

Epicode
CS-0124
Pratica S9/L1
Francesco Ficetti

Traccia.....	3
Svolgimento.....	4
Configurazione degli indirizzi IP.....	4
Kali Linux.....	4
Windows XP.....	5
Attivazione/disattivazione del firewall.....	6
Scansione con nmap.....	7
Firewall spento.....	7
Firewall acceso.....	7
Conclusioni.....	8

Traccia

Verificare in che modo l'attivazione del firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

- 1- Disabilitare il firewall sulla macchina Windows XP.
- 2- Effettuare una scansione con nmap, utilizzare lo switch -sV.
- 3- Abilitare il firewall sulla macchina Windows XP.
- 4- Effettuare un'altra scansione con nmap.
- 5- Trovare le eventuali differenze e motivarle.

Requisiti:

Indirizzo IP di Kali: 192.168.240.100

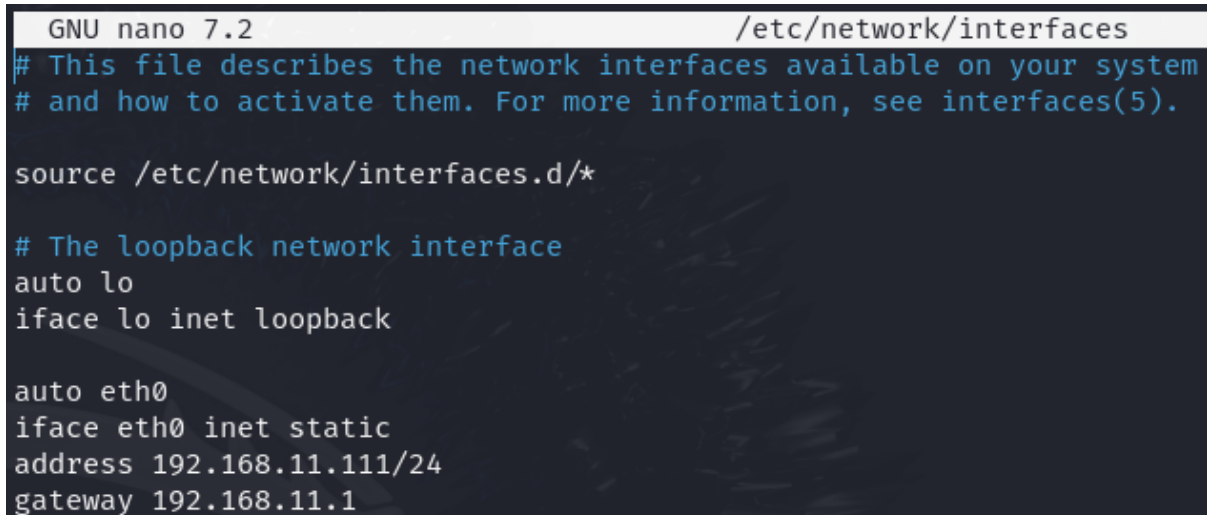
Indirizzo IP di Windows XP: 192.168.240.150

Svolgimento

Configurazione degli indirizzi IP

Kali Linux

Eseguire il comando *sudo nano /etc/network/interfaces*, per modificare il file di configurazione delle interfacce di rete.



```
GNU nano 7.2 /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 192.168.11.111/24
gateway 192.168.11.1
```

Una volta modificato il file come in figura, per applicare le modifiche è necessario riavviare il servizio, per farlo, eseguire il comando *sudo /etc/init.d/networking restart*.

Windows XP

Cliccare su *Start* → *Pannello di controllo* → *Rete e connessioni internet* → *Connessioni di rete* → doppio clic su *Connessione alla rete locale (LAN)*.

Si apre una nuova finestra, cliccare su *Proprietà*.

Si apre una nuova finestra, doppio clic su *Protocollo Internet (TCP/IP)*.

Si apre la finestra seguente:

Proprietà - Protocollo Internet (TCP/IP)

Generale

È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.

☐ Ottieni automaticamente un indirizzo IP

☒ Utilizza il seguente indirizzo IP:

Indirizzo IP: 192 . 168 . 240 . 150

Subnet mask: 255 . 255 . 255 . 0

Gateway predefinito: 192 . 168 . 240 . 1

☐ Ottieni indirizzo server DNS automaticamente

☒ Utilizza i seguenti indirizzi server DNS:

Server DNS preferito: . . .

Server DNS alternativo: . . .

Avanzate...

