

SECURITY OPERATIONS: AZIONI PREVENTIVE

ATTIVITÀ

1. Verifica dell'impatto che l'abilitazione di un firewall ha sui risultati di una scansione dei servizi dall'esterno
2. Monitoraggio dei log prodotti dalle operazioni effettuate

REQUISITI

- IP Kali Linux: 192.168.240.100
- IP Windows XP: 192.168.240.150

REQUISITI

Preliminarmente alle attività di test odierne, configuriamo gli indirizzi di rete delle macchine coinvolte sulla stessa rete interna e riavviamo i servizi di rete, nel seguente modo:

Kali → 192.168.240.100

Windows XP → 192.168.240.150

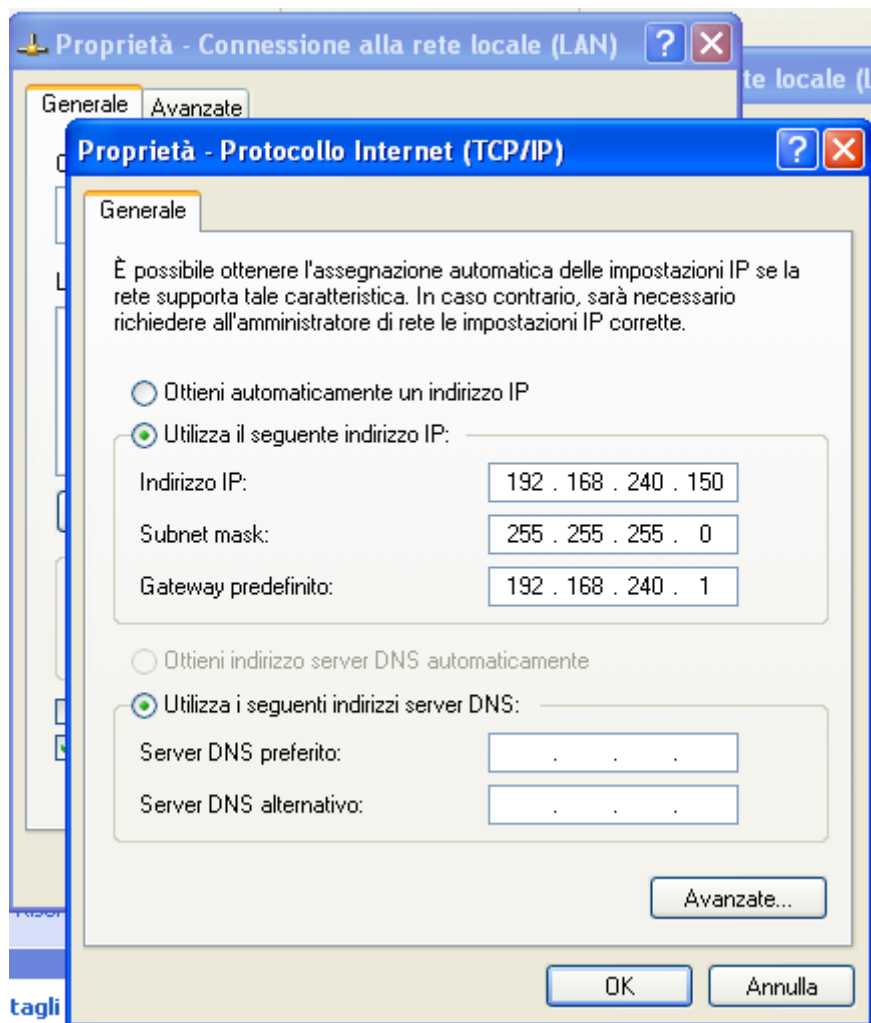
```
GNU nano 6.4 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

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
```

```
(kali@kali)-[~]
$ sudo /etc/init.d/networking restart
[sudo] password for kali:
Restarting networking (via systemctl): networking.service.
```



