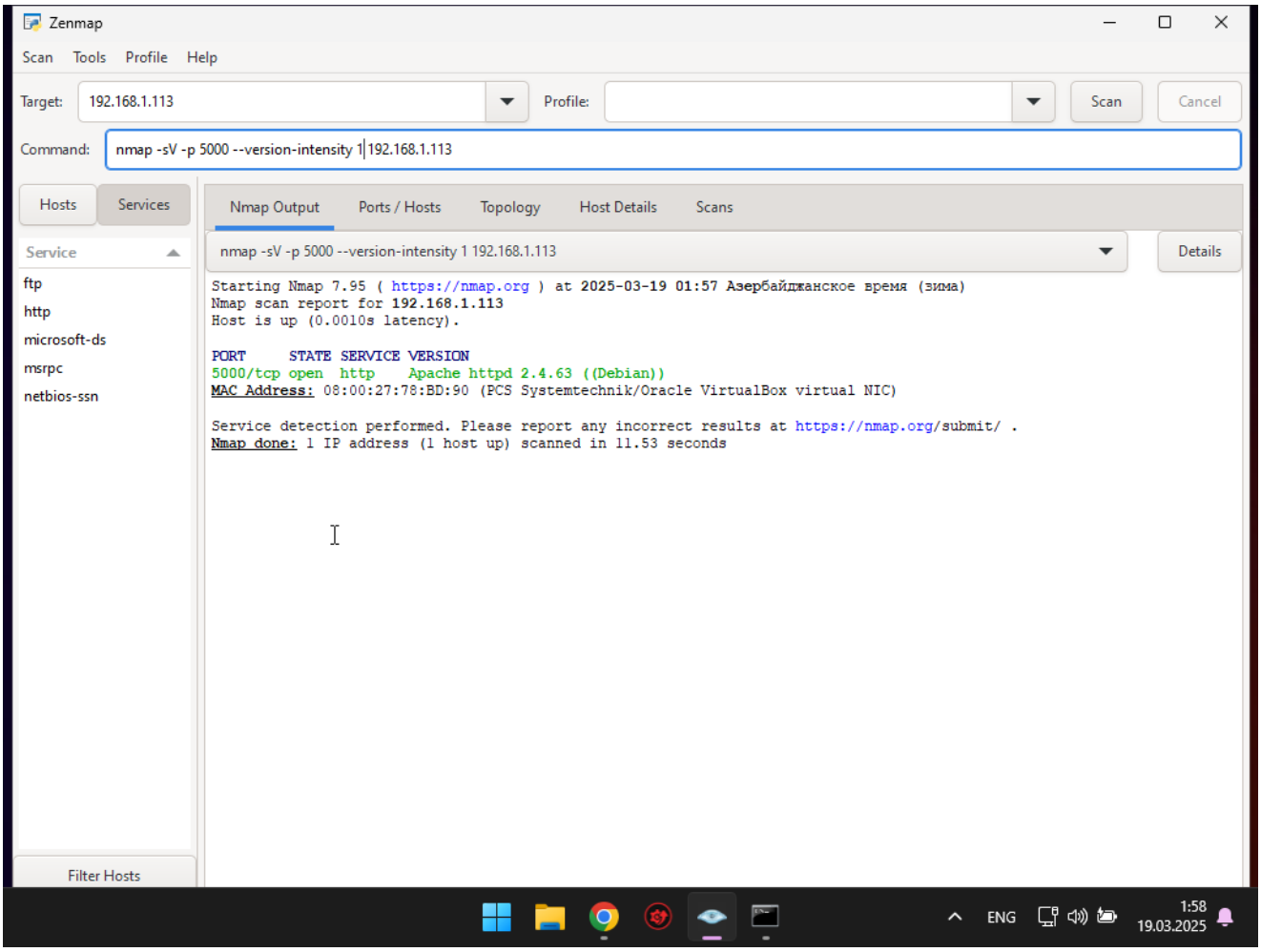


Результат сканирования не изменился. Видимо в задании предполагалось, что после запуска сервиса pgsql должен появиться порт pg, однако это требует дополнительной настройки сервиса, т.к. по умолчанию pg слушает только localhost.

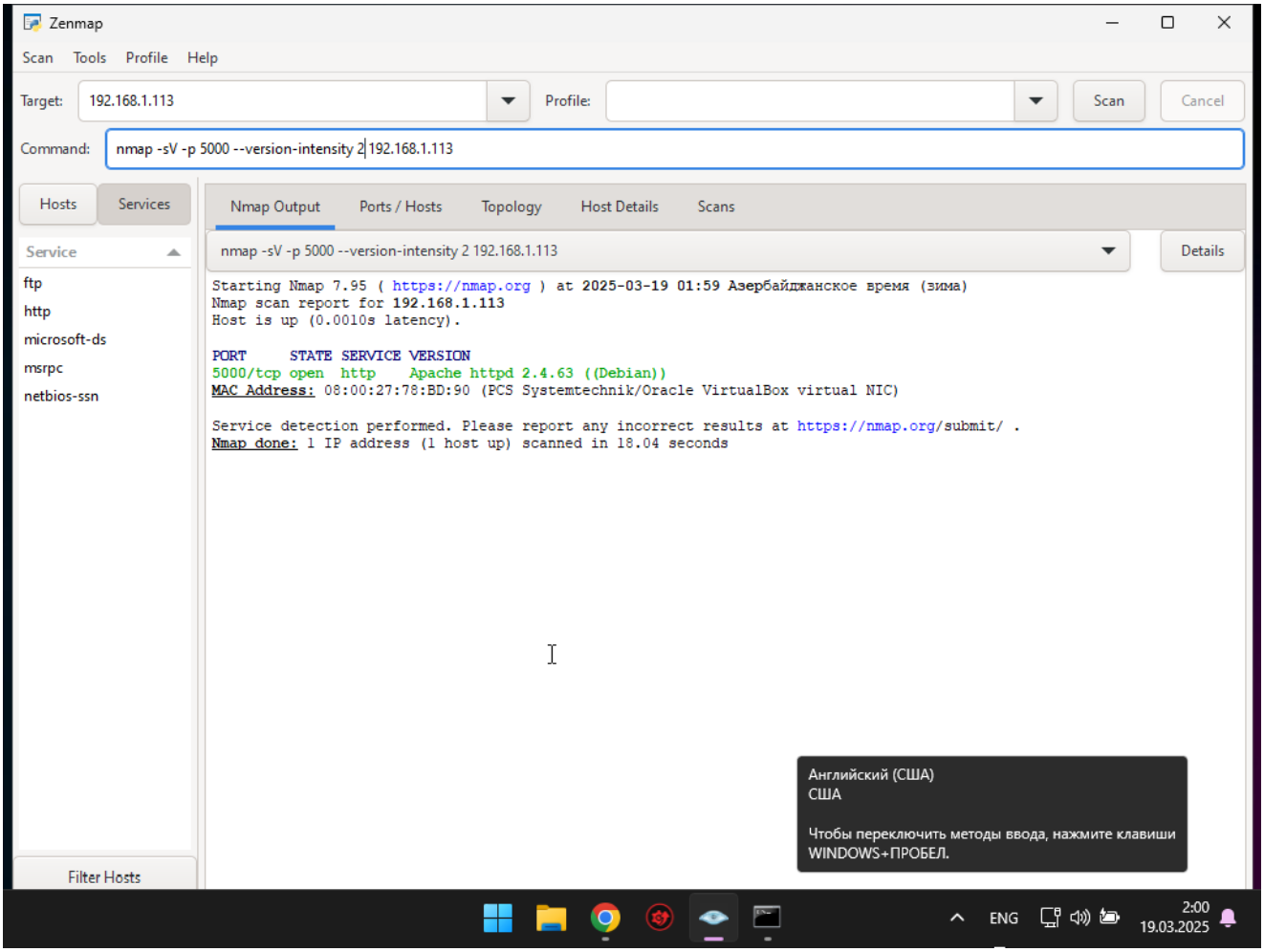
Шаг 13. Просканируйте нестандартный порт из 7 и порт Postgresql, указывая уровни интенсивности от 1 до 9. Сравните полученные результаты и опишите, какие результаты соответствуют действительности.

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

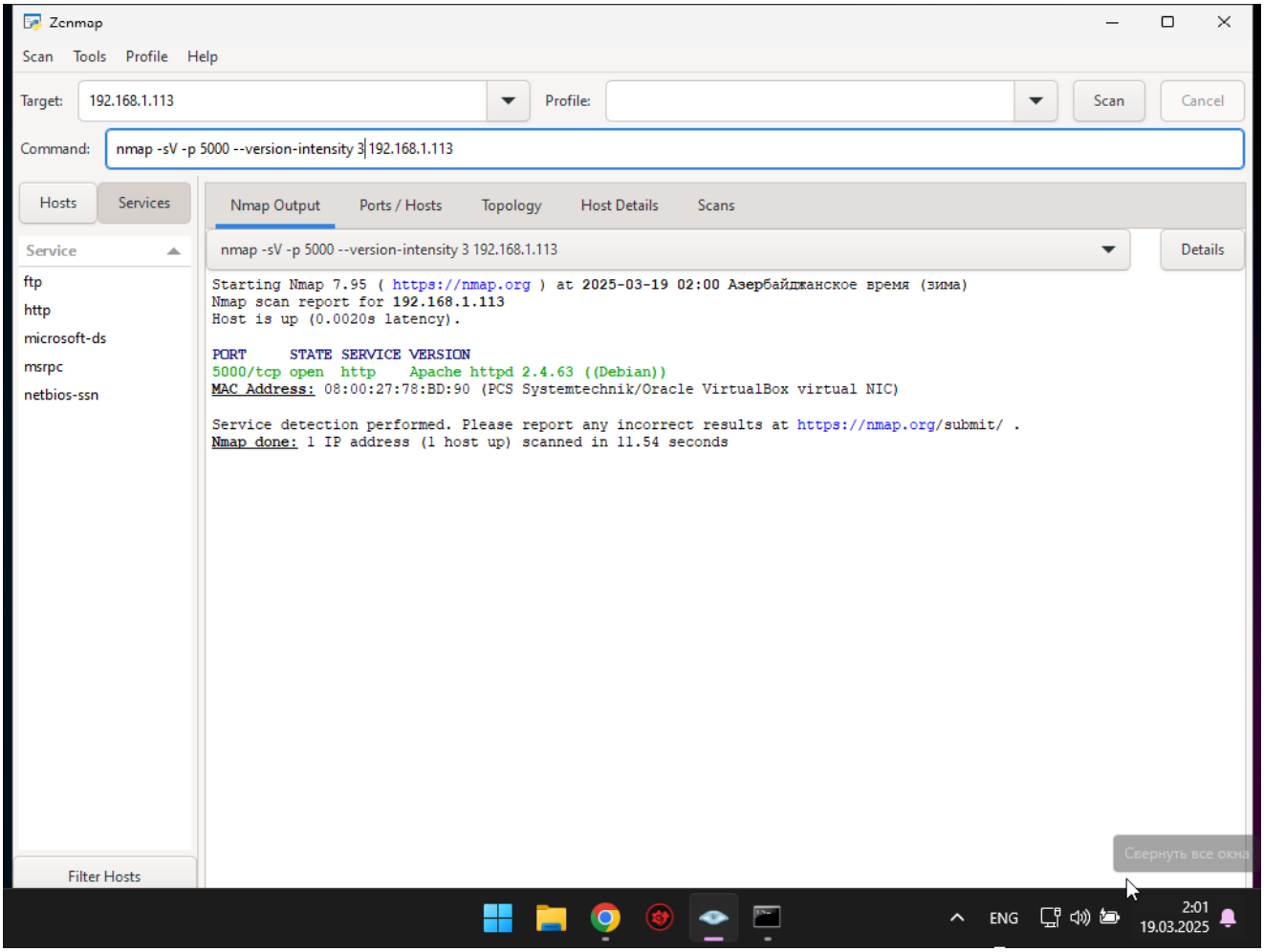
Интенсивность 1


Zenmap
Scan Tools Profile Help
Target: 192.168.1.113
Profile:
Scan
Cancel
Command: nmap -sV -p 5000 --version-intensity 1 192.168.1.113
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 1 192.168.1.113
Details
Starting Nmap 7.95 (https://nmap.org) at 2025-03-19 01:57 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 11.53 seconds
ENG
1:58
19.03.2025

