Scanning Procedures for Identifying Open Active Accounts on Hosts

Scanning is a process used to identify active hosts and open services/ports on a target system, often with the goal of assessing security vulnerabilities. This process is essential for penetration testing, security assessments, or ethical hacking, as it helps uncover potential weaknesses in a network or system.

Types of Scanning:

1. **Port Scanning**
2. **Vulnerability Scanning**

Port Scanning Techniques (TCP and UDP):

TCP Scanning Techniques:

Port scanning in TCP can be conducted using different methods to probe the system and understand which services are running. Some common TCP port scanning techniques are:

1. **TCP Connect Scan**:
   - This method involves completing the full three-way handshake to establish a connection. It is easy to detect because it involves establishing a complete connection to the target port.
2. **TCP FIN Scan**:
   - This scan sends a FIN (Finish) flag to the target port, which is used to terminate a connection. Normally, no response should be received if the port is closed, but a reset (RST) signal is sent for open ports, which can help in identifying open ports.
3. **TCP SYN Scan**:
   - This is one of the most popular scanning techniques. It only sends the SYN (synchronize) flag, initiating the handshake process. If the port is open, a SYN-ACK response is received. The scan doesn't complete the handshake, making it more stealthy than a full TCP connection scan.

4. **TCP XMAS Scan**:

    - This scan sends a packet with the FIN, URG, and PSH flags set. These flags are not typically used together, which can confuse the target system. It is stealthier but can be detected by modern firewalls and intrusion detection systems (IDS).

5. **TCP NULL Scan**:

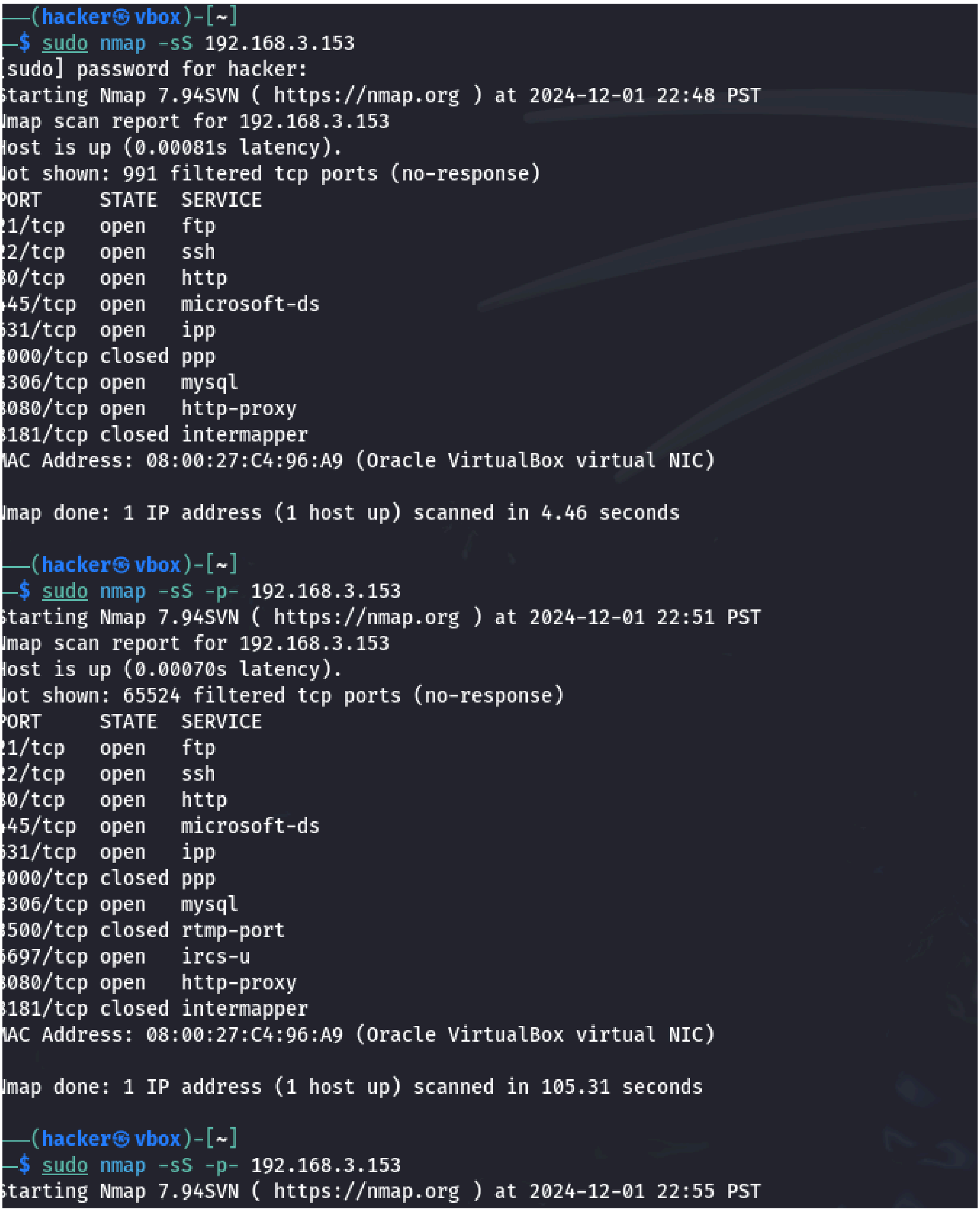
    - In this method, no flags are set in the packet, which can confuse the target system because there is no flag indicating the purpose of the packet. The response behavior helps determine whether the port is open or closed, though it is less commonly used due to detection issues.

