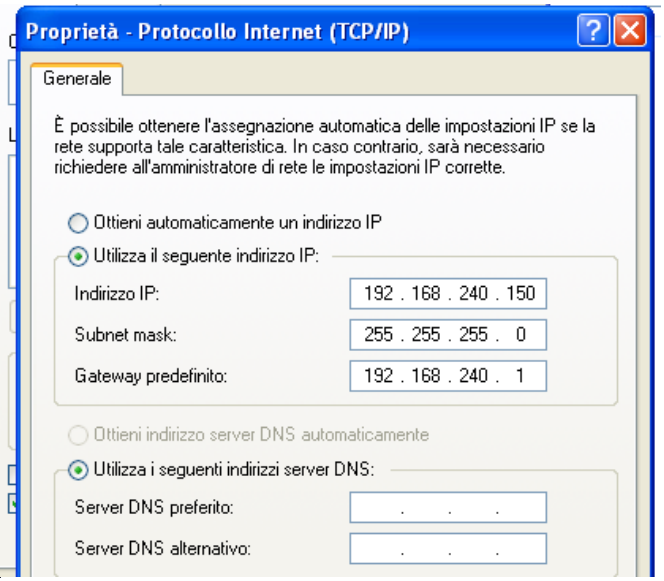
Gabriele Di giampietro **Esercitazione 19-12-2022**

Obbiettivo: Effettuare una scansione nmap sulla VM Windows xp configurata con indirizzo ip 192.169.240.150, prima con Firewall disattivato e poi attivo, analizzare e motivare le differenze dei risultati ottenuti. La macchina attaccante è la VM Kali con ip 192.168.240.100.

Prima parte

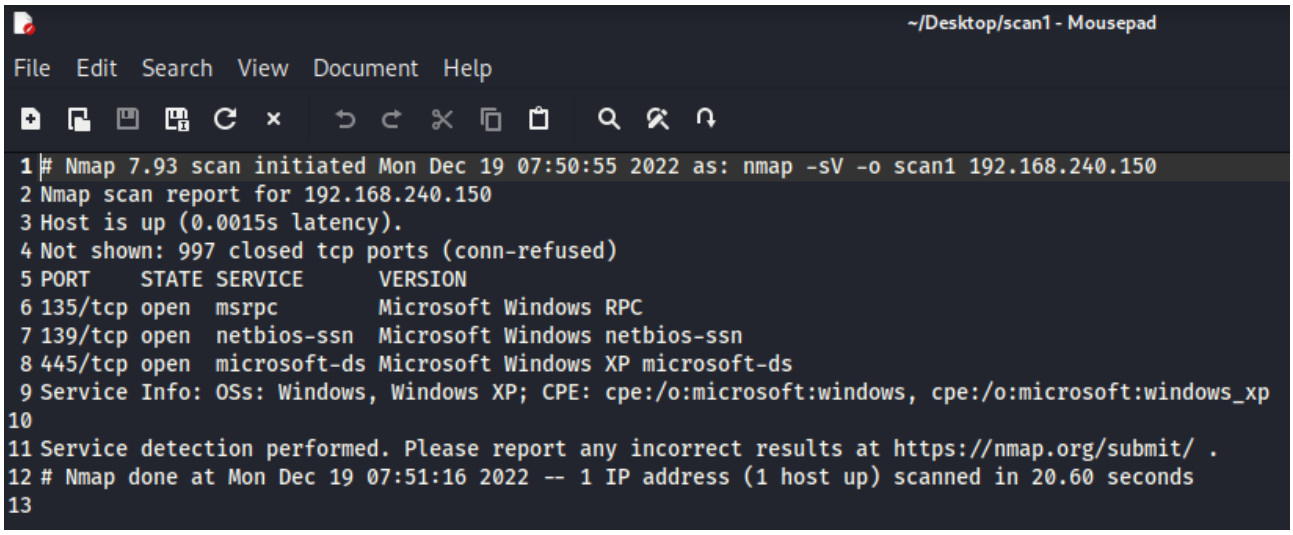
Come prima cosa andiamo ad impostare le configurazioni di rete come richiesto da traccia.