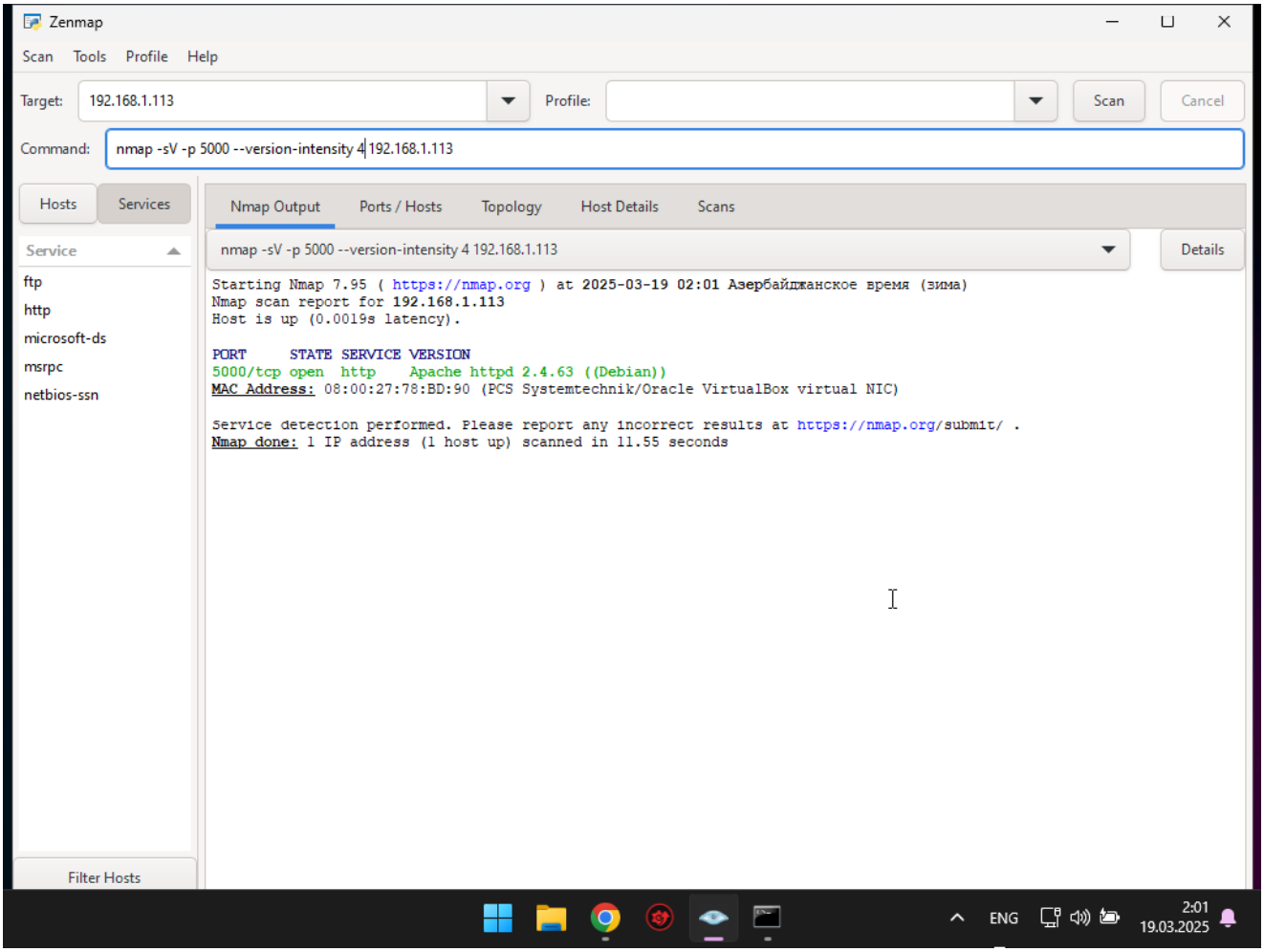
Интенсивность 2



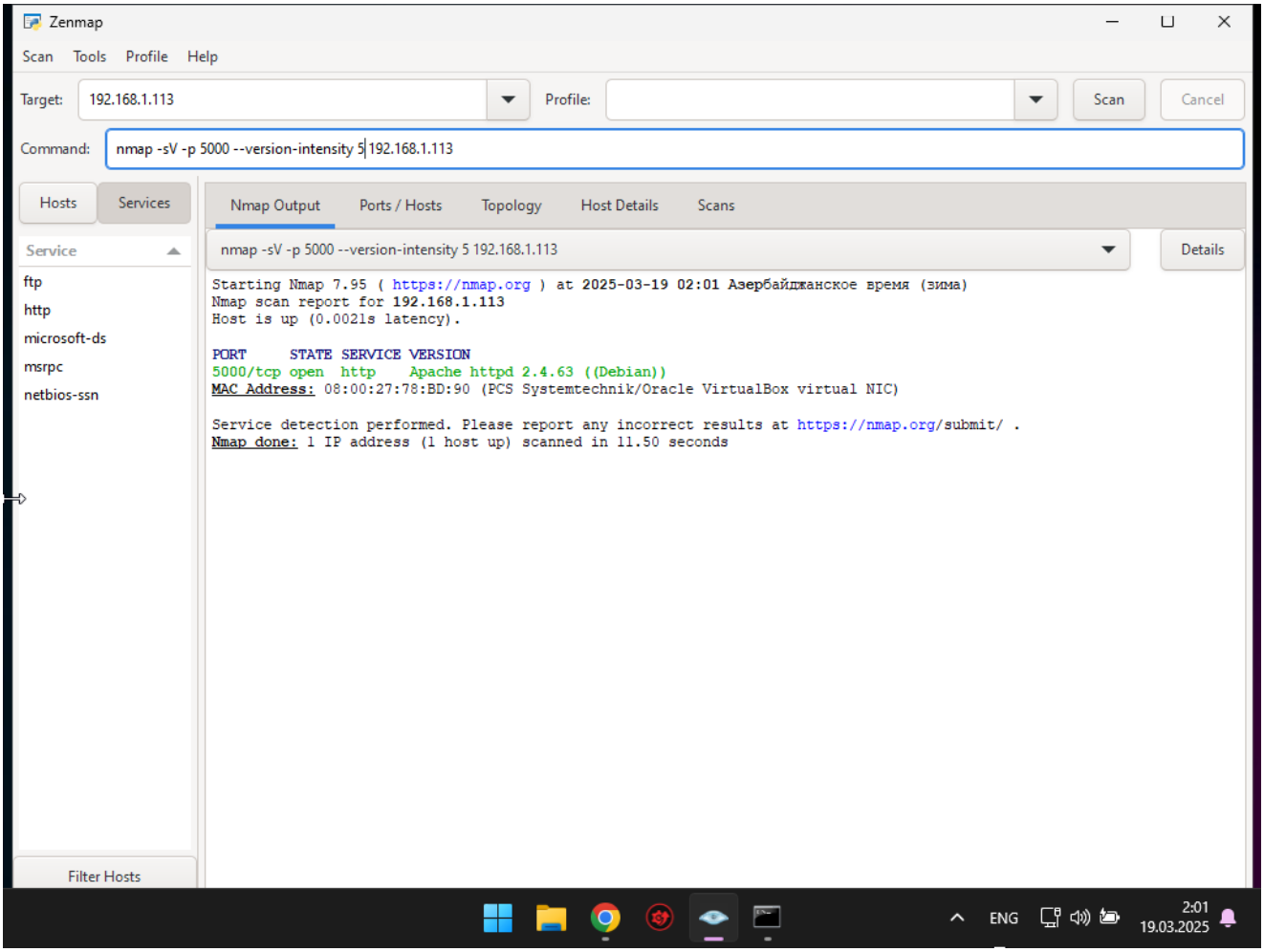
Интенсивность 3



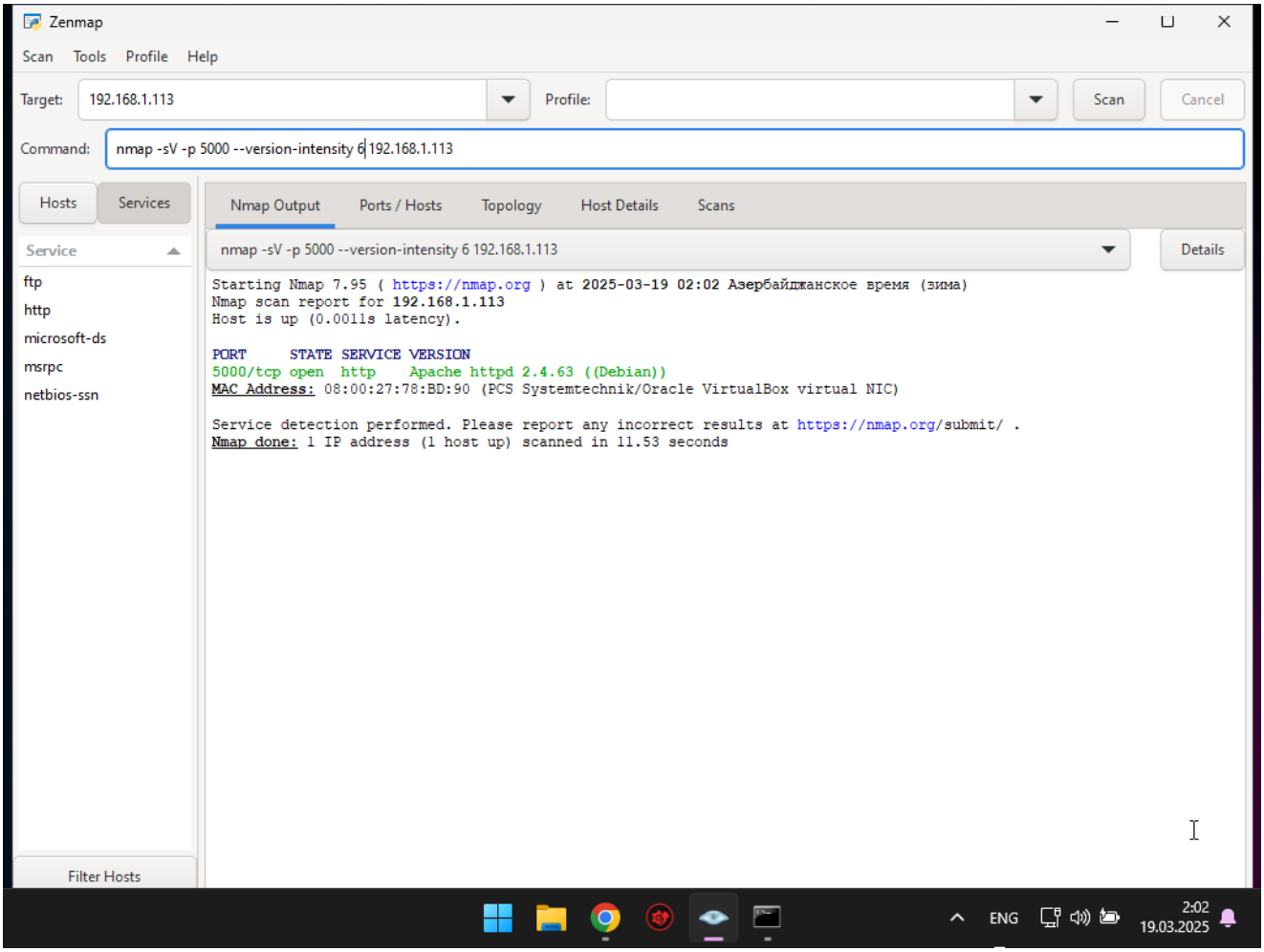
Интенсивность 4



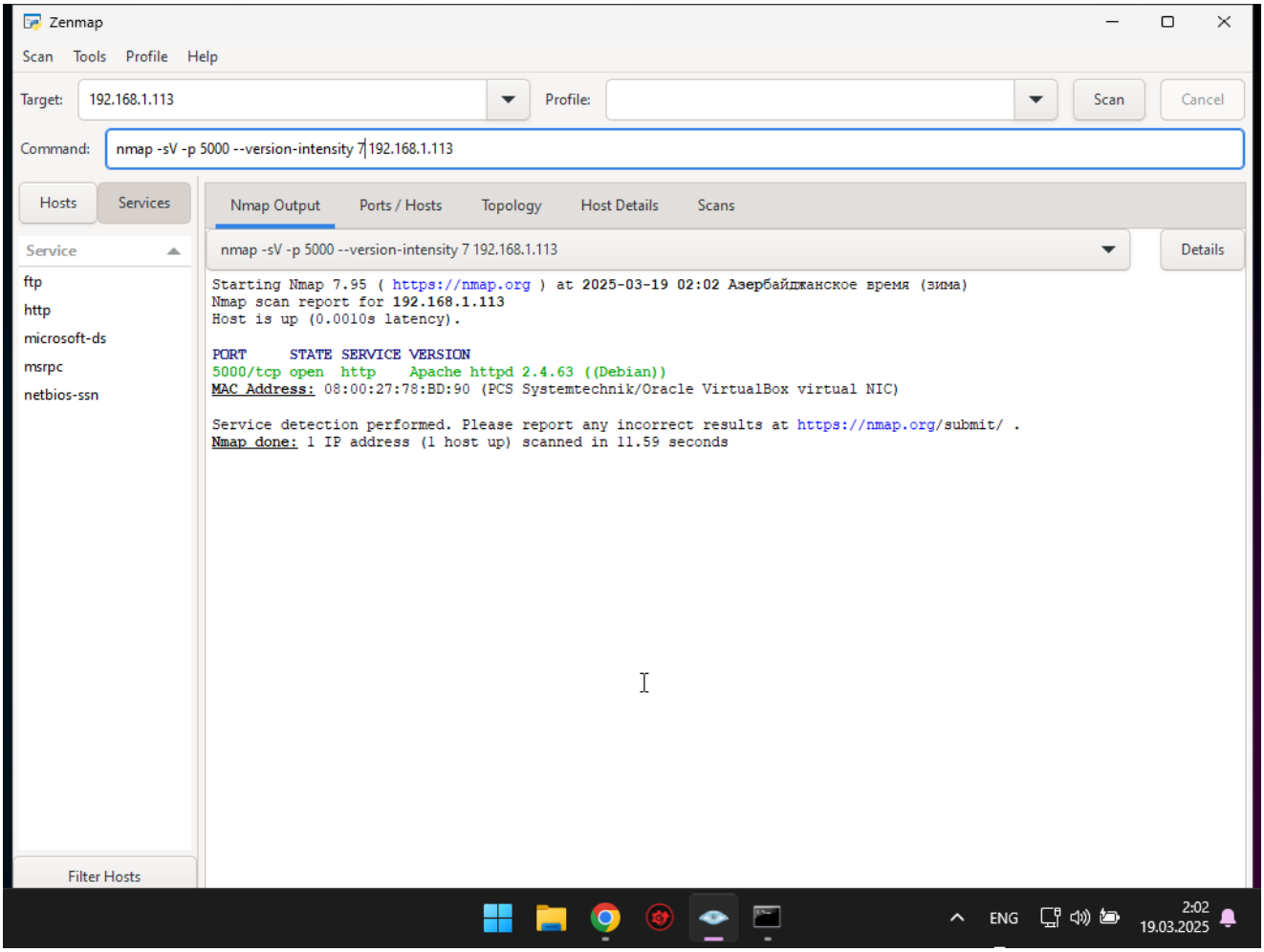
Интенсивность 5



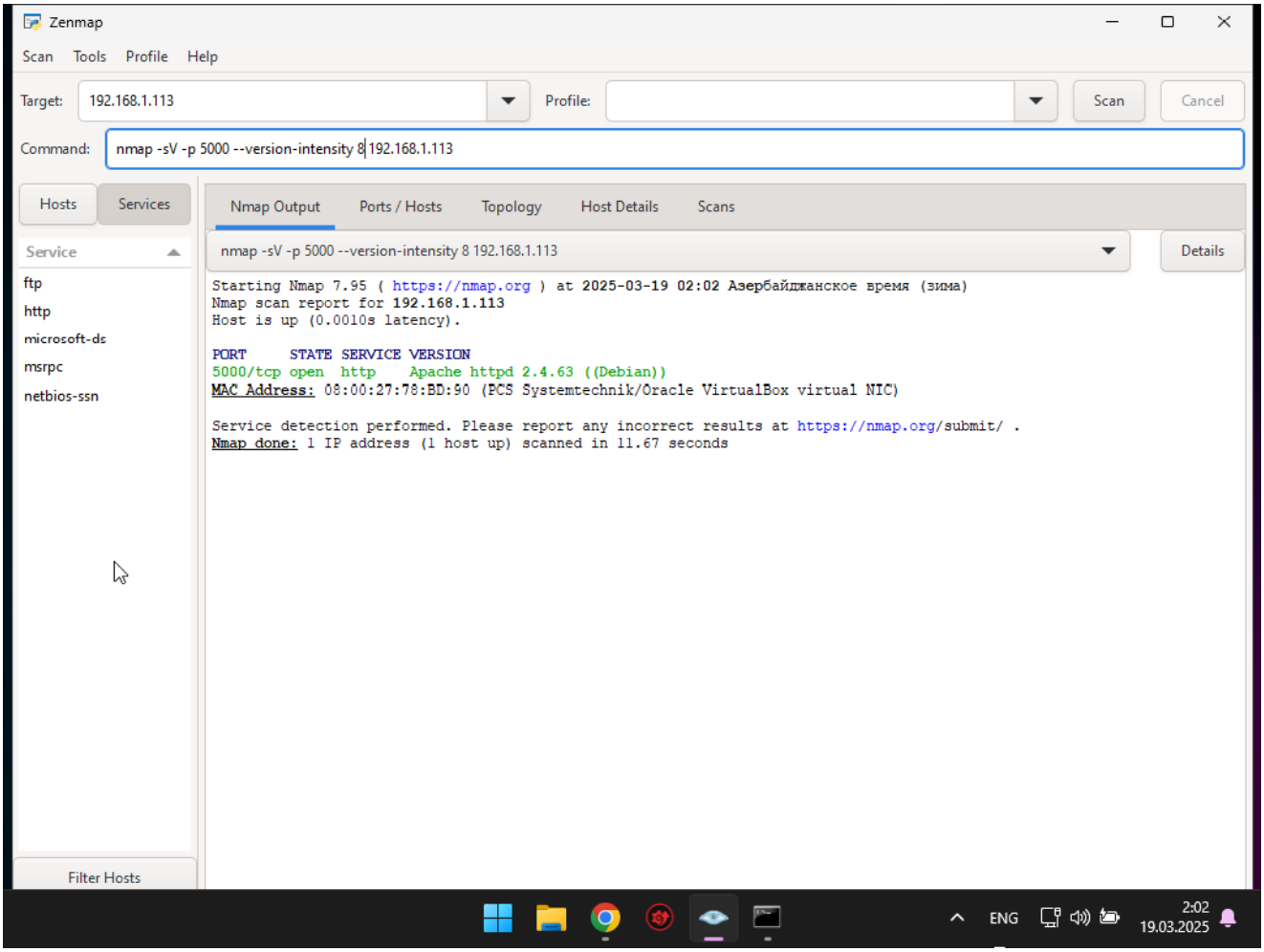
Интенсивность 6



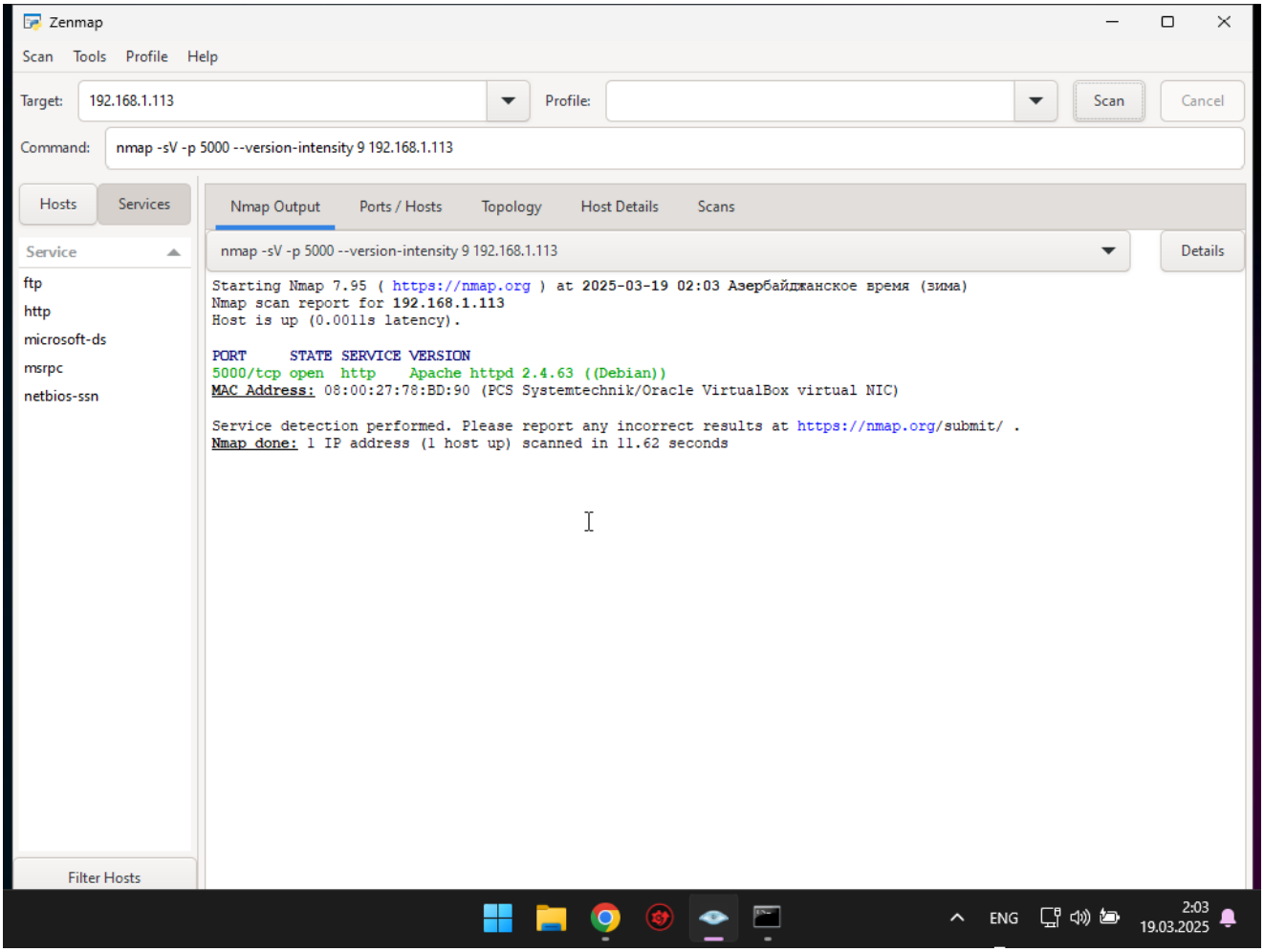
