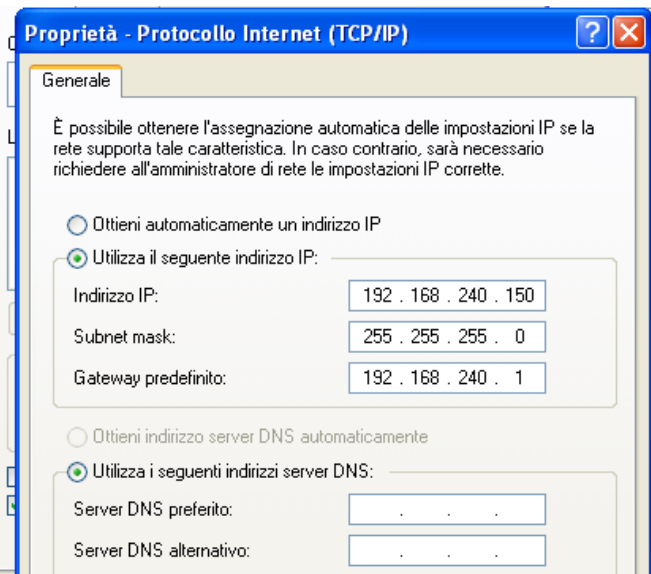


Obbiettivo: Effettuare una scansione nmap sulla VM Windows xp configurata con indirizzo ip 192.169.240.150, prima con Firewall disattivato e poi attivo, analizzare e motivare le differenze dei risultati ottenuti. La macchina attaccante è la VM Kali con ip 192.168.240.100.

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.



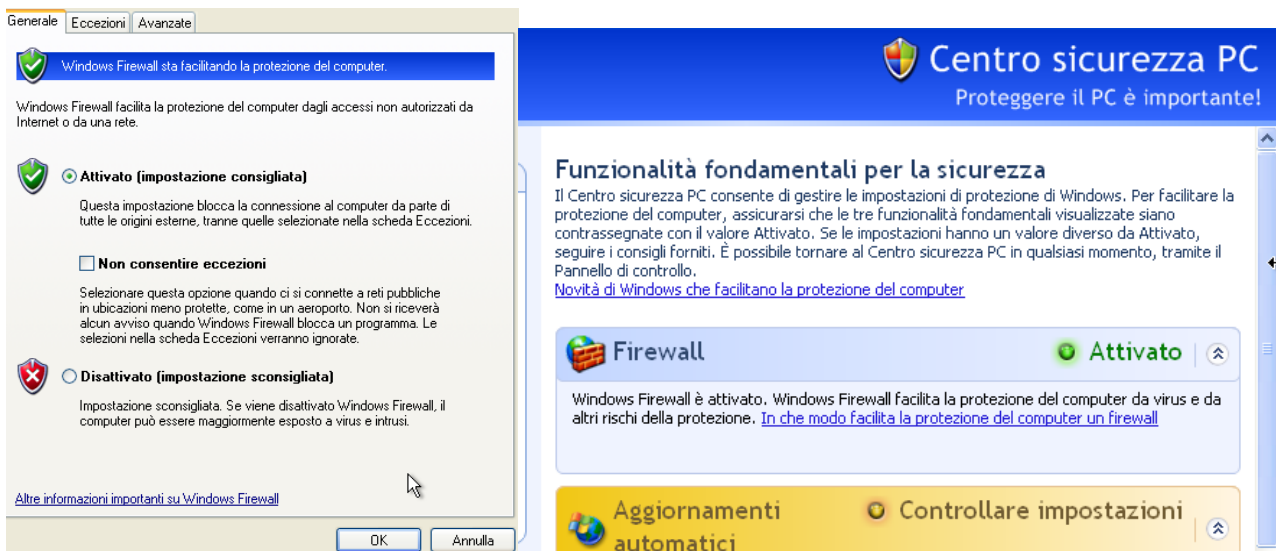
Adesso andiamo a lanciare la nostra scansione nmap sulla nostra macchina target, con lo switch `-o` ci creeremo un piccolo file report della nostra scansione.

```
~/Desktop/scan1 - Mousepad
File Edit Search View Document Help
1 # Nmap 7.93 scan initiated Mon Dec 19 07:50:55 2022 as: nmap -sV -o scan1 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.0015s 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 Dec 19 07:51:16 2022 -- 1 IP address (1 host up) scanned in 20.60 seconds
13
```

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.

```
~/Desktop/scan2 - Mousepad
File Edit Search View Document Help
1 # Nmap 7.93 scan initiated Mon Dec 19 07:52:28 2022 as: nmap -sV -o scan2 192.168.240.150
2 # Nmap done at Mon Dec 19 07:52:31 2022 -- 1 IP address (0 hosts up) scanned in 3.26 seconds
3
```

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

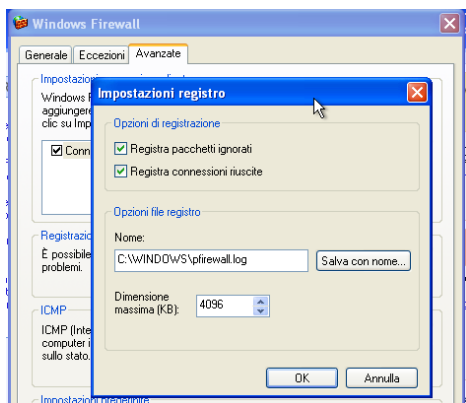
Proviamo ad effettuare un'altra scansione aggiungendo in questo caso lo switch -Pn per aggirare il Firewall ed provare ad ottenere qualche informazione.

```
~/Desktop/scan3 - Mousepad
File Edit Search View Document Help
1 # Nmap 7.93 scan initiated Mon Dec 19 07:52:56 2022 as: nmap -sV -Pn -o scan3 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up.
4 All 1000 scanned ports on 192.168.240.150 are in ignored states.
5 Not shown: 1000 filtered tcp ports (no-response)
6
7 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
8 # Nmap done at Mon Dec 19 07:56:31 2022 -- 1 IP address (1 host up) scanned in 214.93 seconds
9
```

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.



```
pfirewall - 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 tcpack tcpwin icmp type icmpcode info path
2022-12-19 17:13:03 DROP TCP 192.168.240.100 192.168.240.150 52434 80 60 S 676660478 0 64240 - - - RECEIVE
2022-12-19 17:13:03 DROP TCP 192.168.240.100 192.168.240.150 58524 443 60 S 3450274134 0 64240 - - - RECEIVE
2022-12-19 17:13:04 DROP TCP 192.168.240.100 192.168.240.150 58524 443 60 S 3450274134 0 64240 - - - RECEIVE
2022-12-19 17:13:05 DROP TCP 192.168.240.100 192.168.240.150 58532 443 60 S 3998542537 0 64240 - - - RECEIVE
2022-12-19 17:13:05 DROP TCP 192.168.240.100 192.168.240.150 52442 80 60 S 622419554 0 64240 - - - RECEIVE
```