

SECURITY OPERATION: Azioni Preventive

L'esercitazione di oggi è di verificare in che modo l'attivazione del firewall impatta sul risultato di una scansione dei servizi dall'esterno.

FASE 1

Per prima cosa abbiamo impostato i nostri ambienti di lavoro come richiesto dalla traccia.

KALI: Tramite il comando **sudo nano /etc/network/interfaces** siamo andati ad impostare l'IP – 192.168.240.100

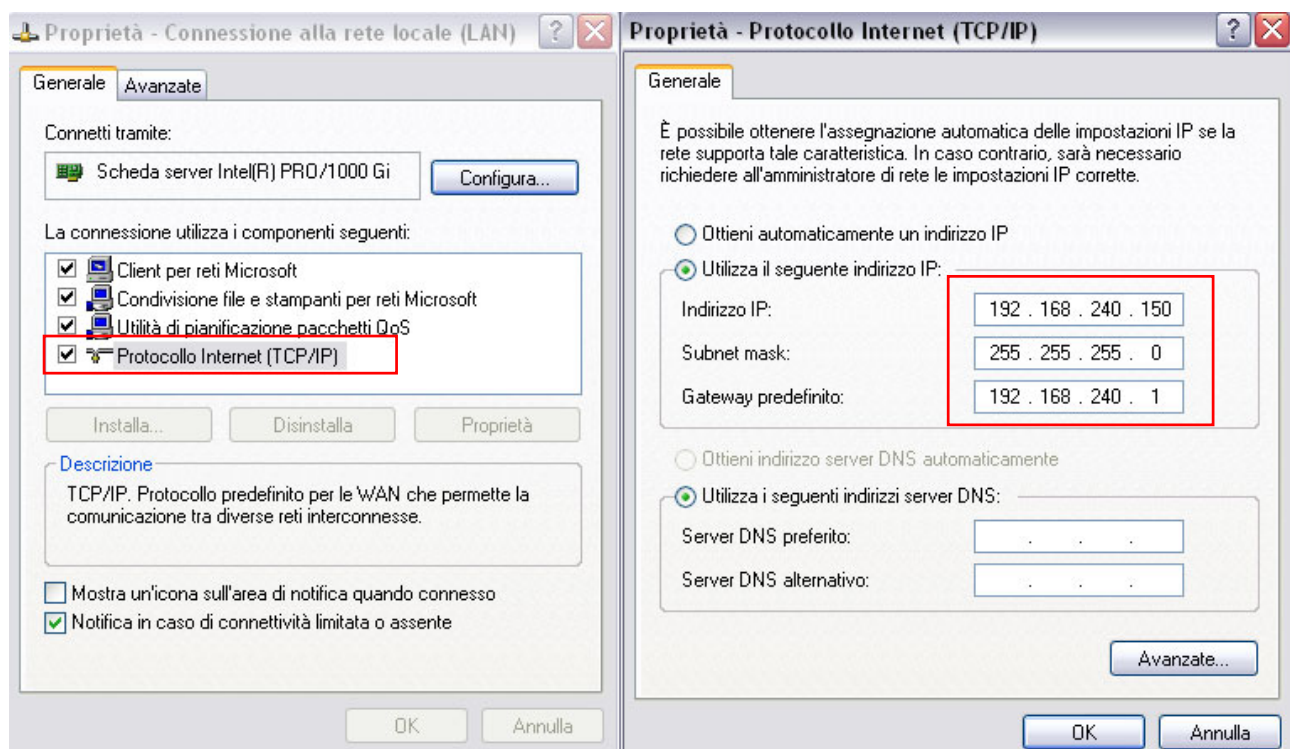
```
File Actions Edit View Help File Actions Edit View Help
GNU nano 6.3
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet static

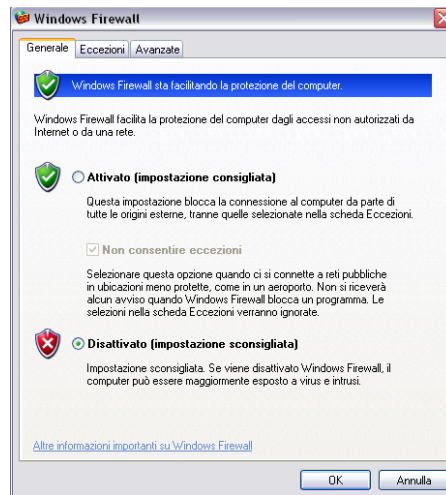
auto eth0
iface eth0 inet static
address 192.168.240.100
netmask 255.255.255.0
network 192.168.240.0
broadcast 192.168.240.255
gateway 192.168.240.1
```