UDP Scanning:

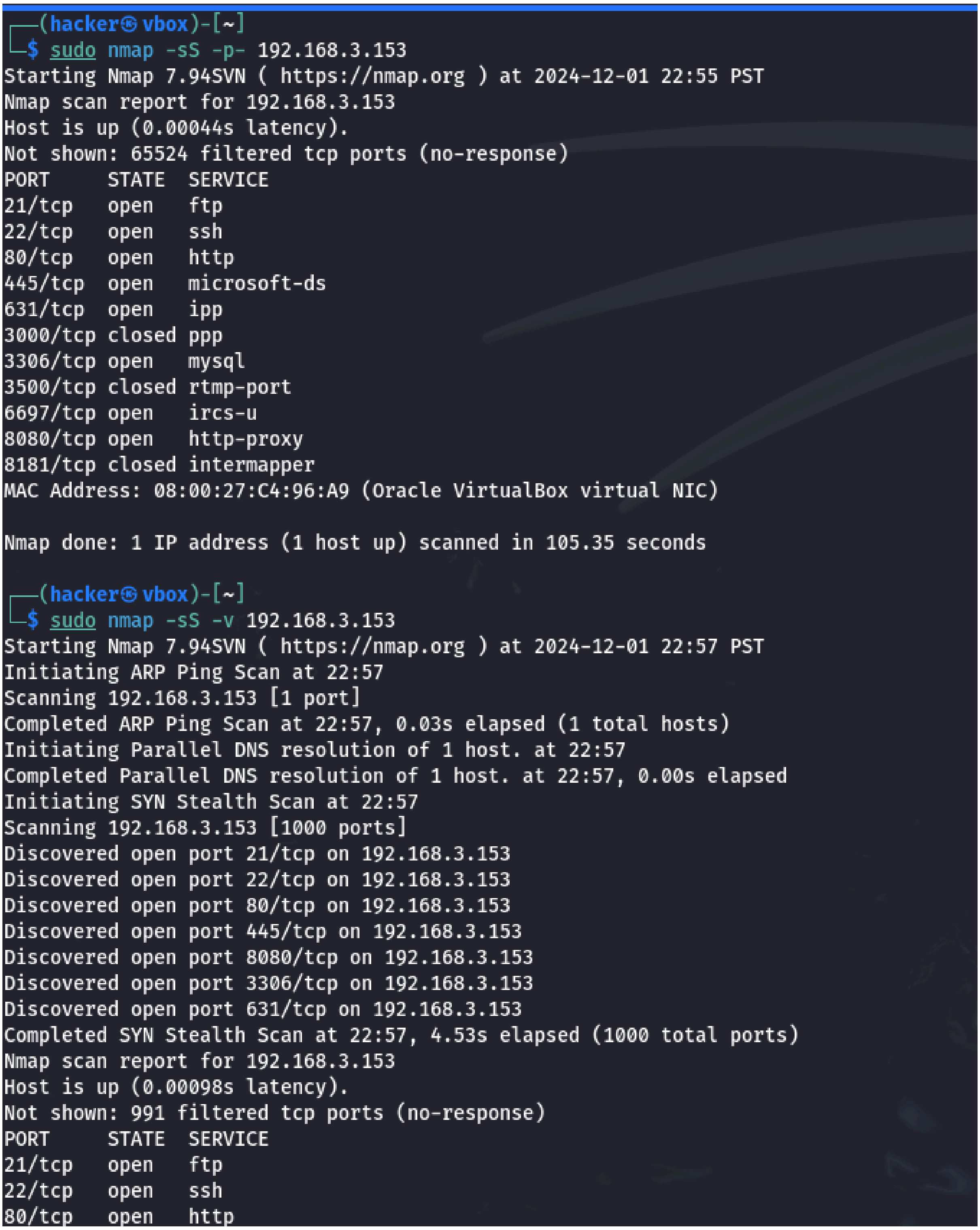
While UDP scanning is generally less reliable than TCP scanning due to the nature of UDP's connectionless protocol, it can still be important for discovering open services on a network.