Интенсивность 7



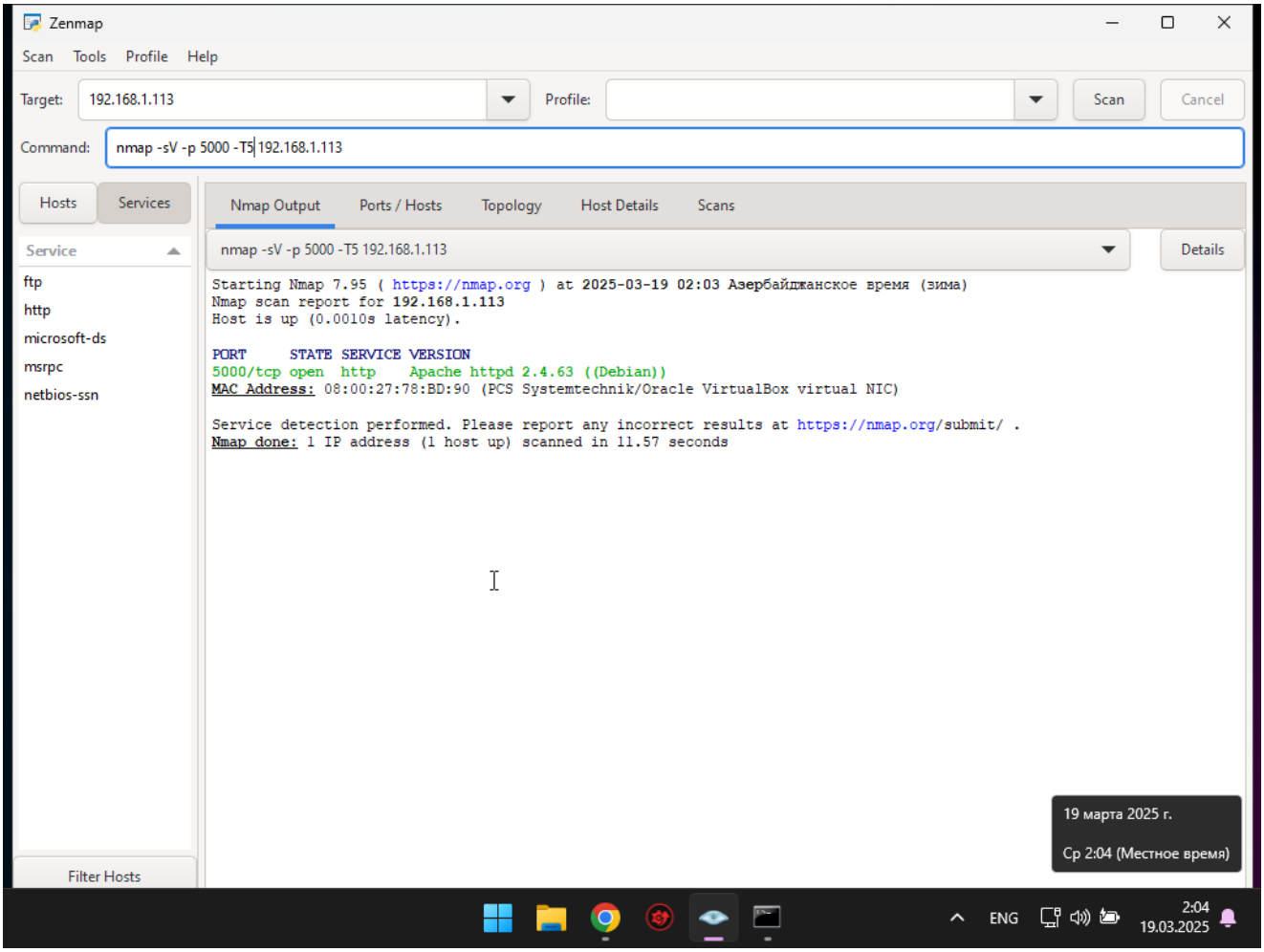
Интенсивность 8



Интенсивность 9



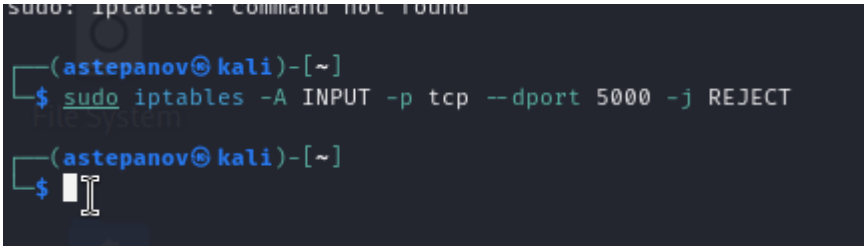
Сканирование с другим флагом (T) с максимальным уровнем интенсивности insane (T5)



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

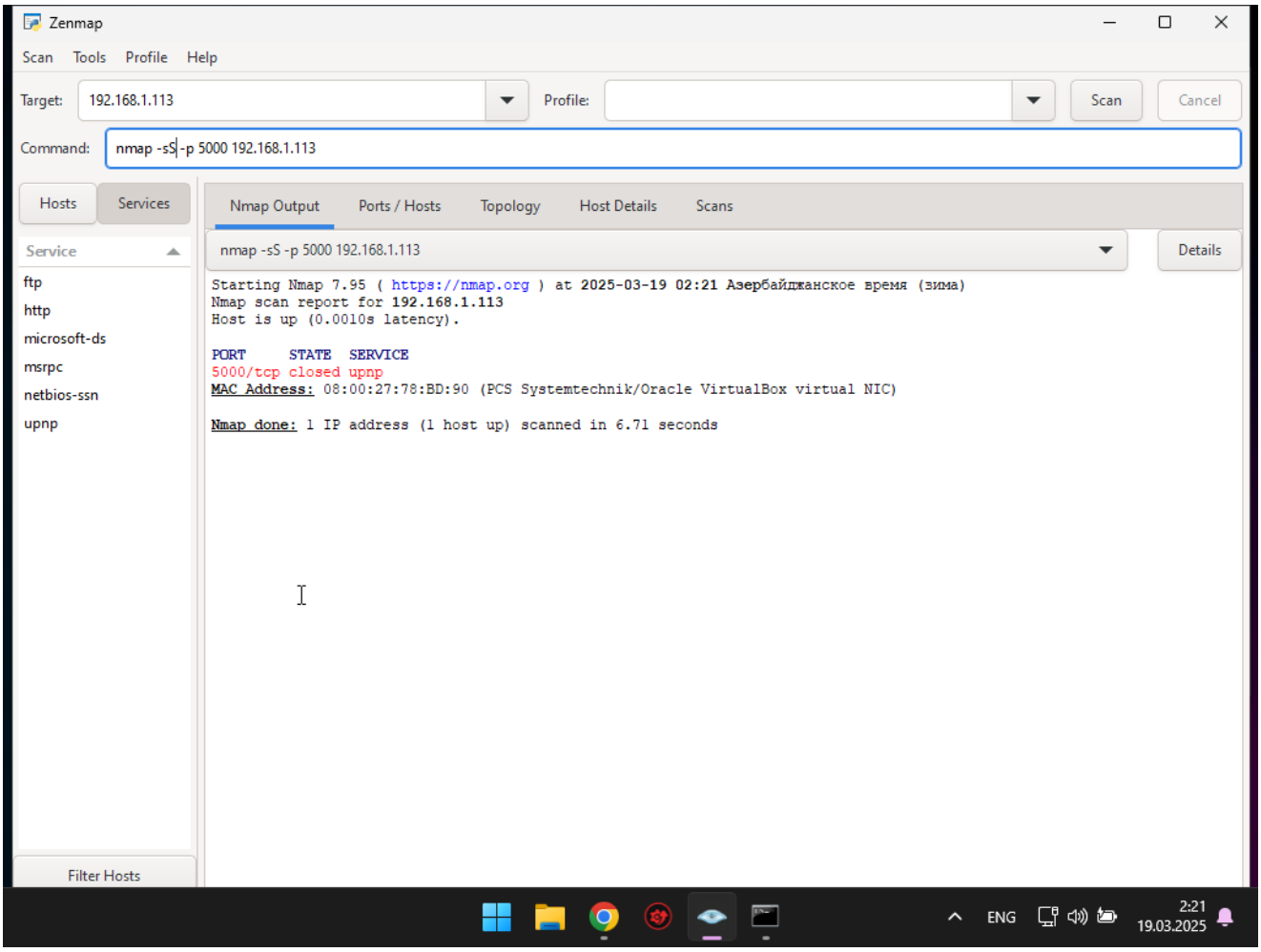