WIN XP: Tramite la schermata di opzioni avanzate nella scheda di rete, protocollo internet TCP/IP impostiamo l'IP – 192.168.240.150



FASE 2

Nella seconda fase abbiamo effettuato una scansione tramite il tool nmap presente su Kali. Per prima cosa andiamo a disattivare il firewall su Windows XP presente come opzioni in Pannello di controllo >> **Windows Firewall**



Utilizzando il comando `nmap -sV -o "nomefile_report" IP BERSAGLIO` diamo inizio alla scansione.

Gli switch inseriti permettono una scansione che come output ci restituisce la Versione dei servizi attivi (-sV) e la creazione di un file di log alla fine (-o "nomefile_log").

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)~[~/Desktop]
$ nmap -sV -o report_nofirewall 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:23 EST
Nmap scan report for 192.168.240.150
Host is up (0.00029s 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 20.77 seconds
```

```
~/Desktop/report_nofirewall - Mousepad
File Edit Search View Document Help
1 # Nmap 7.92 scan initiated Mon Dec 19 08:23:22 2022 as: nmap -sV -o report_nofirewall 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00029s 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 08:23:43 2022 -- 1 IP address (1 host up) scanned in 20.77 seconds
13 |
```

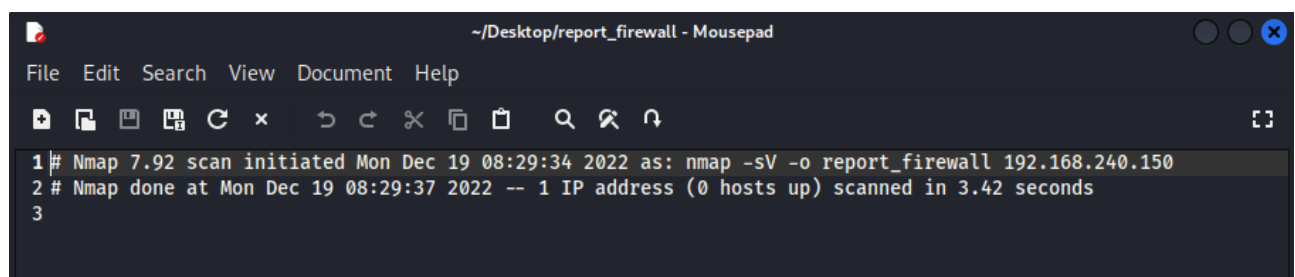
Qui possiamo vedere il risultato del file in output che nmap di crea

Stessa cosa anche per la seconda scansione. Attiviamo il Firewall di Windows XP e lanciamo di nuovo nmap, modificando solamente il nome in output del log che ci salverà



```
(kali㉿kali)-[~/Desktop]
$ nmap -sV -o report_firewall 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:29 EST
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 3.42 seconds
```

Possiamo notare immediatamente che con il firewall attivo e nessuna policy che permetta alla macchina attaccante di “entrare” non ci verrà restituita alcuna informazione utile.



Bonus

Come bonus ci era stato chiesto di notare che differenze c'erano nel log presenti su Windows XP.

Prima di tutto entrano nelle impostazioni del Firewall >> Avanzate.

Da qui ci spostiamo su Registrazione Protezione >> impostazioni e diamo una direzione al nostro file di log che verrà creato.



Con il firewall attivo possiamo avere un log delle "connessioni" in entrata che sono avvenute.

Possiamo notare al suo interno che la nostra macchina Kali (src-ip) ha tentato una connessione con Windows XP (dst-ip). L'azione **DROP** ci fa capire perché il log rilasciato nella seconda scansione di nmap era vuoto