- **UDP Scan**: This scan sends a packet to a target port and waits for a response. If there is no response, it is assumed the port is open (or filtered by a firewall). If a response is received (such as an ICMP port unreachable message), it is considered closed.

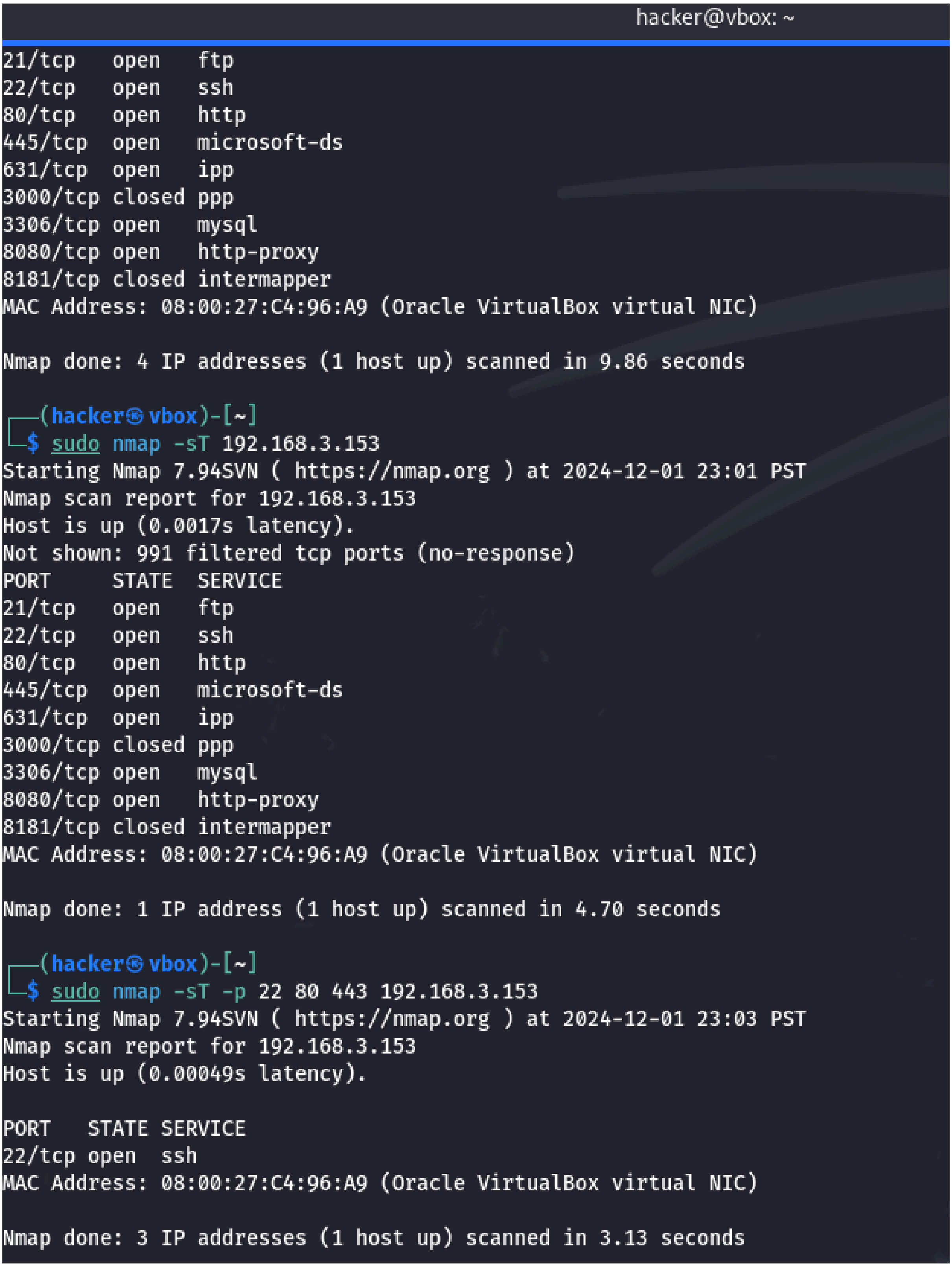
Each scanning technique has different levels of effectiveness and stealth, making it suitable for different scenarios depending on the target and the assessment’s objectives.