Verifichiamo l'effettiva comunicazione tra le due macchine con un ping test, che ha esito positivo.

```
(kali@kali)~$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data:
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.584 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1.26 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.94 ms
^C
--- 192.168.240.150 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.584/1.260/1.943/0.554 ms
```

```
Esecuzione di Ping 192.168.240.100 con 32 byte di dati:
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64
```

ATTIVITÀ

1. Verifica dell'impatto che l'abilitazione di un firewall ha sui risultati di una scansione dei servizi dall'esterno

Lo scopo dell'attività odierna è mettere a confronto i risultati di una scansione dei servizi dall'esterno su una VM Windows XP in assenza di protezione derivante da un firewall, con una scansione sulla medesima VM in presenza di un firewall abilitato.

Per prima cosa, verifichiamo che il firewall in Windows XP sia disabilitato:



Possiamo procedere con il primo test: da Kali, avviamo una scansione dei servizi con nmap, attivando gli switch **-sV** – Version Detection, e **-o** (produzione di un report dei risultati della scansione in output su un file di testo).

Eseguiamo dunque il comando

nmap -sV -o /home/kali/Desktop/Report_No-Firewall.txt 192.168.240.150

```
(kali㉿kali)-[~]
$ nmap -sV -o /home/kali/Desktop/Report_No-Firewall.txt 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-20 03:37 CET
Nmap scan report for 192.168.240.150
Host is up (0.27s 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 21.55 seconds
```

```

1 # Nmap 7.93 scan initiated Tue Dec 20 03:37:36 2022 as: nmap -sV -o /home/kali/Desktop/
  Report_No-Firewall.txt 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.27s 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 Tue Dec 20 03:37:57 2022 -- 1 IP address (1 host up) scanned in 21.55 seconds
13

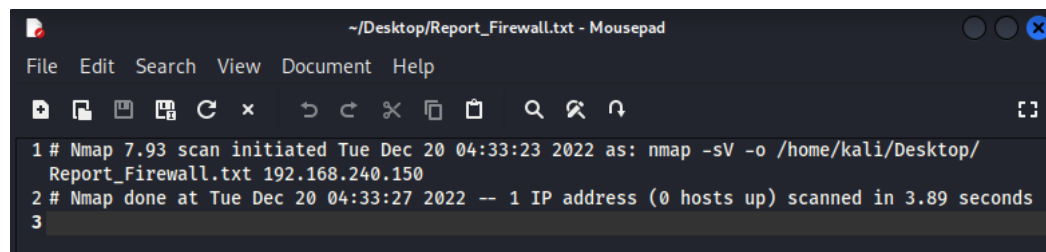
```

Come si vede, la scansione restituisce dati su alcune porte aperte e i relativi servizi in ascolto. Inoltre, viene correttamente rilevato il sistema operativo.

Procediamo adesso all'attivazione del firewall in Windows XP, e ripetiamo la scansione:



```
(kali㉿kali)-[~]
$ nmap -sV -o /home/kali/Desktop/Report_Firewall.txt 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-20 04:33 CET
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 3.89 seconds
```



```
~/Desktop/Report_Firewall.txt - Mousepad
File Edit Search View Document Help
1 # Nmap 7.93 scan initiated Tue Dec 20 04:33:23 2022 as: nmap -sV -o /home/kali/Desktop/Report_Firewall.txt 192.168.240.150
2 # Nmap done at Tue Dec 20 04:33:27 2022 -- 1 IP address (0 hosts up) scanned in 3.89 seconds
3
```