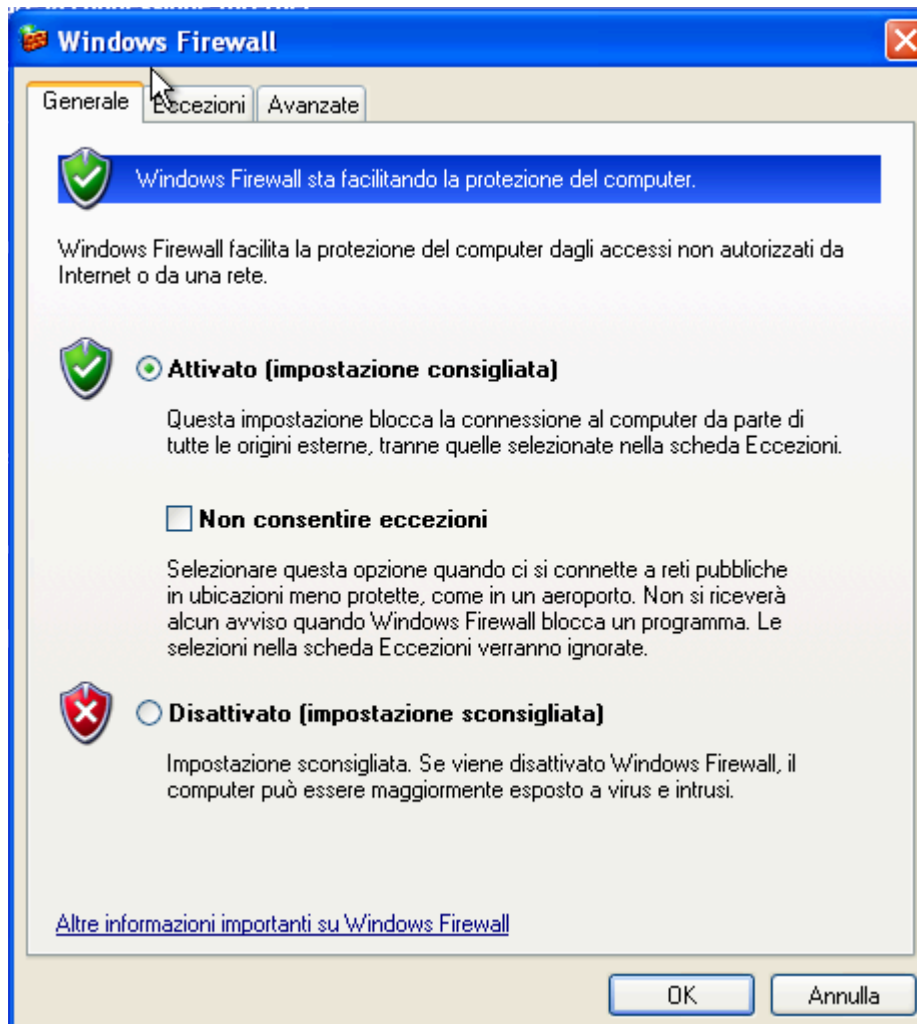
OK Annulla

Compilare i campi richiesti e cliccare su *OK*.

Attivazione/disattivazione del firewall

Cliccare su *Start* → *Pannello di controllo* → *Rete e connessioni internet* → Windows Firewall.

Si apre la finestra seguente:



Se è selezionata la voce Attivato (impostazione consigliata), il firewall è acceso.

Se è selezionata la voce Disattivato (impostazione sconsigliata), il firewall è spento.

Scansione con nmap

Firewall spento

Il comando da eseguire è *nmap 192.168.240.150 -sV -o report_firewallOff*.

```
(francesco@kali)-[~]
$ nmap 192.168.240.150 -sV -o report_FirewallOff
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 11:15 CET
Nmap scan report for 192.168.240.150
Host is up (0.42s 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 21.13 seconds
```

Per leggere il contenuto del report, eseguire il comando *cat report_firewallOff*.

```
(francesco@kali)-[~]
$ cat report_FirewallOff
# Nmap 7.94SVN scan initiated Mon Mar 18 11:15:36 2024 as: nmap -sV -o report_FirewallOff 192.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.42s 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 at Mon Mar 18 11:15:57 2024 -- 1 IP address (1 host up) scanned in 21.13 seconds
```

Nmap è riuscito a trovare 3 porte aperte, ed i loro relativi servizi.

Firewall acceso

Il comando da eseguire è *nmap 192.168.240.150 -sV -o report_firewallOn*.

```
(francesco@kali)-[~]
$ nmap 192.168.240.150 -sV -o report_FirewallOn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 11:14 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 3.42 seconds
```

Per leggere il contenuto del report, eseguire il comando *cat report_firewallOn*.

```
(francesco@kali)-[~]
$ cat report_FirewallOn
# Nmap 7.94SVN scan initiated Mon Mar 18 11:14:54 2024 as: nmap -sV -o report_FirewallOn 192.168.240.150
# Nmap done at Mon Mar 18 11:14:57 2024 -- 1 IP address (0 hosts up) scanned in 3.42 seconds
```

Nmap non è riuscito ad eseguire la scansione, perché il firewall blocca tutte le richieste di ping, di conseguenza nmap considera questo host spento.

Per eseguire una scansione ignorando il ping, il comando è il seguente: *nmap 192.168.240.150 -sV -Pn -o report_FirewallOn_noPing*.

```
(francesco@kali)~$ nmap 192.168.240.150 -sV -Pn -o report_FirewallOn_noPing
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 15:01 CET
Nmap scan report for 192.168.240.150
Host is up (0.0073s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
2869/tcp   closed iclslap
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 24.11 seconds
```

Per leggere il contenuto del report, eseguire il comando *cat report_firewallOn_noPing*.

```
(francesco@kali)~$ cat report_FirewallOn_noPing
# Nmap 7.94SVN scan initiated Mon Mar 18 15:01:44 2024 as: nmap -sV -Pn -o report_FirewallOn_noPing 192.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.0073s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
2869/tcp   closed iclslap
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 at Mon Mar 18 15:02:08 2024 -- 1 IP address (1 host up) scanned in 24.11 seconds
```

Nmap è riuscito a trovare alcune porte aperte, ma non sono uguali a quelle trovate in precedenza.

Conclusioni

Il firewall blocca la maggior parte delle richieste provenienti dall'esterno, aumentando così la sicurezza della macchina.