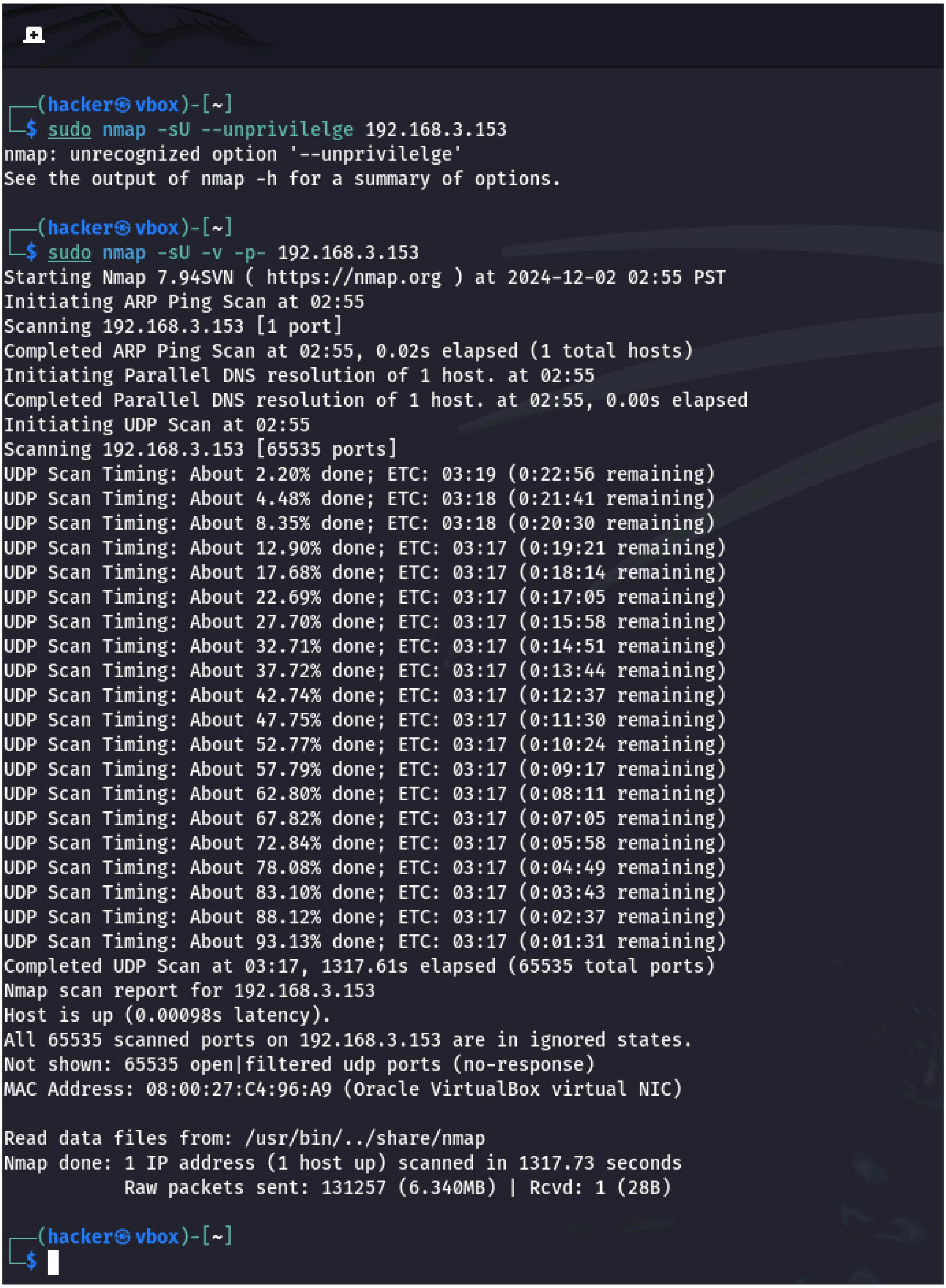
```
──(hacker㉿vbox)-[~]
─$ sudo nmap -sS 192.168.3.153
[sudo] password for hacker:
tarting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 22:48 PST
map scan report for 192.168.3.153
ost is up (0.00081s latency).
ot shown: 991 filtered tcp ports (no-response)
ORT     STATE  SERVICE
1/tcp   open   ftp
2/tcp   open   ssh
0/tcp   open   http
45/tcp  open   microsoft-ds
31/tcp  open   ipp
000/tcp closed ppp
306/tcp open   mysql
080/tcp open   http-proxy
181/tcp closed intermapper
AC Address: 08:00:27:C4:96:A9 (Oracle VirtualBox virtual NIC)

map done: 1 IP address (1 host up) scanned in 4.46 seconds

──(hacker㉿vbox)-[~]
─$ sudo nmap -sS -p- 192.168.3.153
tarting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 22:51 PST
map scan report for 192.168.3.153
ost is up (0.00070s latency).
ot shown: 65524 filtered tcp ports (no-response)
ORT     STATE  SERVICE
1/tcp   open   ftp
2/tcp   open   ssh
0/tcp   open   http
45/tcp  open   microsoft-ds
31/tcp  open   ipp
000/tcp closed ppp
306/tcp open   mysql
500/tcp closed rtmp-port
697/tcp open   ircs-u
080/tcp open   http-proxy
181/tcp closed intermapper
AC Address: 08:00:27:C4:96:A9 (Oracle VirtualBox virtual NIC)

map done: 1 IP address (1 host up) scanned in 105.31 seconds

──(hacker㉿vbox)-[~]
─$ sudo nmap -sS -p- 192.168.3.153
tarting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 22:55 PST
```



```
┌──(hacker㉿vbox)-[~]
└─$ sudo nmap -sS -p- 192.168.3.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 22:55 PST
Nmap scan report for 192.168.3.153
Host is up (0.00044s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
3500/tcp closed rtmp-port
6697/tcp open   ircs-u
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:C4:96:A9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 105.35 seconds

┌──(hacker㉿vbox)-[~]
└─$ sudo nmap -sS -v 192.168.3.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 22:57 PST
Initiating ARP Ping Scan at 22:57