Шаг 14. Заблокируйте любой порт из открытых на машине Linux с помощью iptables по политике REJECT.

Блокируем 5000-ый порт



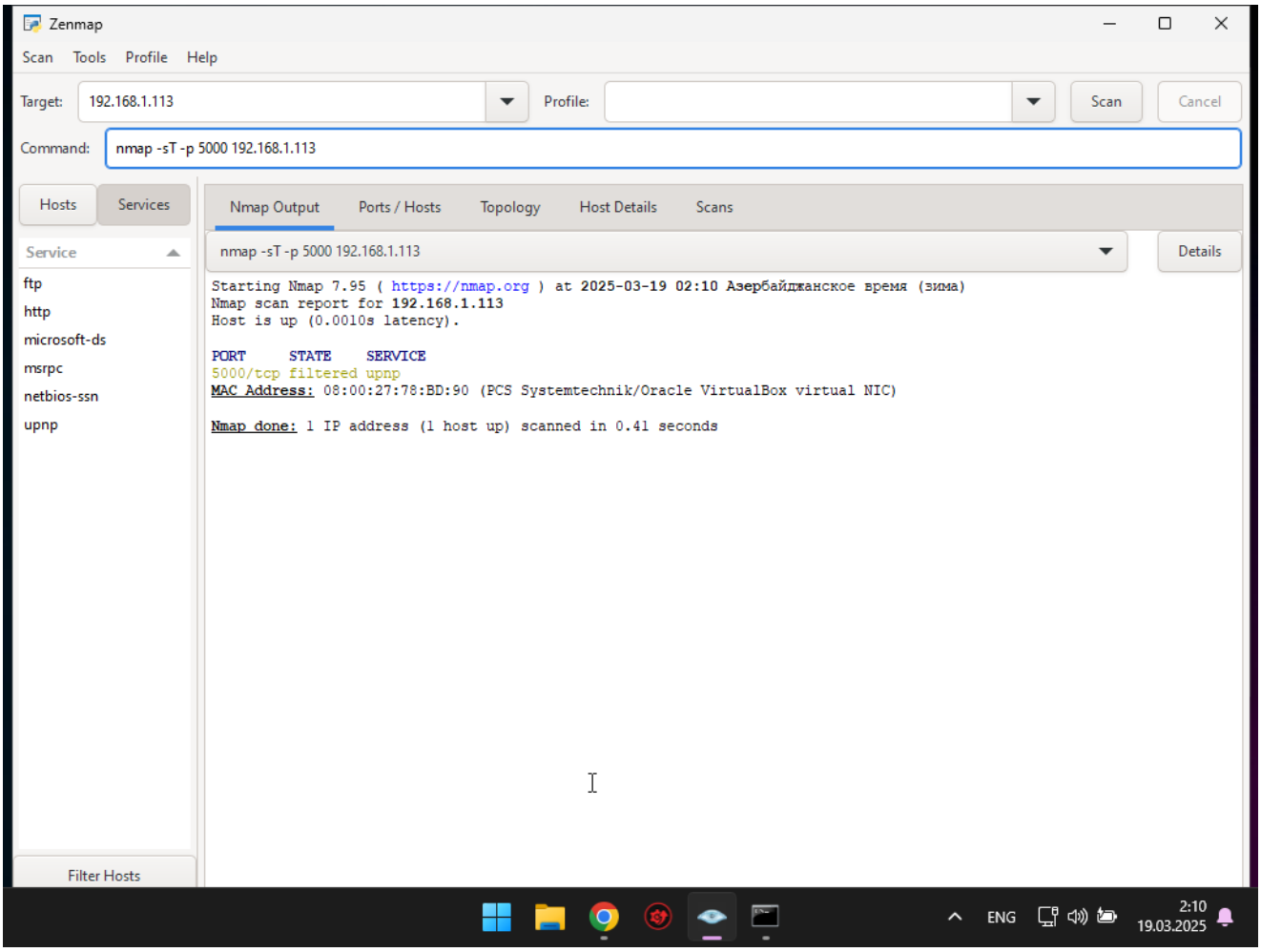
Шаг 15. Просканируйте заблокированный в пункте 13 (14) порт типами сканирования TCP SYN Scan, TCP Connect Scan, UDP Scan, TCP FIN Scan, TCP NULL Scan, TCP Xmas Scan и TCP ACK Scan. Сравните полученные результаты.