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback


auto eth0
iface eth0 inet static
address 192.168.240.100/24
gateway 192.168.240.1
```



Dopo aver messo in comunicazione le nostre VM, verifichiamo che il Firewall della VM Windows XP sia disattivato.

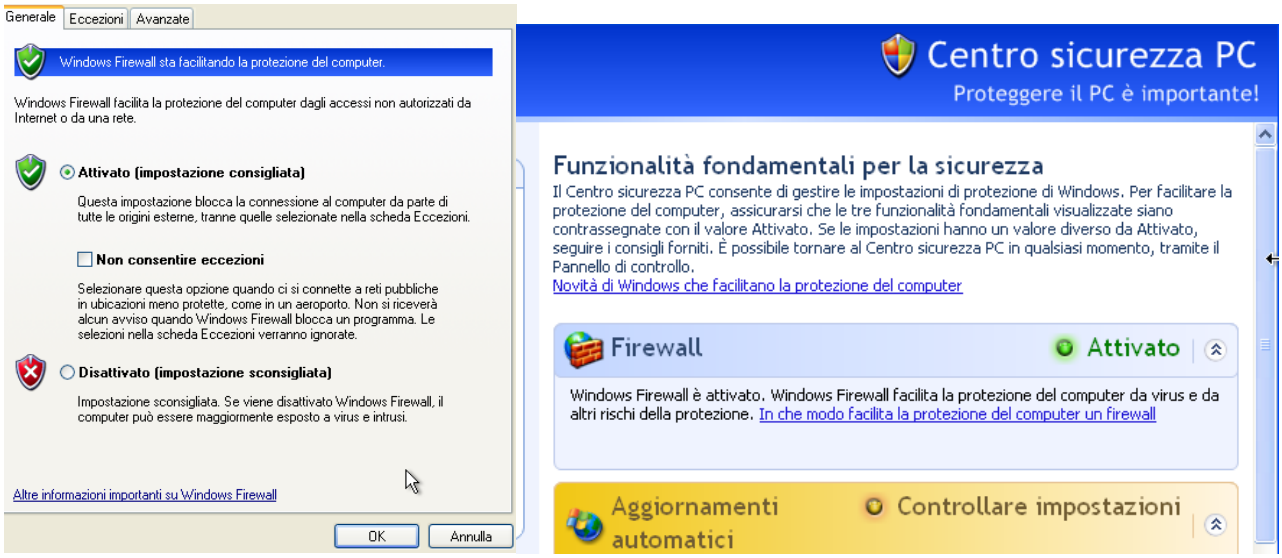
Adesso andiamo a lanciare la nostra scansione nmap sulla nostra macchina target, con lo switch –o ci creeremo un piccolo file report della nostra scansione.



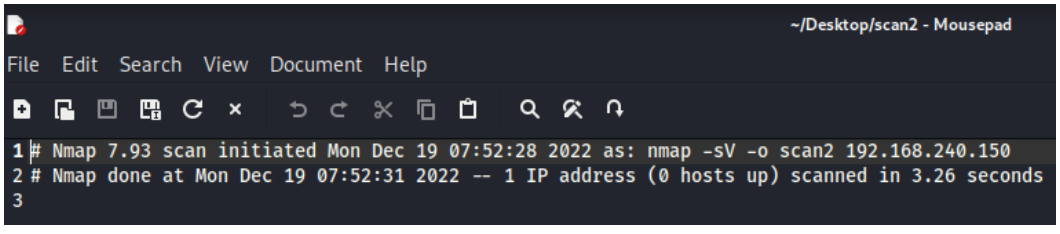
Abbiamo così trovato le porte aperte sul nostro target e con lo switch –sV abbiamo anche enumerato i relativi servizi attivi.

Seconda Parte

Adesso invece andremo ad attivare il Firewall di Windows Xp per notare che differenza riscontriamo se avviamo una scansione.

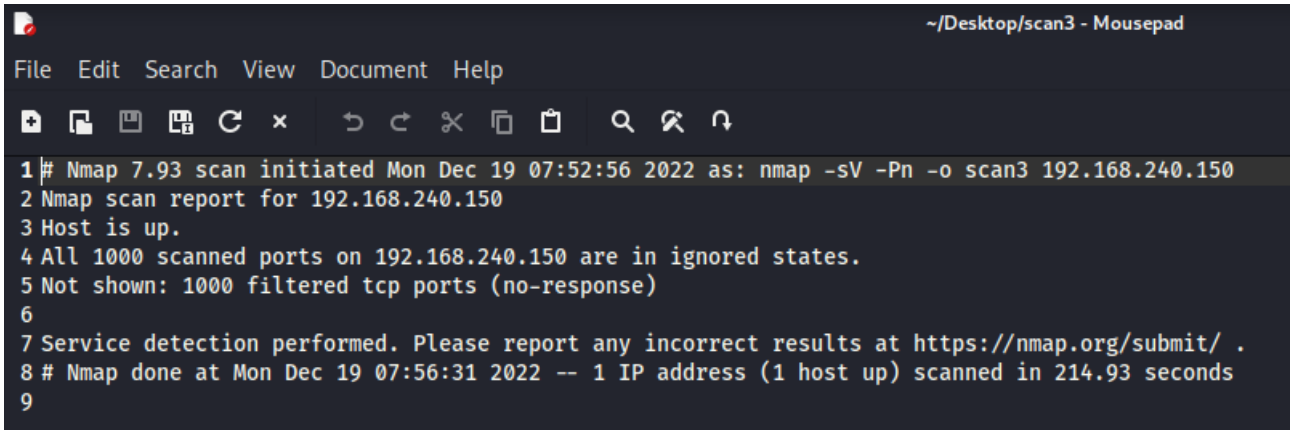


Andiamo adesso ad avviare la nostra scansione con nmap.



Possiamo notare che non siamo riusciti ad enumerare nessun servizio, tantomeno a controllare eventuali porte aperte. Questo perché il Firewall blocca la nostra scansione.

Proviamo ad effettuare un'altra scansione aggiungendo in questo caso lo switch –Pn per aggirare il Firewall ed provare ad ottenere qualche informazione.



In questo caso riusciamo ad ottenere qualche informazione in più, non sappiamo ancora quali porte e servizi sono attivi, notiamo solo che le porte con protocollo TCP sono filtrate e non ci danno responso. Conferma che il Firewall ci sta bloccando la nostra scansione, quindi risulta essere un ottimo strumento come prevenzione del rischio.

Bonus

Abbiamo anche controllato i log che venivano salvati su Windows XP, sul file pfirewall.log che abbiamo impostato sulle opzioni avanzate del firewall, dal quale abbiamo notato che con il firewall attivo registrava la nostra scansione, ma che veniva bloccata indicata dalla scritta DROP che vediamo nell'immagine seguente.