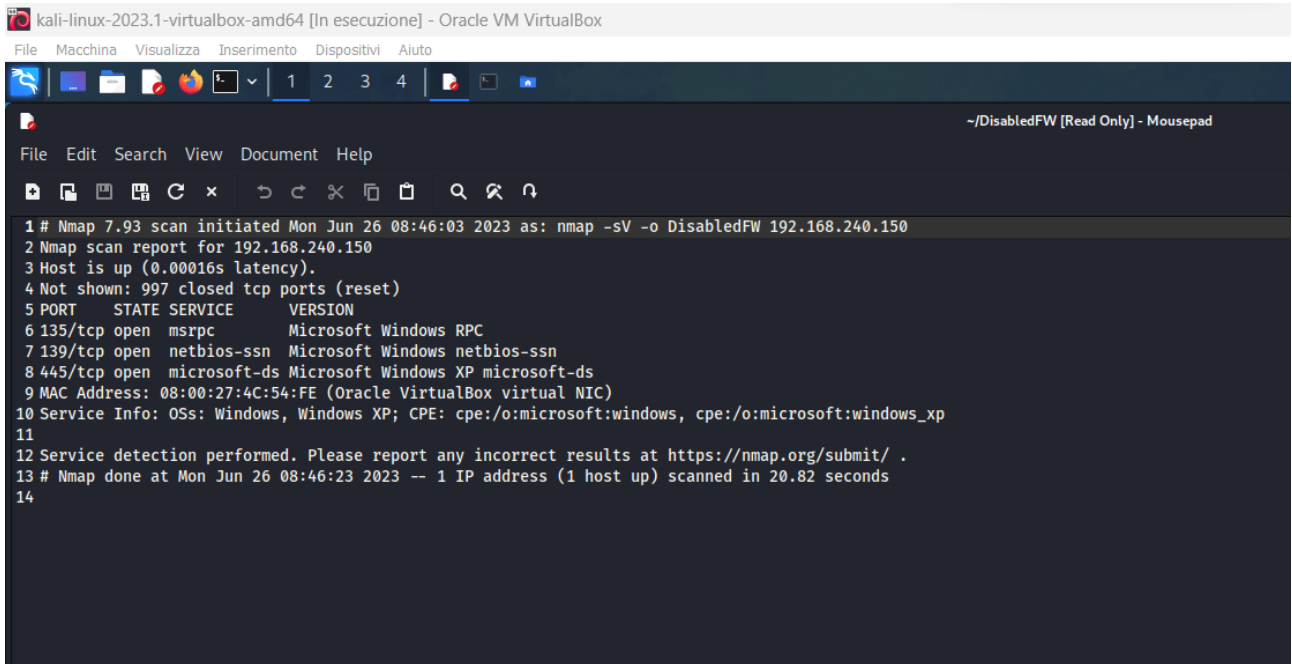


# Epicode Week 3 Day 1

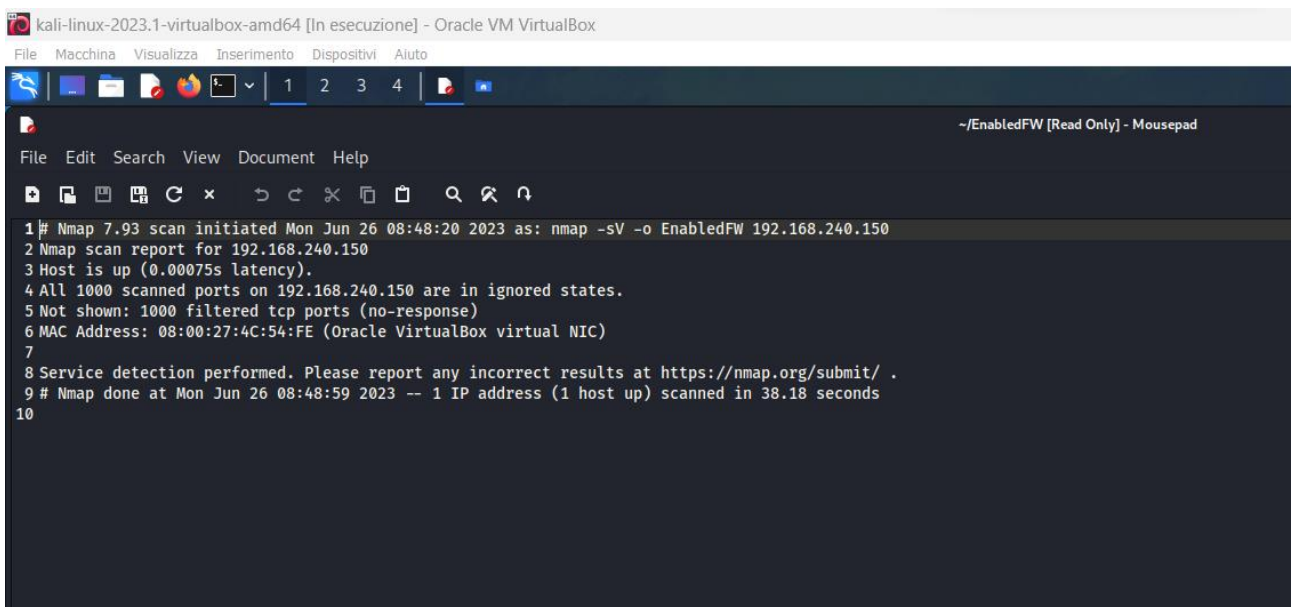
Si può notare come, con il Firewall disabilitato, nmap riesca ad eseguire senza nessun problema la scansione sulla macchina XP bersaglio.



