

LOG FIREWALL WINDOWS XP

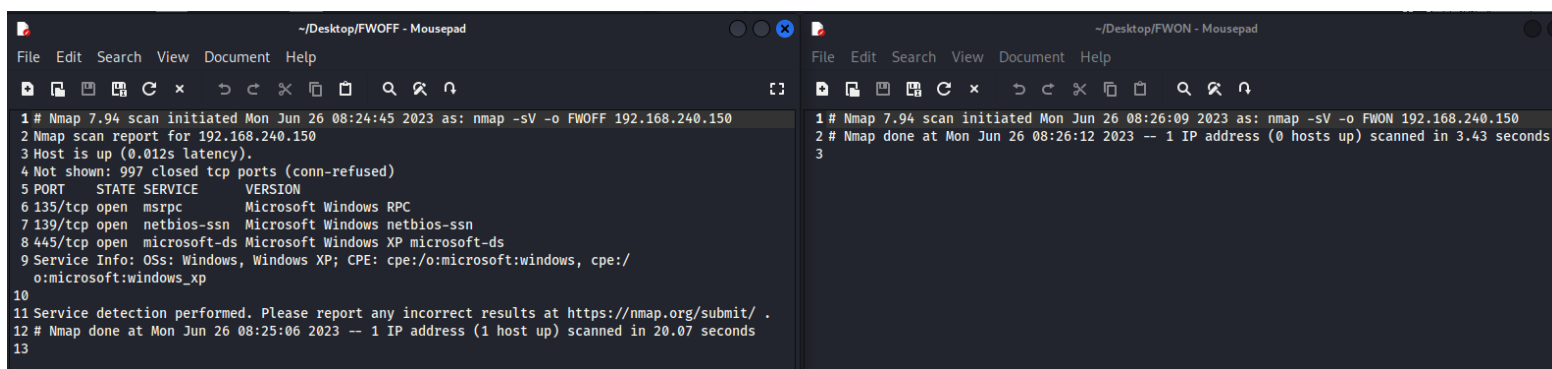
- Inizialmente ho effettuato una scansione NMAP con firewall disattivato su Windows XP, la quale mi ha restituito le porte aperte con regolare servizio attivo sulle stesse.
- In seguito, dopo aver attivato il firewall di Windows XP, ho effettuato nuovamente una scansione NMAP, ma la scansione non mi ha restituito risultati.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o FWOFF
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-26 08:24 EDT
Nmap scan report for 192.168.240.150
Host is up (0.012s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.07 seconds