TCP SYN Scan



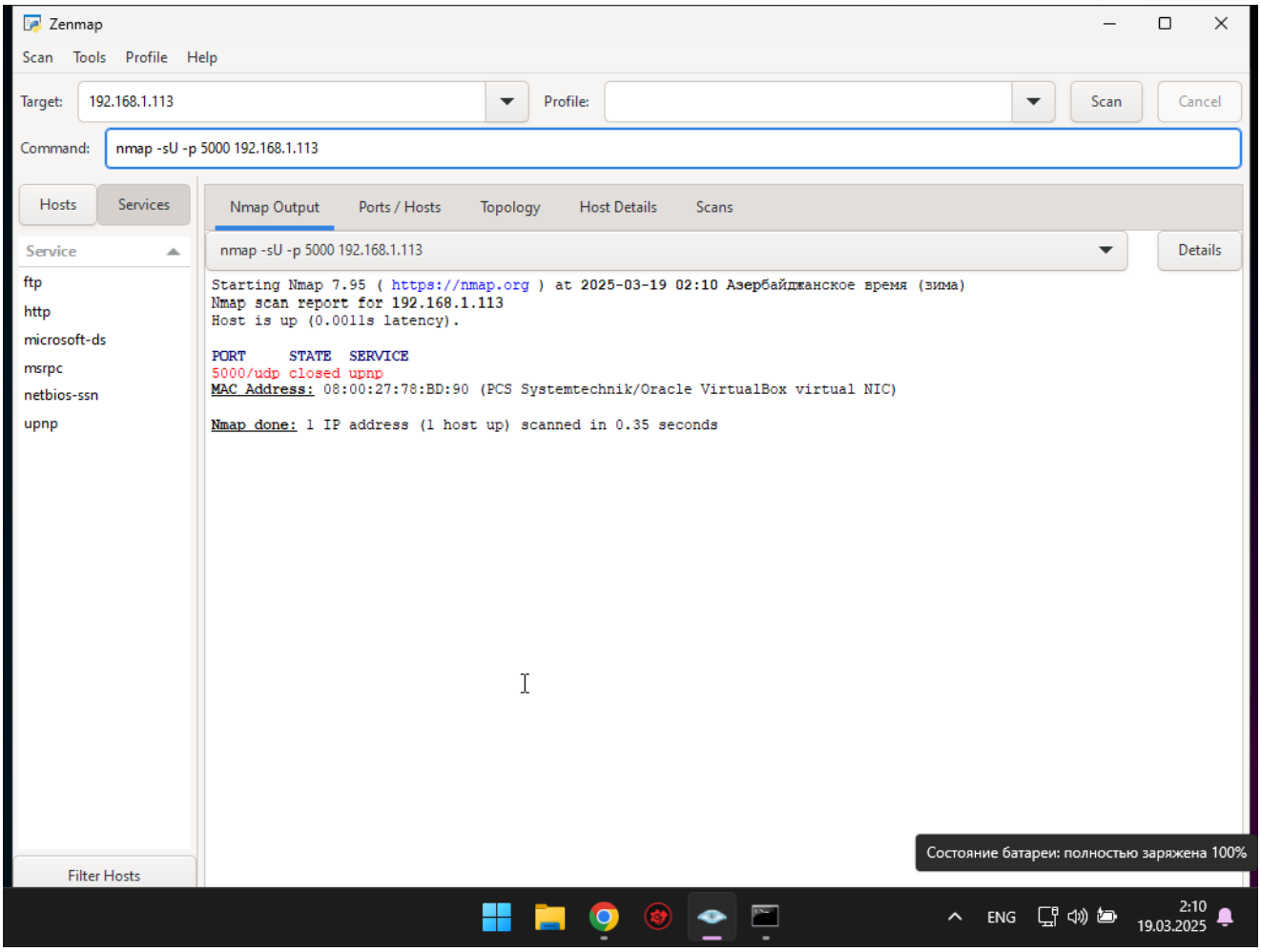
REJECT отправляет ответ RST, nmap считает порт закрытым.