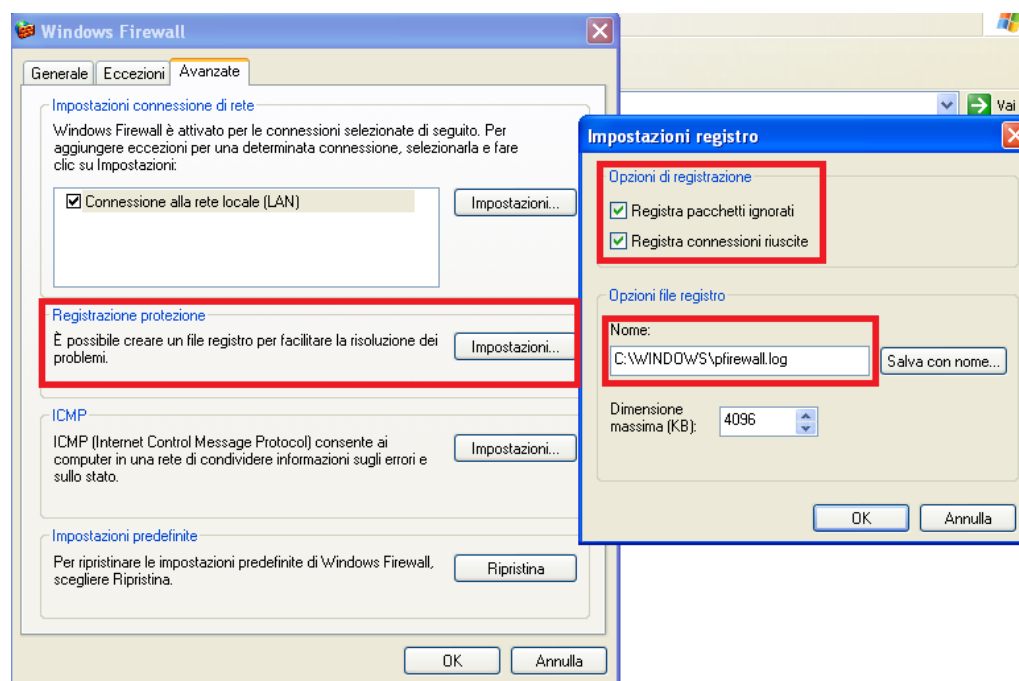
Come è evidente, l'attivazione del firewall rende la macchina apparentemente irraggiungibile (*"host seems down"*). Volendo investigare più approfonditamente, eseguiamo una scansione che salta l'host discovery (switch **-Pn**): l'informazione che ne ricaviamo è che le porte analizzate sono **filtrate**. Abbiamo dunque la conferma che sulla macchina target è attivo un firewall.

```
(kali㉿kali)-[~]
$ nmap -Pn -T5 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-20 04:37 CET
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

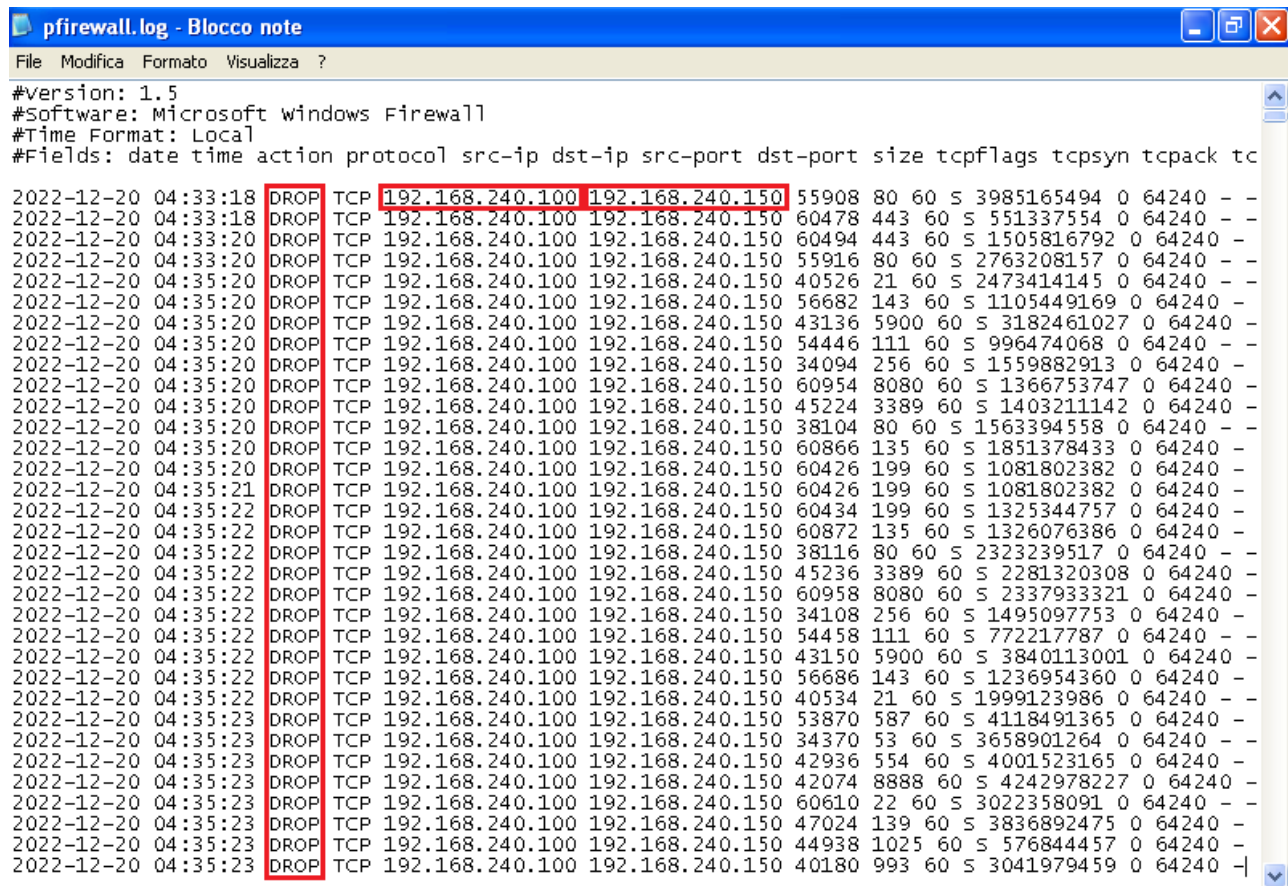
Nmap done: 1 IP address (1 host up) scanned in 64.32 seconds
```

