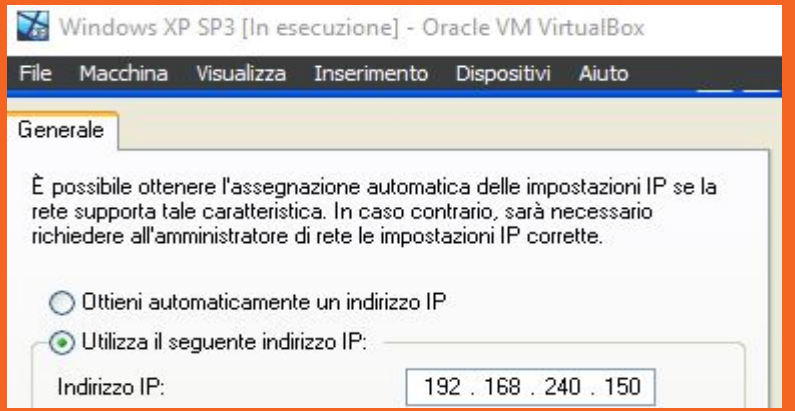
S9/L1 Epicode Cybersecurity

Security Operation: azioni preventive

Indice

- Cambio indirizzi IP
- Prima scansione nmap
- Attivazione Firewall
- Seconda scansione nmap
- Considerazioni

Nell'esercizio di oggi andremo a vedere le differenze tra un firewall disattivato ed uno in funzione tramite nmap. Per prima cosa modifichiamo gli indirizzi IP come richiesto.

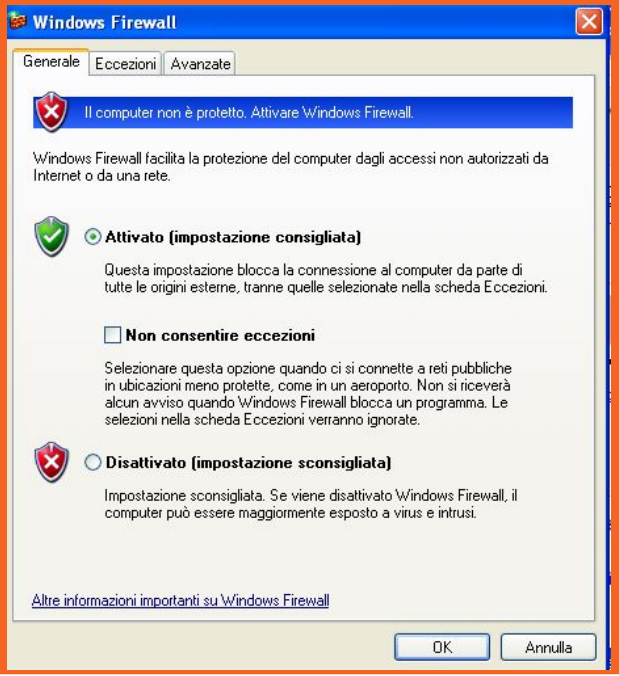


Andiamo quindi ad effettuare una scansione con nmap. Possiamo vedere come 3 porte risultino aperte.

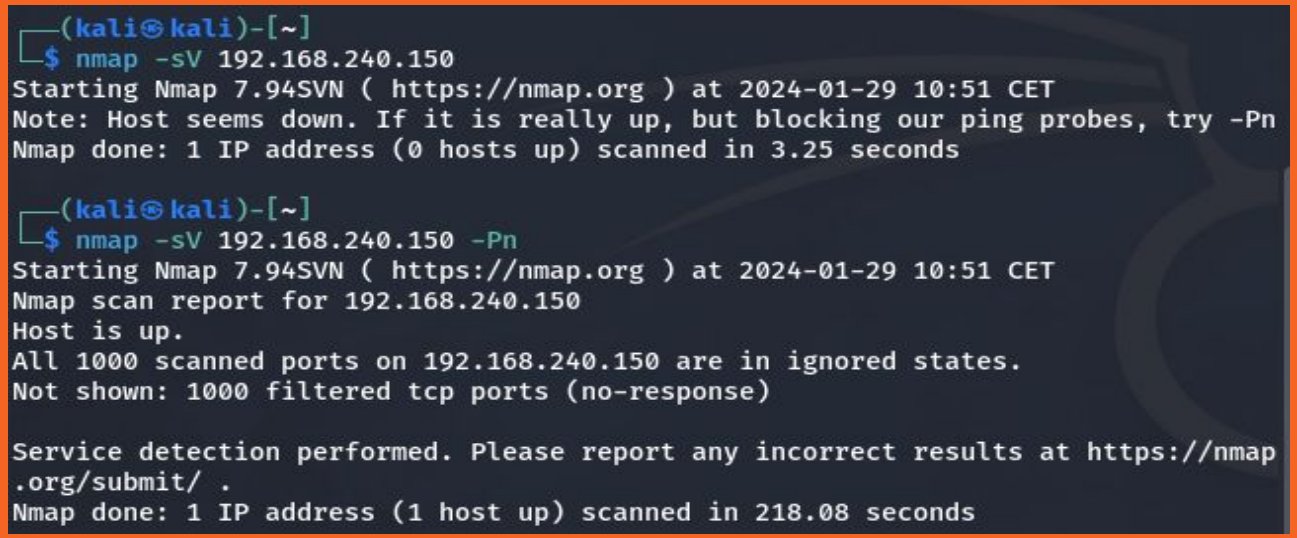
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 10:13 CET
Nmap scan report for 192.168.240.150
Host is up (0.18s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft 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:mi
crosoft: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 21.93 seconds
```

Accedendo a Windows Firewall, andiamo ad attivare il servizio.



Dopo averlo attivato, andiamo ad effettuare la seconda scansione. Win XP risulterà spento, quindi effettuiamo una seconda scansione inserendo il comando '-Pn' come consigliato.



In conclusione, tramite questo esercizio possiamo vedere come, tramite l'attivazione di un firewall, tutte le porte vengano filtrate e di conseguenza diventi molto più difficile exploitare la macchina.