TCP Connect Scan



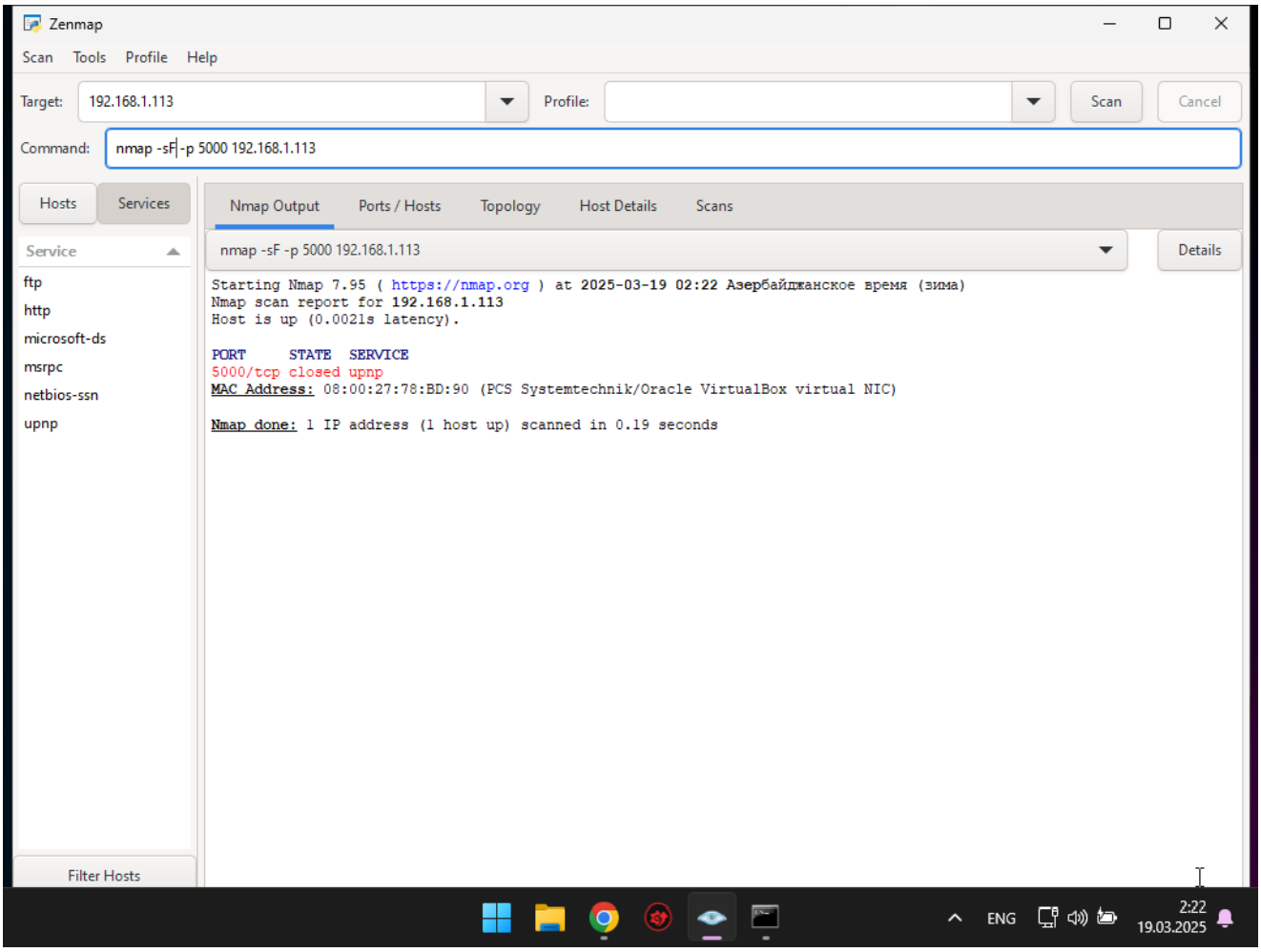
Порт показывается как filtered

UDP Scan



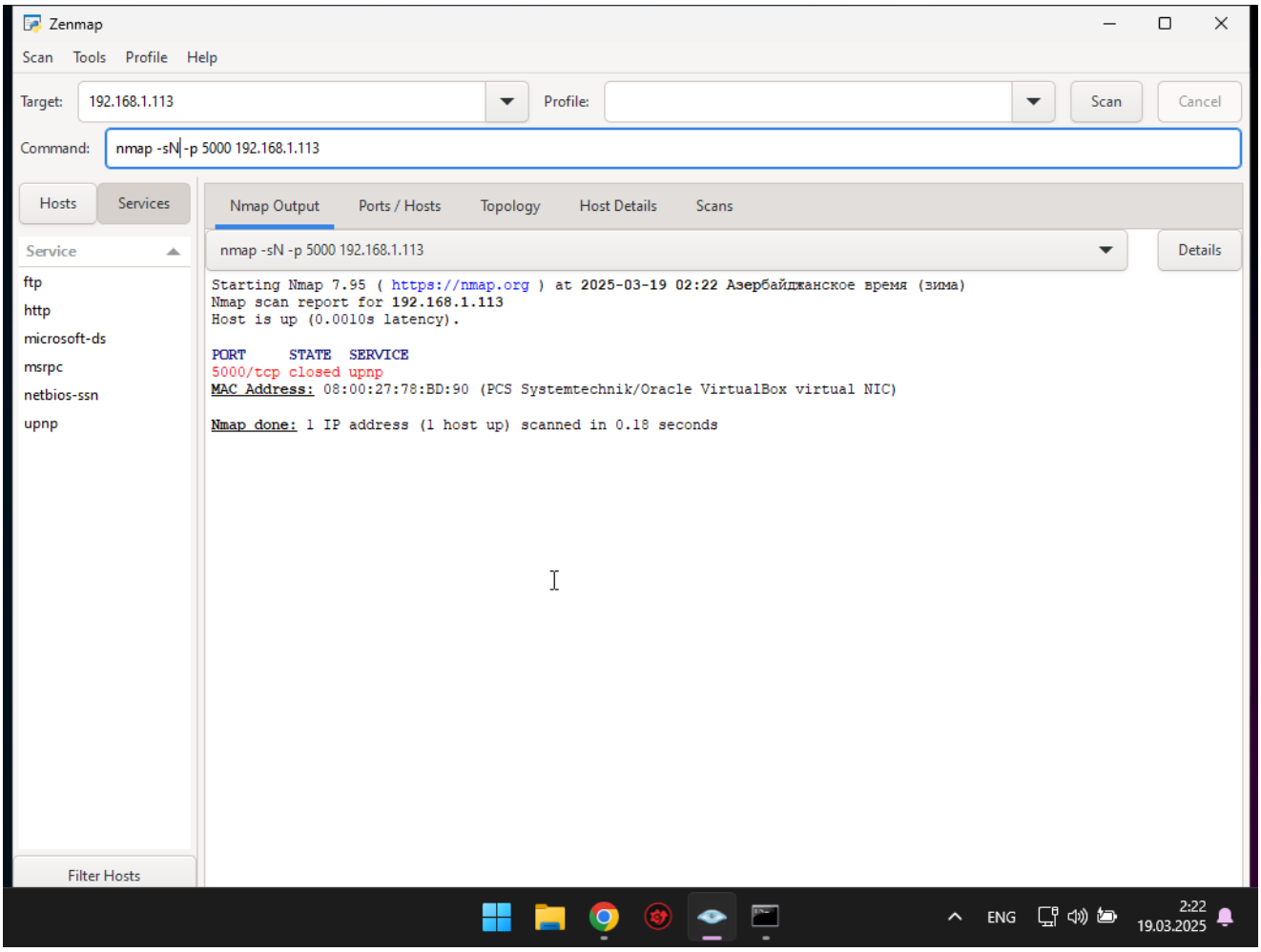
Порт показывается как closed

TCP FIN Scan



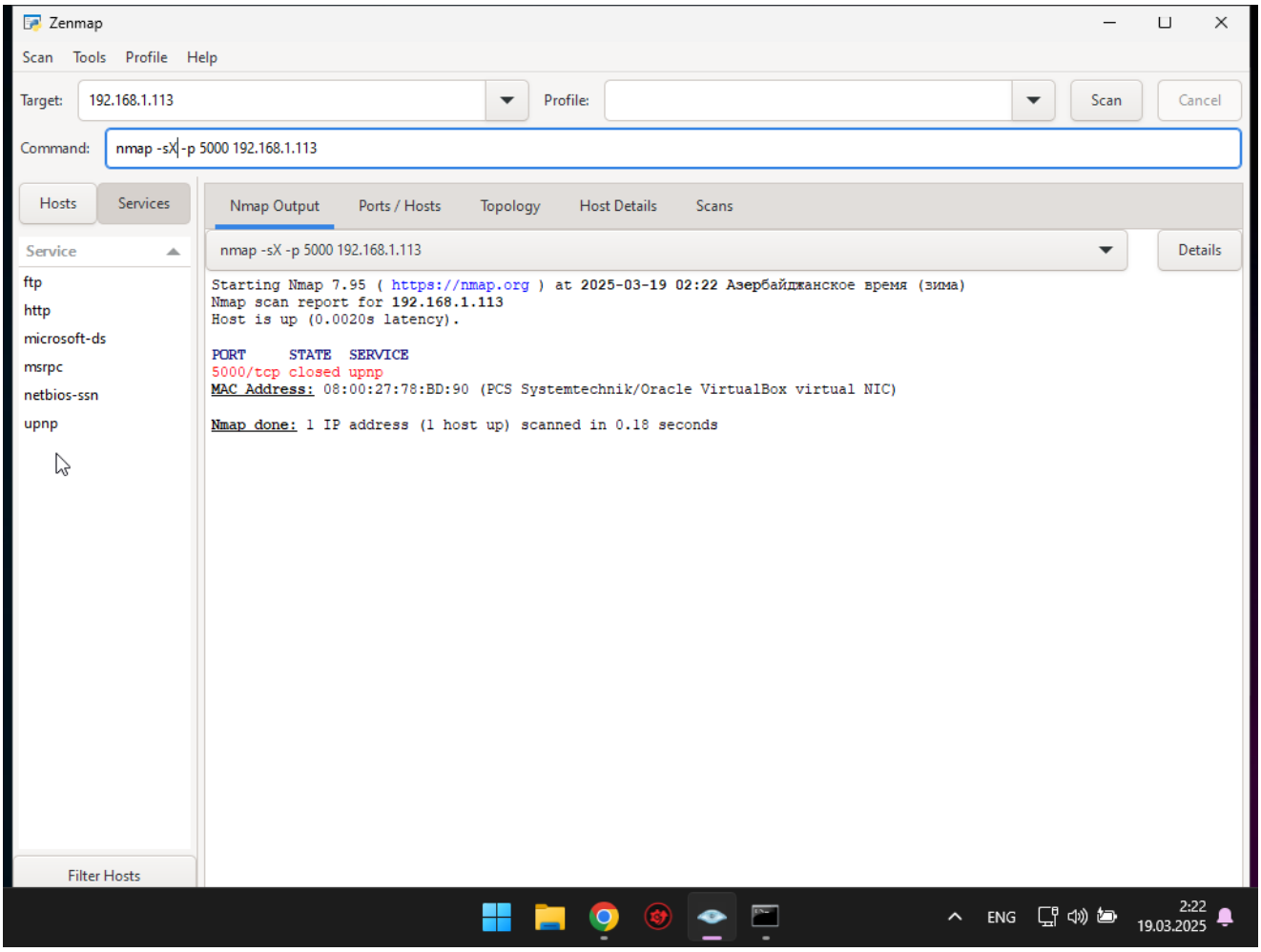
Порт показывается как closed

TCP NULL Scan



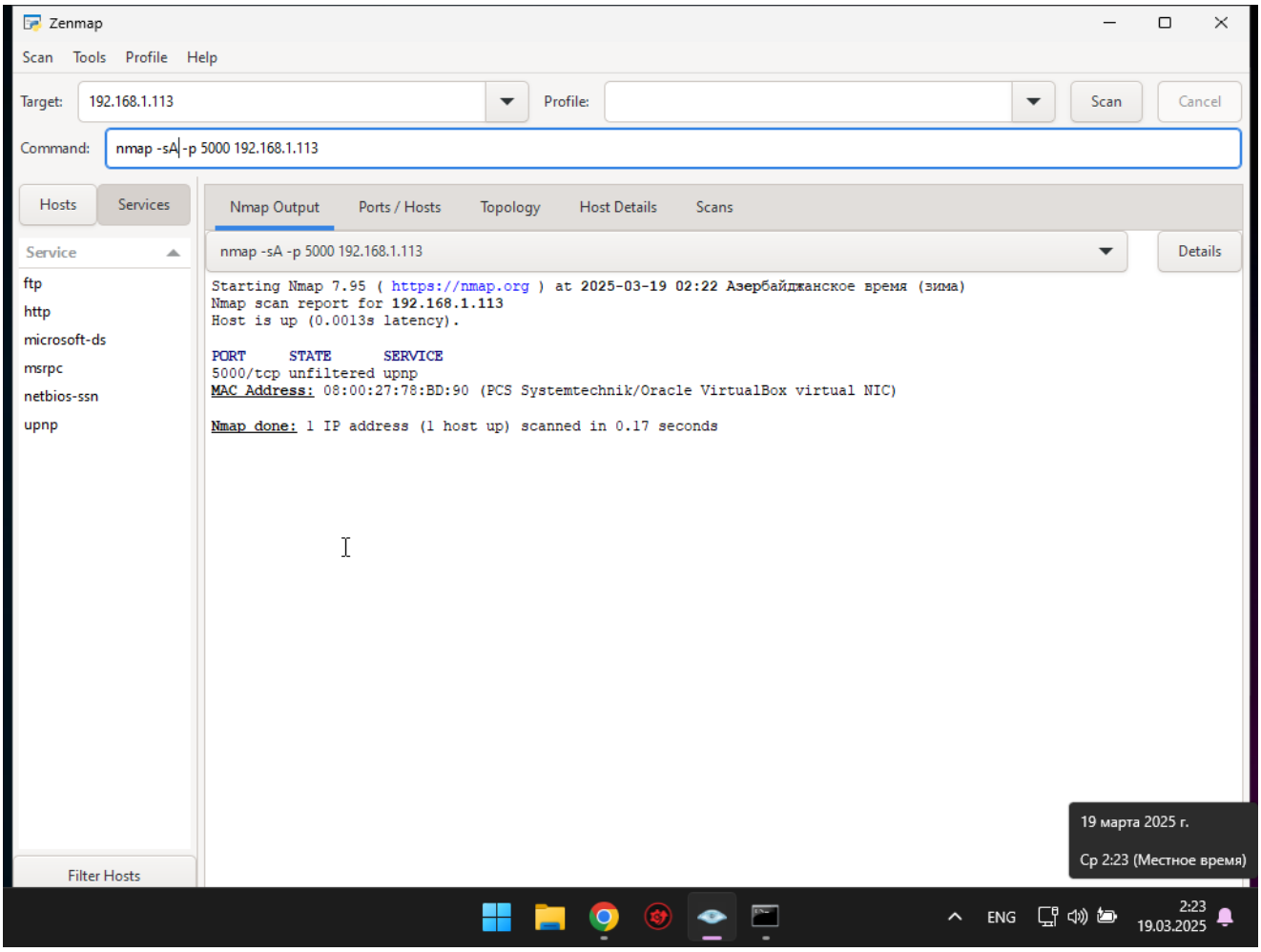
Порт показывается как closed