2. Monitoraggio dei log prodotti dalle operazioni effettuate

Procediamo all'abilitazione dei log per le attività del firewall:



I log verranno salvati nella cartella C:\WINDOWS all'interno del file **pfirewall.log**



```
#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 tc

2022-12-20 04:33:18 DROP TCP 192.168.240.100 192.168.240.150 55908 80 60 S 3985165494 0 64240 - -
2022-12-20 04:33:18 DROP TCP 192.168.240.100 192.168.240.150 60478 443 60 S 551337554 0 64240 - -
2022-12-20 04:33:20 DROP TCP 192.168.240.100 192.168.240.150 60494 443 60 S 1505816792 0 64240 - -
2022-12-20 04:33:20 DROP TCP 192.168.240.100 192.168.240.150 55916 80 60 S 2763208157 0 64240 - -
2022-12-20 04:35:20 DROP TCP 192.168.240.100 192.168.240.150 40526 21 60 S 2473414145 0 64240 - -
2022-12-20 04:35:20 DROP TCP 192.168.240.100 192.168.240.150 56682 143 60 S 1105449169 0 64240 - -
2022-12-20 04:35:20 DROP TCP 192.168.240.100 192.168.240.150 43136 5900 60 S 3182461027 0 64240 - -
2022-12-20 04:35:20 DROP TCP 192.168.240.100 192.168.240.150 54446 111 60 S 996474068 0 64240 - -
2022-12-20 04:35:20 DROP TCP 192.168.240.100 192.168.240.150 34094 256 60 S 1559882913 0 64240 - -
2022-12-20 04:35:20 DROP TCP 192.168.240.100 192.168.240.150 60954 8080 60 S 1366753747 0 64240 - -
2022-12-20 04:35:20 DROP TCP 192.168.240.100 192.168.240.150 45224 3389 60 S 1403211142 0 64240 - -
2022-12-20 04:35:20 DROP TCP 192.168.240.100 192.168.240.150 38104 80 60 S 1563394558 0 64240 - -
2022-12-20 04:35:20 DROP TCP 192.168.240.100 192.168.240.150 60866 135 60 S 1851378433 0 64240 - -
2022-12-20 04:35:20 DROP TCP 192.168.240.100 192.168.240.150 60426 199 60 S 1081802382 0 64240 - -
2022-12-20 04:35:21 DROP TCP 192.168.240.100 192.168.240.150 60426 199 60 S 1081802382 0 64240 - -
2022-12-20 04:35:22 DROP TCP 192.168.240.100 192.168.240.150 60434 199 60 S 1325344757 0 64240 - -
2022-12-20 04:35:22 DROP TCP 192.168.240.100 192.168.240.150 60872 135 60 S 1326076386 0 64240 - -
2022-12-20 04:35:22 DROP TCP 192.168.240.100 192.168.240.150 38116 80 60 S 2323239517 0 64240 - -
2022-12-20 04:35:22 DROP TCP 192.168.240.100 192.168.240.150 45236 3389 60 S 2281320308 0 64240 - -
2022-12-20 04:35:22 DROP TCP 192.168.240.100 192.168.240.150 60958 8080 60 S 2337933321 0 64240 - -
2022-12-20 04:35:22 DROP TCP 192.168.240.100 192.168.240.150 34108 256 60 S 1495097753 0 64240 - -
2022-12-20 04:35:22 DROP TCP 192.168.240.100 192.168.240.150 54458 111 60 S 772217787 0 64240 - -
2022-12-20 04:35:22 DROP TCP 192.168.240.100 192.168.240.150 43150 5900 60 S 3840113001 0 64240 - -
2022-12-20 04:35:22 DROP TCP 192.168.240.100 192.168.240.150 56686 143 60 S 1236954360 0 64240 - -
2022-12-20 04:35:22 DROP TCP 192.168.240.100 192.168.240.150 40534 21 60 S 1999123986 0 64240 - -
2022-12-20 04:35:23 DROP TCP 192.168.240.100 192.168.240.150 53870 587 60 S 4118491365 0 64240 - -
2022-12-20 04:35:23 DROP TCP 192.168.240.100 192.168.240.150 34370 53 60 S 3658901264 0 64240 - -
2022-12-20 04:35:23 DROP TCP 192.168.240.100 192.168.240.150 42936 554 60 S 4001523165 0 64240 - -
2022-12-20 04:35:23 DROP TCP 192.168.240.100 192.168.240.150 42074 8888 60 S 4242978227 0 64240 - -
2022-12-20 04:35:23 DROP TCP 192.168.240.100 192.168.240.150 60610 22 60 S 3022358091 0 64240 - -
2022-12-20 04:35:23 DROP TCP 192.168.240.100 192.168.240.150 47024 139 60 S 3836892475 0 64240 - -
2022-12-20 04:35:23 DROP TCP 192.168.240.100 192.168.240.150 44938 1025 60 S 576844457 0 64240 - -
2022-12-20 04:35:23 DROP TCP 192.168.240.100 192.168.240.150 40180 993 60 S 3041979459 0 64240 -
```

Come possiamo notare, all'interno del file di log abbiamo evidenza di tutte le azioni effettuate dal firewall nell'interazione con il **source IP**, ossia l'indirizzo IP di Kali (192.168.240.100): le richieste di connessione sono state scartate (**DROP**). Inoltre, per ogni tentativo di connessione vengono anche registrate altre preziose informazioni come il timestamp, la source port e la destination port.