(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o FWON
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-26 08:26 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.43 seconds
```

- Con lo -switch -o ho salvato i report nel mio KALI.

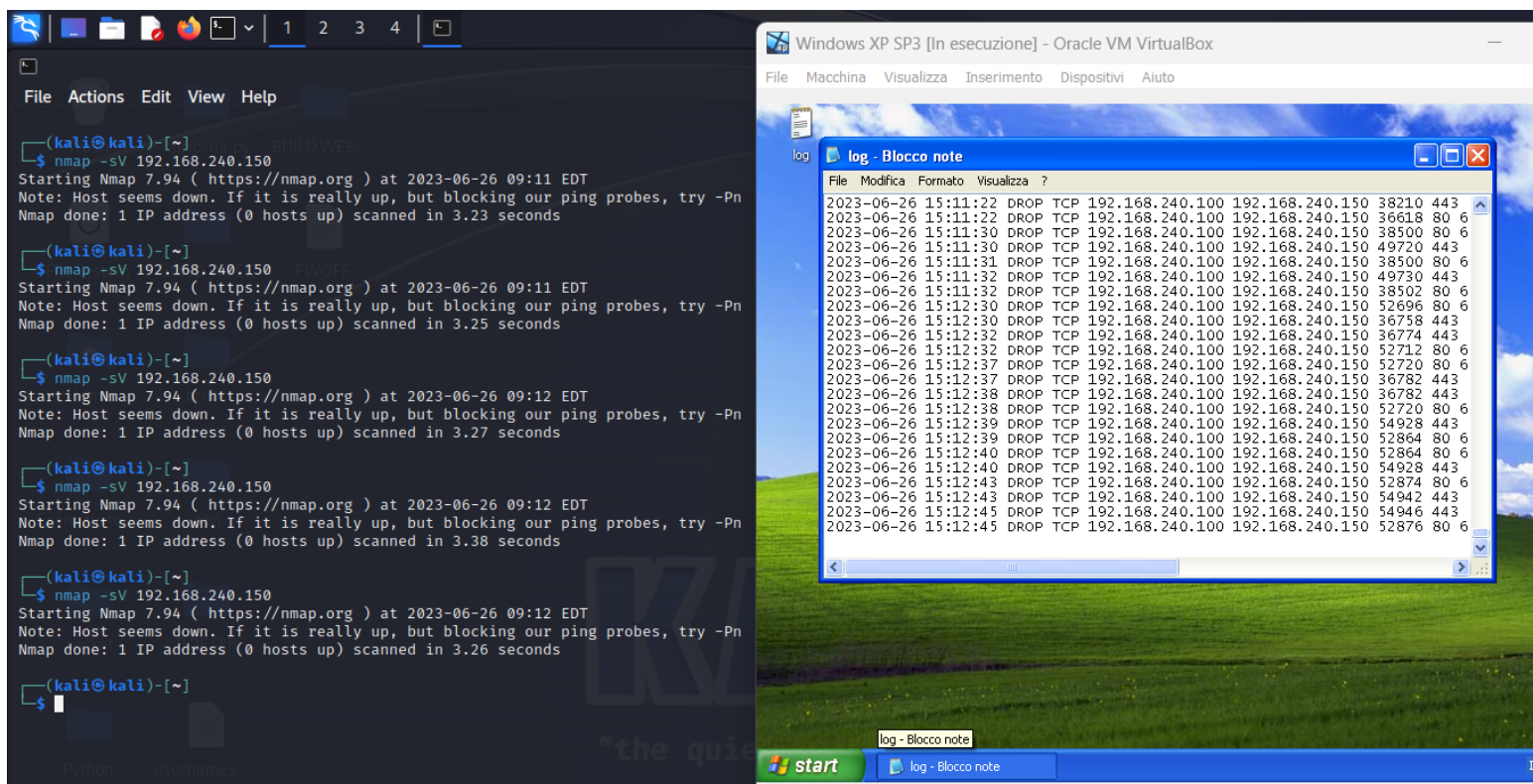


The screenshot shows two side-by-side Mousepad windows. The left window, titled '~/Desktop/FWOFF - Mousepad', contains the Nmap scan results for 192.168.240.150 with the -o FWOFF switch, showing open ports 135, 139, and 445. The right window, titled '~/Desktop/FWON - Mousepad', contains the Nmap scan results for the same IP with the -o FWON switch, showing that the host is down.

```
1 # Nmap 7.94 scan initiated Mon Jun 26 08:24:45 2023 as: nmap -sV -o FWOFF 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.012s latency).
4 Not shown: 997 closed tcp ports (conn-refused)
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 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
12 # Nmap done at Mon Jun 26 08:25:06 2023 -- 1 IP address (1 host up) scanned in 20.07 seconds
13
```

```
1 # Nmap 7.94 scan initiated Mon Jun 26 08:26:09 2023 as: nmap -sV -o FWON 192.168.240.150
2 # Nmap done at Mon Jun 26 08:26:12 2023 -- 1 IP address (0 hosts up) scanned in 3.43 seconds
3
```

- Ho settato le impostazioni avanzate del firewall di Windows, in modo tale da farmi registrare in un file sia i pacchetti ignorati che le connessioni riuscite. Nel frattempo ho eseguito varie scansioni da Kali e il file si aggiornava nel mentre con tutti i tentativi di connessione. Si noti che il tentativo di connessione viene rifiutato “DROP” dal firewall di Windows XP.



- Ho disattivato nuovamente il firewall, ma in questo caso i risultati non venivano registrati nel file di log.