TCP Xmas Scan



Порт показывается как closed

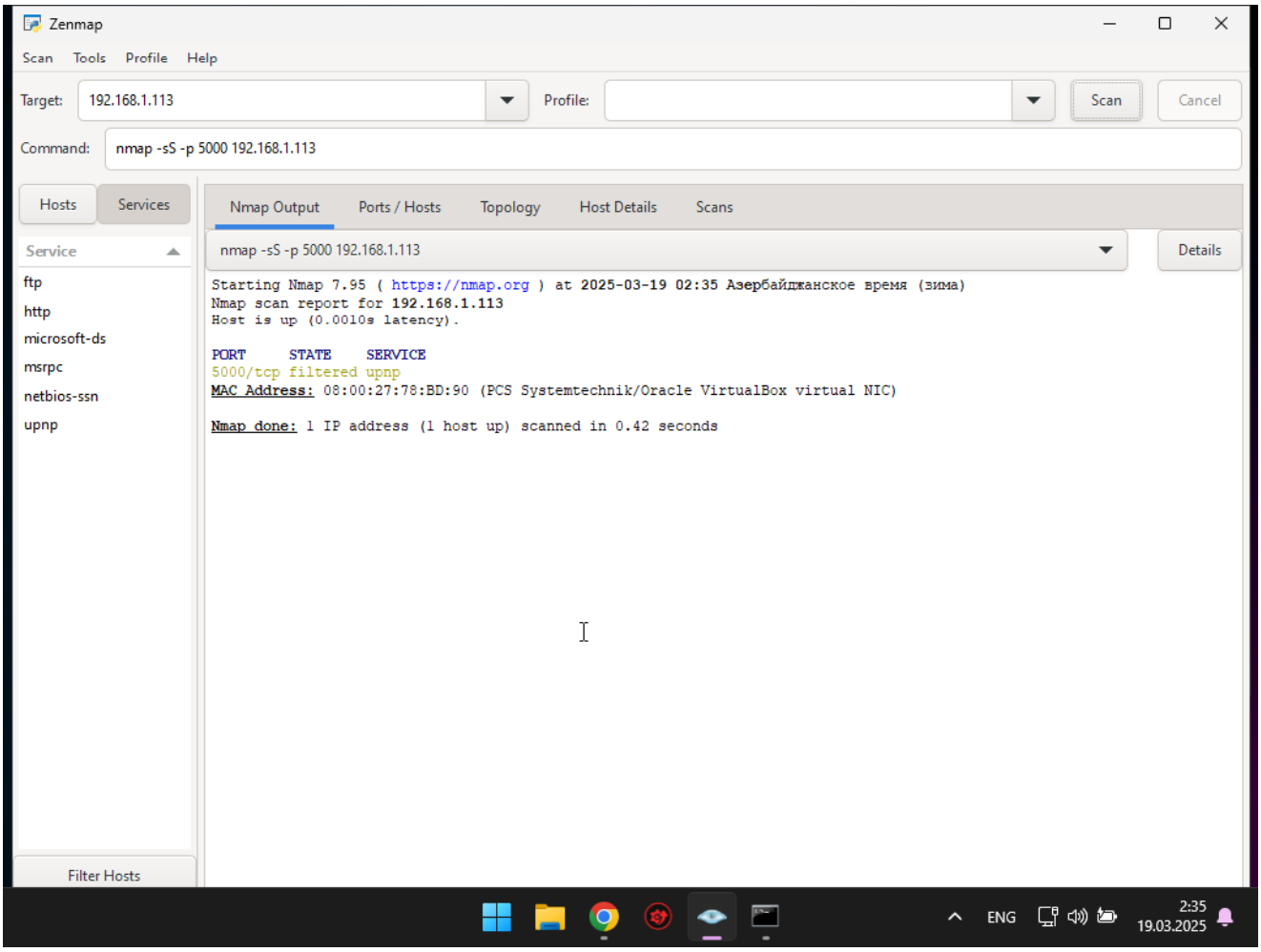
TCP ACK Scan



Порт показывается как unfiltered

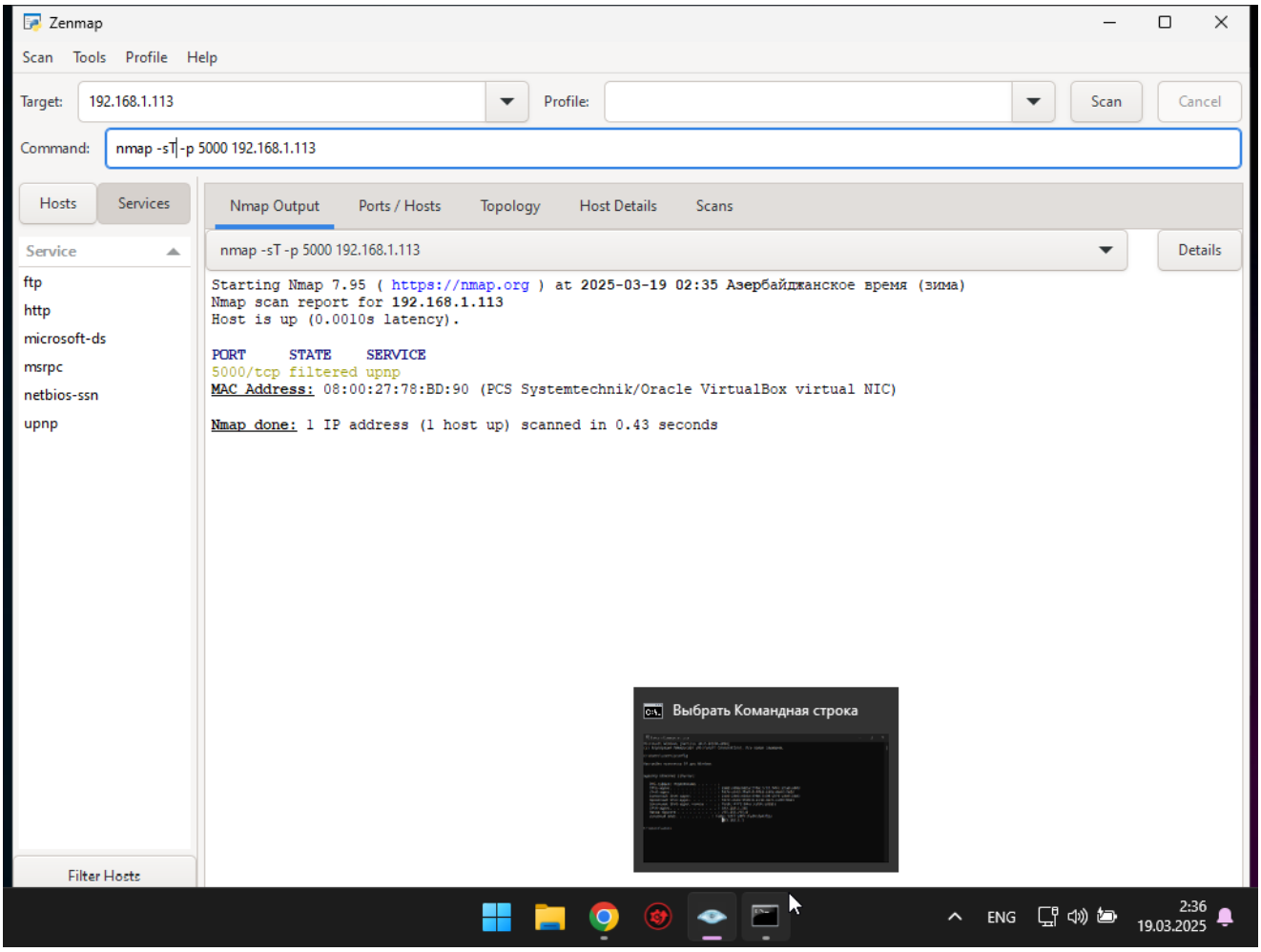
Шаг 16. Удалите правило из пункта 13 (14) и добавьте аналогичное, но с политикой DROP. Повторите пункт 14 (15). Сравните результаты с пунктом 14 (15).

