

# Pratica S9/L1

Traccia:

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.

La macchina Windows XP in formato OVA che abbiamo utilizzato nella Unit 2 ha di default il Firewall disabilitato.

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch `-sV`, per la service detection)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch `-sV`

Requisiti:

Configurate l'indirizzo di Windows XP come di seguito: 192.168.240.150

Configurate l'indirizzo della macchina Kali come di seguito:

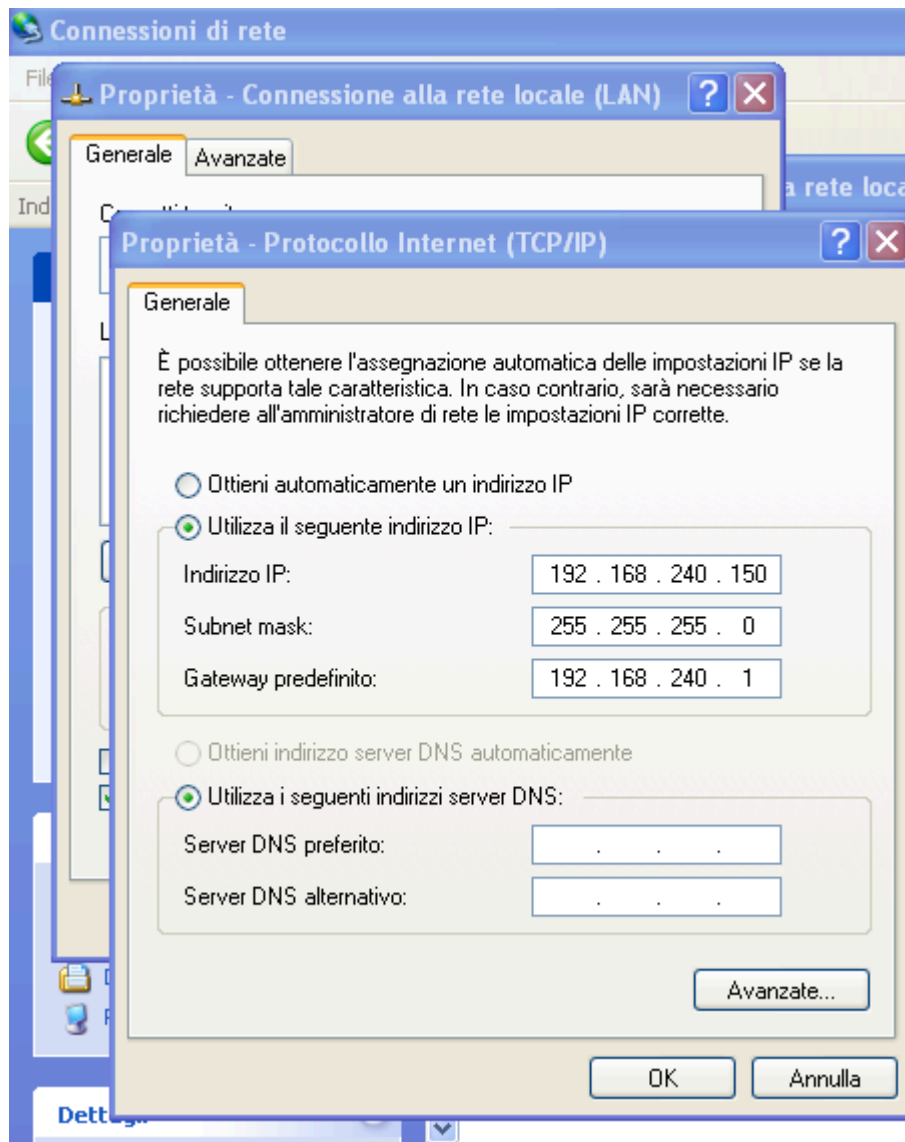
192.168.240.100

Strumento utilizzato :