Scanning 192.168.3.153 [1 port]
Completed ARP Ping Scan at 22:57, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:57
Completed Parallel DNS resolution of 1 host. at 22:57, 0.00s elapsed
Initiating SYN Stealth Scan at 22:57
Scanning 192.168.3.153 [1000 ports]
Discovered open port 21/tcp on 192.168.3.153
Discovered open port 22/tcp on 192.168.3.153
Discovered open port 80/tcp on 192.168.3.153
Discovered open port 445/tcp on 192.168.3.153
Discovered open port 8080/tcp on 192.168.3.153
Discovered open port 3306/tcp on 192.168.3.153
Discovered open port 631/tcp on 192.168.3.153
Completed SYN Stealth Scan at 22:57, 4.53s elapsed (1000 total ports)
Nmap scan report for 192.168.3.153
Host is up (0.00098s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
```



```
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:C4:96:A9 (Oracle VirtualBox virtual NIC)

Nmap done: 4 IP addresses (1 host up) scanned in 9.86 seconds

┌──(hacker㉿vbox)-[~]
└─$ sudo nmap -sT 192.168.3.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 23:01 PST
Nmap scan report for 192.168.3.153
Host is up (0.0017s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:C4:96:A9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.70 seconds

┌──(hacker㉿vbox)-[~]
└─$ sudo nmap -sT -p 22 80 443 192.168.3.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 23:03 PST
Nmap scan report for 192.168.3.153
Host is up (0.00049s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:C4:96:A9 (Oracle VirtualBox virtual NIC)

Nmap done: 3 IP addresses (1 host up) scanned in 3.13 seconds
```



```
┌──(hacker㉿vbox)-[~]
└─$ sudo nmap -sU --unprivilelge 192.168.3.153
nmap: unrecognized option '--unprivilelge'
See the output of nmap -h for a summary of options.

┌──(hacker㉿vbox)-[~]
└─$ sudo nmap -sU -v -p- 192.168.3.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-02 02:55 PST
Initiating ARP Ping Scan at 02:55
Scanning 192.168.3.153 [1 port]