TCP SYN Scan



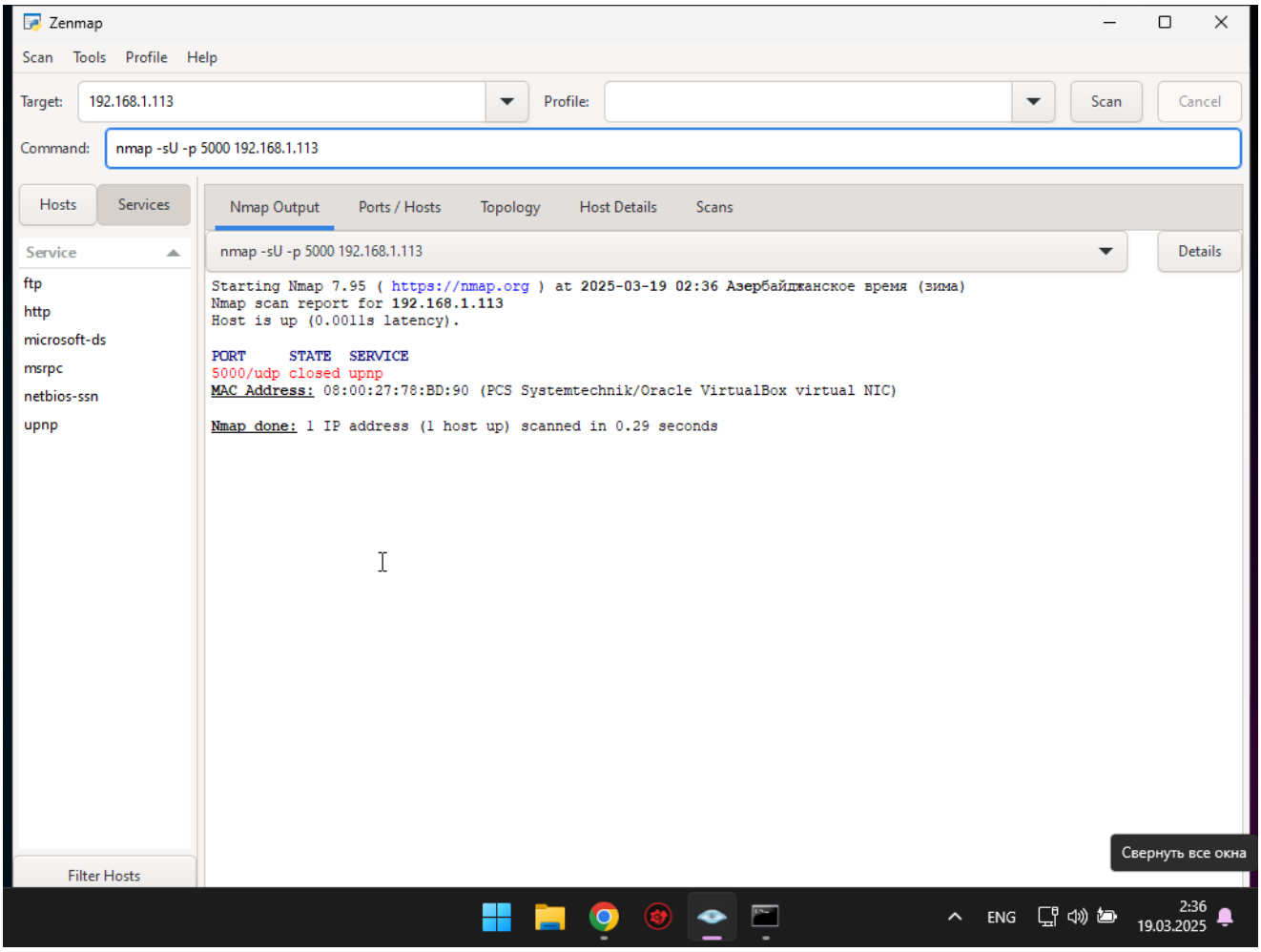
Порт показывается как filtered

TCP Connect Scan



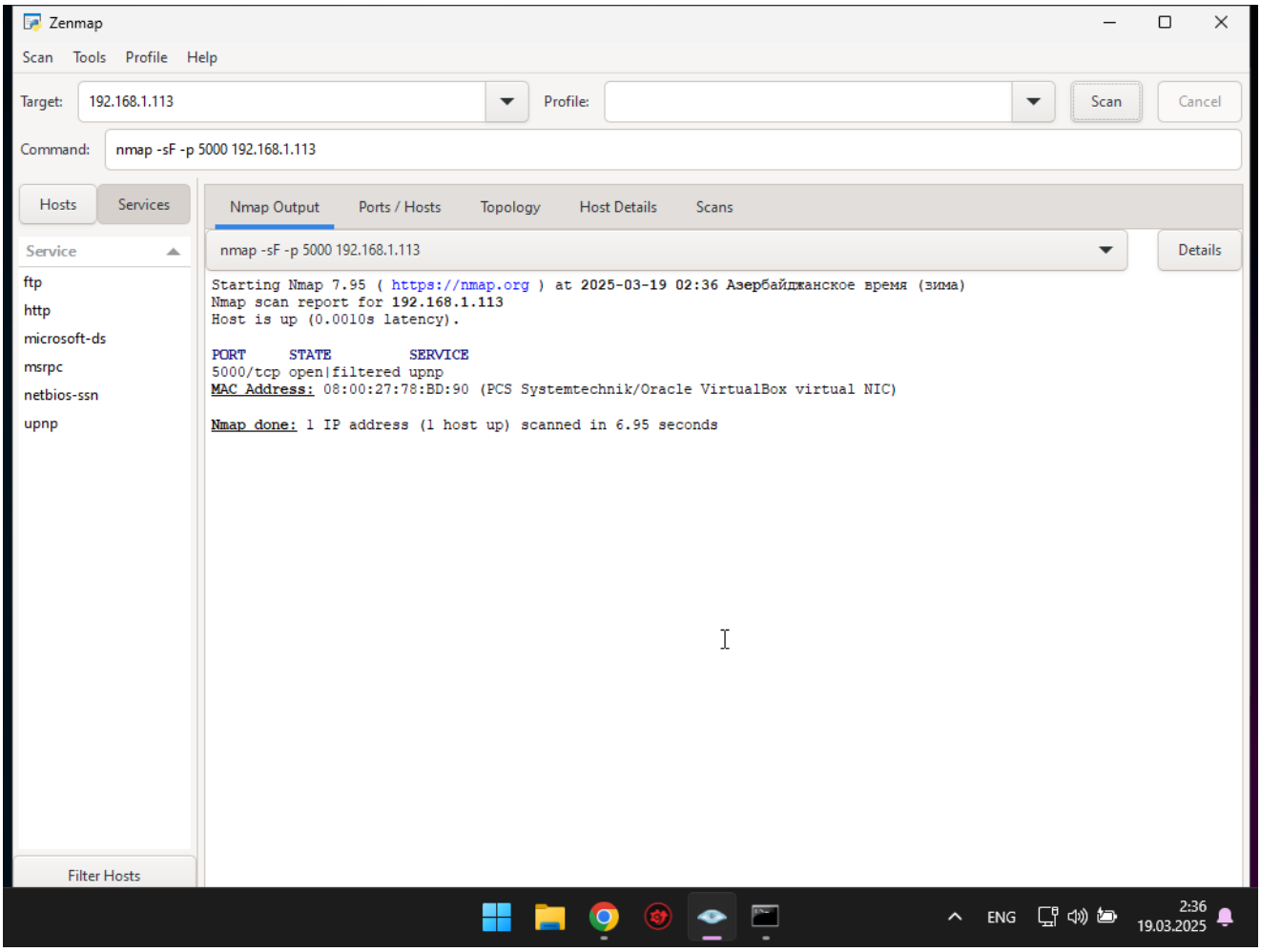
Порт показывается как filtered

UDP Scan



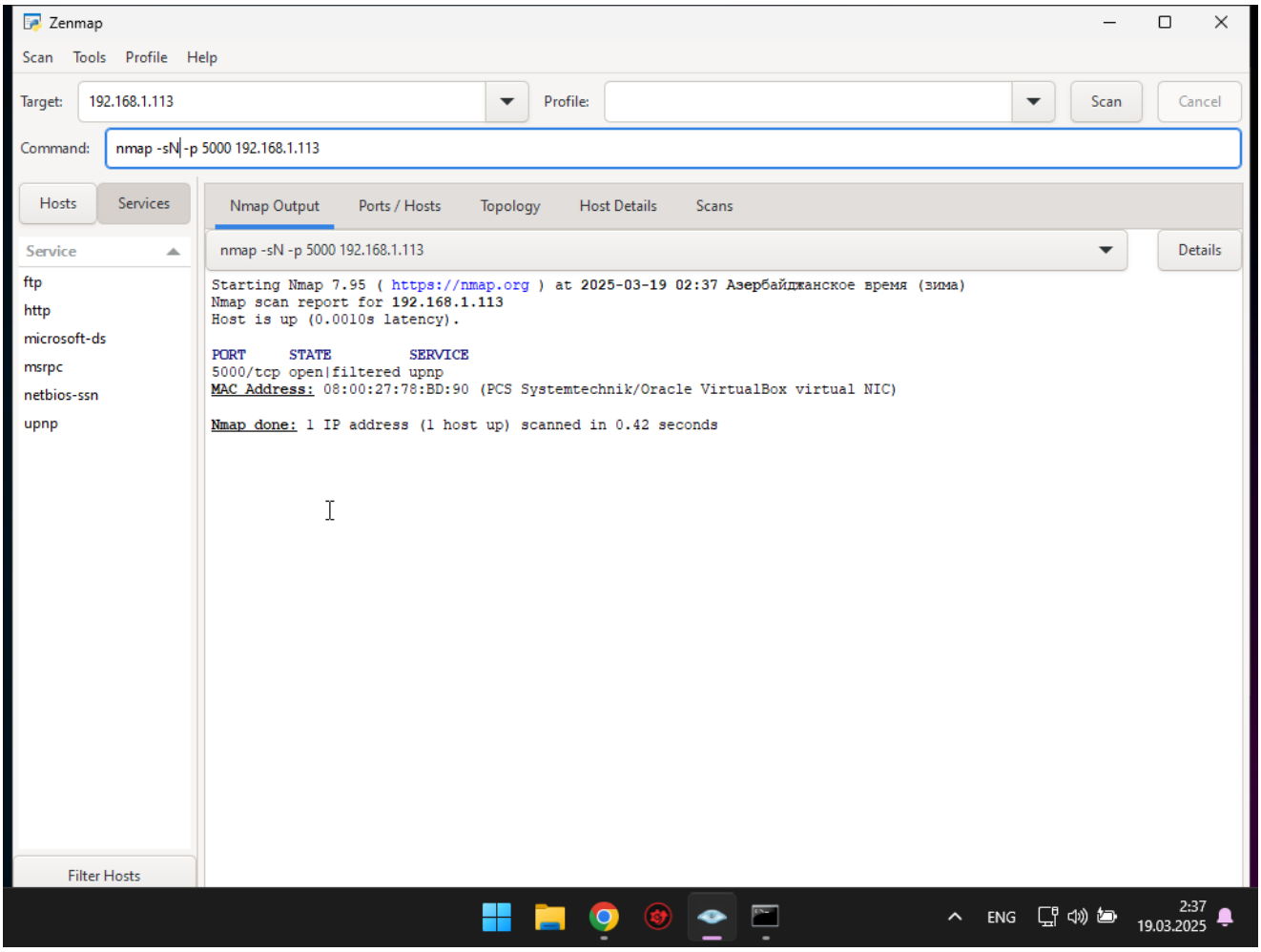
Порт показывается как closed

TCP FIN Scan



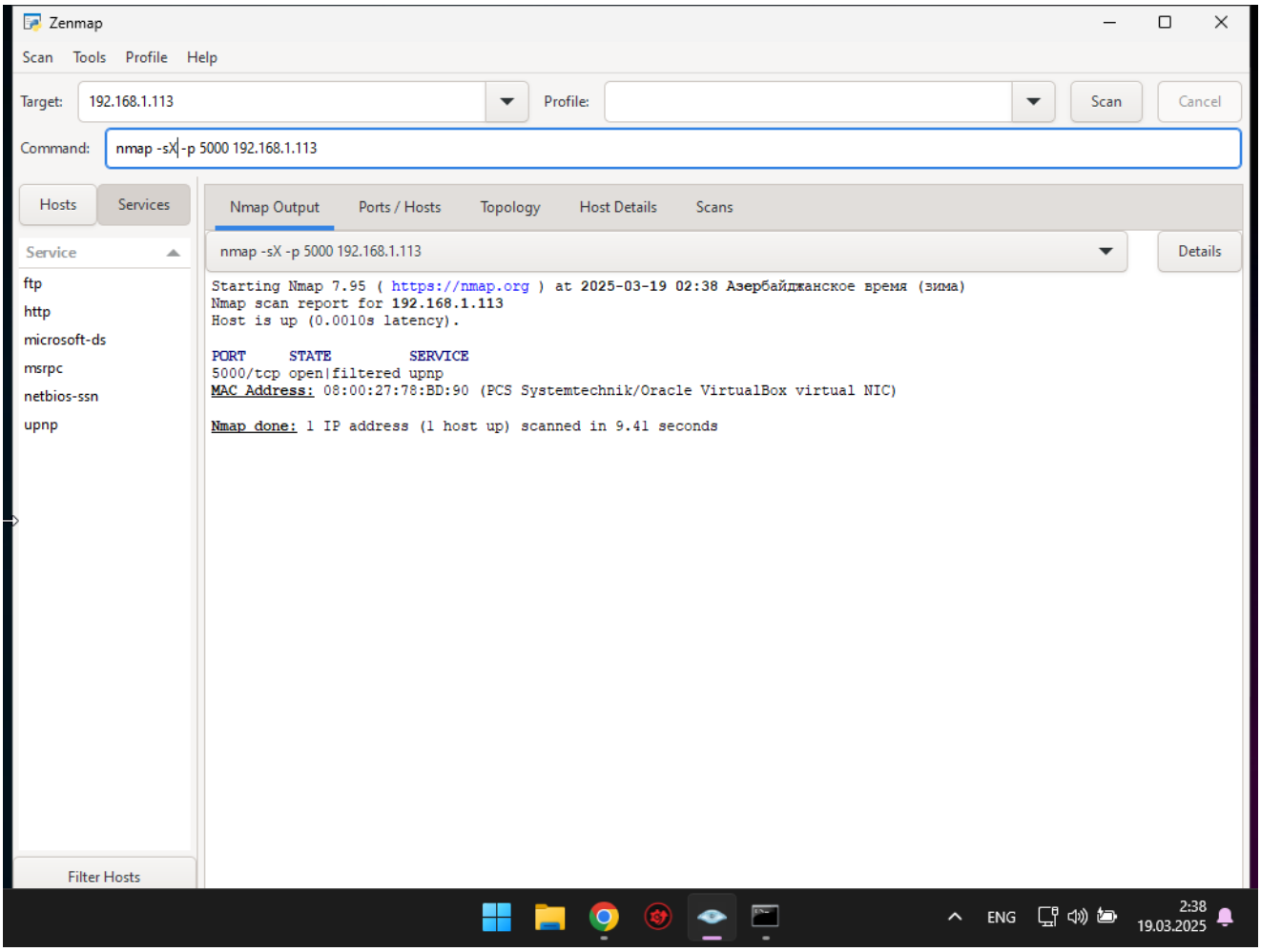
Порт показывается как open|filtered

TCP NULL Scan



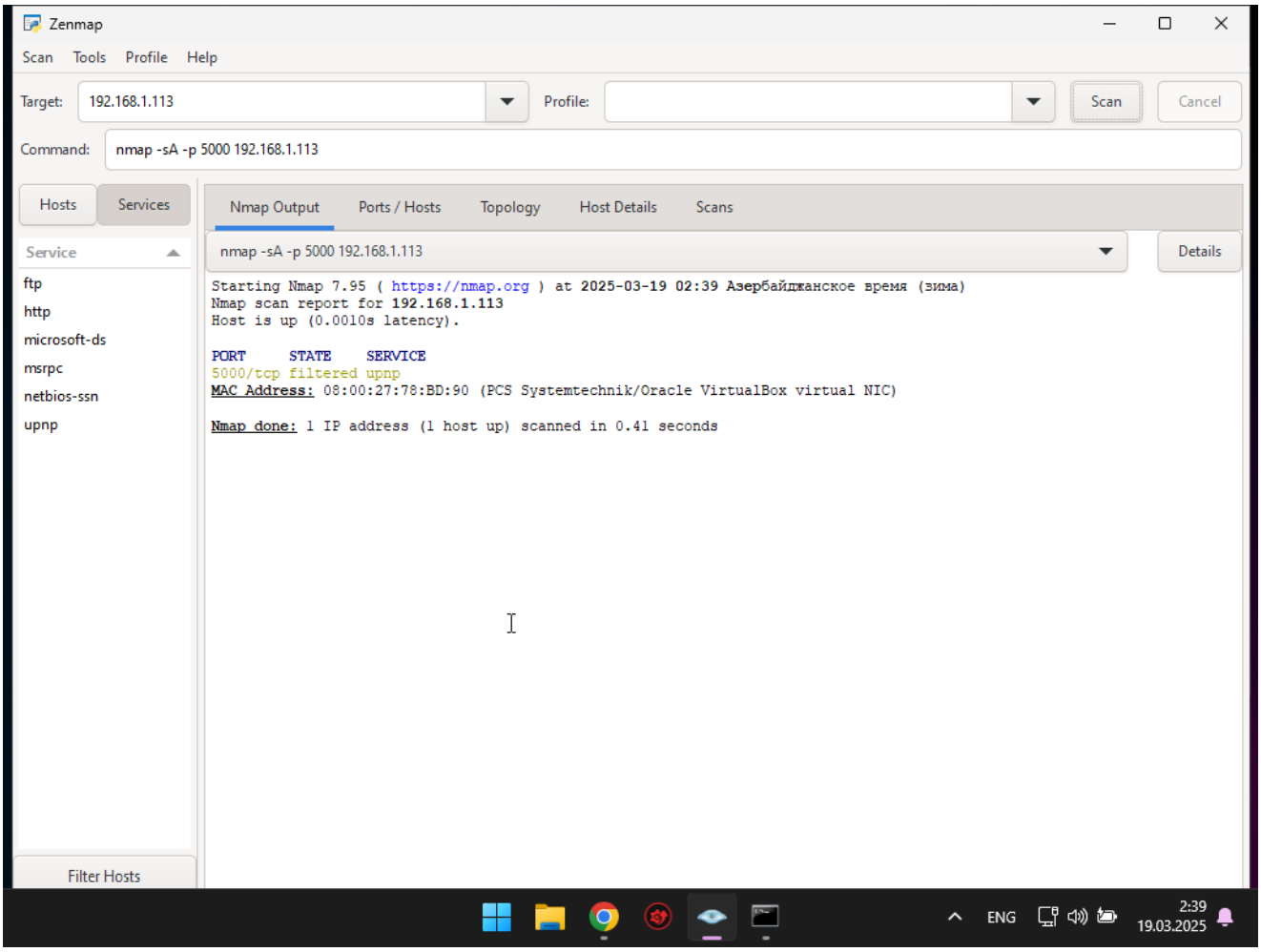
Порт показывается как open|filtered

TCP Xmas Scan



Порт показывается как open|filtered

TCP ACK Scan



Порт показывается как filtered