- nmap

- 1) Configurazione delle rete dei dispositivi

Dalla richiesta abbiamo configurato gli indirizzi ip delle due macchine kali e windows



```
GNU nano 2.2.6 /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/*

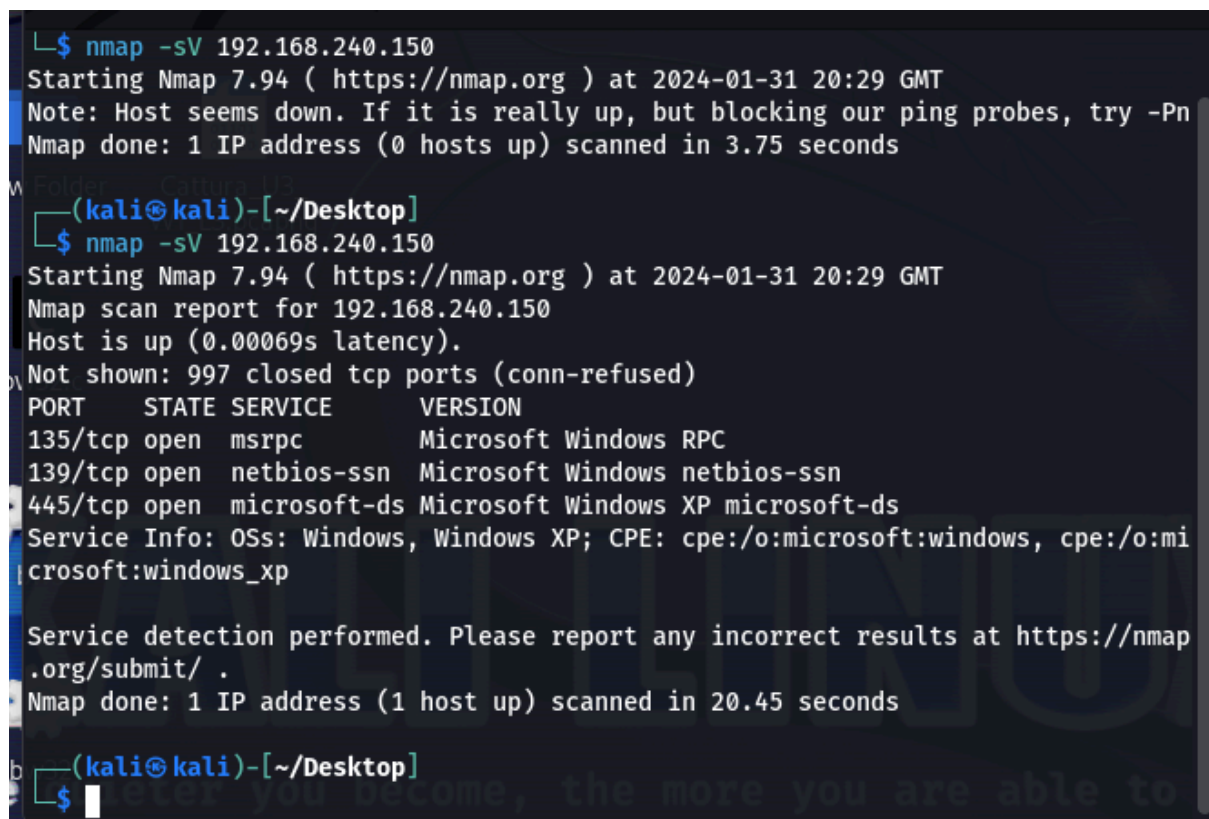
# The loopback network interface
auto lo
iface lo inet loopback

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

## 2) Nmap without firewall on

Utilizziamo lo strumento Nmap per fare le scansioni alle porte di windows con il seguente comando :

```
nmap -sV 192.168.240.150
```



```
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-31 20:29 GMT
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 3.75 seconds

(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-31 20:29 GMT
Nmap scan report for 192.168.240.150
Host is up (0.00069s 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 20.45 seconds

(kali㉿kali)-[~/Desktop]
└─$
```

Notiamo dall'immagine che ci sono 3 porte aperte che possono essere sfruttate dagli attaccanti .

## 3) Nmap with Firewall on

Facendo uno secondo scan con il firewall attivato , possiamo notare dall'immagine che non ci da nessun risultato trovato

```
Nmap scan report for 192.168.240.150
Host is up (0.00069s 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 20.45 seconds
```

```
(kali㉿kali)-[~/Desktop]
```

```
$ nmap -sV 192.168.240.150
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-31 20:31 GMT
```

```
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
```

```
Ping Scan Timing: About 50.00% done; ETC: 20:31 (0:00:01 remaining)
```

```
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 3.34 seconds
```

```
(kali㉿kali)-[~/Desktop]
```

```
$
```