The screenshot shows a terminal window titled "kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox". The terminal is running an nmap scan on 192.168.240.150 with the option -o DisabledFW. The output shows that the host is up and several ports are open, including 135/tcp (msrpc), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds). The scan was completed in 20.82 seconds.

```
1 # Nmap 7.93 scan initiated Mon Jun 26 08:46:03 2023 as: nmap -sV -o DisabledFW 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00016s latency).
4 Not shown: 997 closed tcp ports (reset)
5 PORT      STATE SERVICE      VERSION
6 135/tcp    open  msrpc        Microsoft Windows RPC
7 139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
8 445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
9 MAC Address: 08:00:27:4C:54:FE (Oracle VirtualBox virtual NIC)
10 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
11
12 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
13 # Nmap done at Mon Jun 26 08:46:23 2023 -- 1 IP address (1 host up) scanned in 20.82 seconds
14
```

Molto diverso il risultato nel momento in cui il Firewall viene attivato:



The screenshot shows a terminal window titled "kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox". The terminal is running an nmap scan on 192.168.240.150 with the option -o EnabledFW. The output shows that all 1000 scanned ports are in ignored states, indicating that the firewall is blocking the scan. The scan was completed in 38.18 seconds.

```
1 # Nmap 7.93 scan initiated Mon Jun 26 08:48:20 2023 as: nmap -sV -o EnabledFW 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00075s latency).
4 All 1000 scanned ports on 192.168.240.150 are in ignored states.
5 Not shown: 1000 filtered tcp ports (no-response)
6 MAC Address: 08:00:27:4C:54:FE (Oracle VirtualBox virtual NIC)
7
8 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
9 # Nmap done at Mon Jun 26 08:48:59 2023 -- 1 IP address (1 host up) scanned in 38.18 seconds
10
```

Si noti inoltre, come il file di log, ovviamente vuoto finché il Firewall rimane disattivato, inizi a registrare le policy di “DROP” nei confronti della richiesta di connessione da parte della macchina attaccante.

```
log - Blocco note
File Modifica Formato Visualizza ?
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcppack tc
2023-06-26 14:51:07 DROP TCP 192.168.240.100 192.168.240.150 56803 443 44 S 819054648 0 1024 - -
2023-06-26 14:51:07 DROP TCP 192.168.240.100 192.168.240.150 56803 80 44 S 819054648 0 1024 - - -
2023-06-26 14:51:07 DROP TCP 192.168.240.100 192.168.240.150 56803 135 44 S 819054648 0 1024 - -
2023-06-26 14:51:07 DROP TCP 192.168.240.100 192.168.240.150 56803 3389 44 S 819054648 0 1024 - -
2023-06-26 14:51:07 DROP TCP 192.168.240.100 192.168.240.150 56803 1720 44 S 819054648 0 1024 - -
2023-06-26 14:51:07 DROP TCP 192.168.240.100 192.168.240.150 56803 554 44 S 819054648 0 1024 - -
2023-06-26 14:51:07 DROP TCP 192.168.240.100 192.168.240.150 56803 256 44 S 819054648 0 1024 - -
2023-06-26 14:51:07 DROP TCP 192.168.240.100 192.168.240.150 56803 995 44 S 819054648 0 1024 - -
2023-06-26 14:51:07 DROP TCP 192.168.240.100 192.168.240.150 56803 5900 44 S 819054648 0 1024 - -
2023-06-26 14:51:07 DROP TCP 192.168.240.100 192.168.240.150 56803 25 44 S 819054648 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 25 44 S 819185722 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 5900 44 S 819185722 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 995 44 S 819185722 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 256 44 S 819185722 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 554 44 S 819185722 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 1720 44 S 819185722 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 3389 44 S 819185722 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 135 44 S 819185722 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 80 44 S 819185722 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 443 44 S 819185722 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56803 110 44 S 819054648 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56803 1723 44 S 819054648 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56803 111 44 S 819054648 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56803 22 44 S 819054648 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56803 445 44 S 819054648 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56803 8888 44 S 819054648 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56803 139 44 S 819054648 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56803 3306 44 S 819054648 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56803 199 44 S 819054648 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56803 143 44 S 819054648 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 143 44 S 819185722 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 199 44 S 819185722 0 1024 - -
2023-06-26 14:51:08 DROP TCP 192.168.240.100 192.168.240.150 56805 3306 44 S 819185722 0 1024 - -
```