Completed ARP Ping Scan at 02:55, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:55
Completed Parallel DNS resolution of 1 host. at 02:55, 0.00s elapsed
Initiating UDP Scan at 02:55
Scanning 192.168.3.153 [65535 ports]
UDP Scan Timing: About 2.20% done; ETC: 03:19 (0:22:56 remaining)
UDP Scan Timing: About 4.48% done; ETC: 03:18 (0:21:41 remaining)
UDP Scan Timing: About 8.35% done; ETC: 03:18 (0:20:30 remaining)
UDP Scan Timing: About 12.90% done; ETC: 03:17 (0:19:21 remaining)
UDP Scan Timing: About 17.68% done; ETC: 03:17 (0:18:14 remaining)
UDP Scan Timing: About 22.69% done; ETC: 03:17 (0:17:05 remaining)
UDP Scan Timing: About 27.70% done; ETC: 03:17 (0:15:58 remaining)
UDP Scan Timing: About 32.71% done; ETC: 03:17 (0:14:51 remaining)
UDP Scan Timing: About 37.72% done; ETC: 03:17 (0:13:44 remaining)
UDP Scan Timing: About 42.74% done; ETC: 03:17 (0:12:37 remaining)
UDP Scan Timing: About 47.75% done; ETC: 03:17 (0:11:30 remaining)
UDP Scan Timing: About 52.77% done; ETC: 03:17 (0:10:24 remaining)
UDP Scan Timing: About 57.79% done; ETC: 03:17 (0:09:17 remaining)
UDP Scan Timing: About 62.80% done; ETC: 03:17 (0:08:11 remaining)
UDP Scan Timing: About 67.82% done; ETC: 03:17 (0:07:05 remaining)
UDP Scan Timing: About 72.84% done; ETC: 03:17 (0:05:58 remaining)
UDP Scan Timing: About 78.08% done; ETC: 03:17 (0:04:49 remaining)
UDP Scan Timing: About 83.10% done; ETC: 03:17 (0:03:43 remaining)
UDP Scan Timing: About 88.12% done; ETC: 03:17 (0:02:37 remaining)
UDP Scan Timing: About 93.13% done; ETC: 03:17 (0:01:31 remaining)
Completed UDP Scan at 03:17, 1317.61s elapsed (65535 total ports)
Nmap scan report for 192.168.3.153
Host is up (0.00098s latency).
All 65535 scanned ports on 192.168.3.153 are in ignored states.
Not shown: 65535 open|filtered udp ports (no-response)
MAC Address: 08:00:27:C4:96:A9 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1317.73 seconds
           Raw packets sent: 131257 (6.340MB) | Rcvd: 1 (28B)

┌──(hacker㉿vbox)-[~]
└─$ 
```