

FIREWALL

TESTING

Michelangelo Borromeo



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



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 e -o nomefilereport per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch-sV.
5. Trovare le eventuali differenze e motivarle.

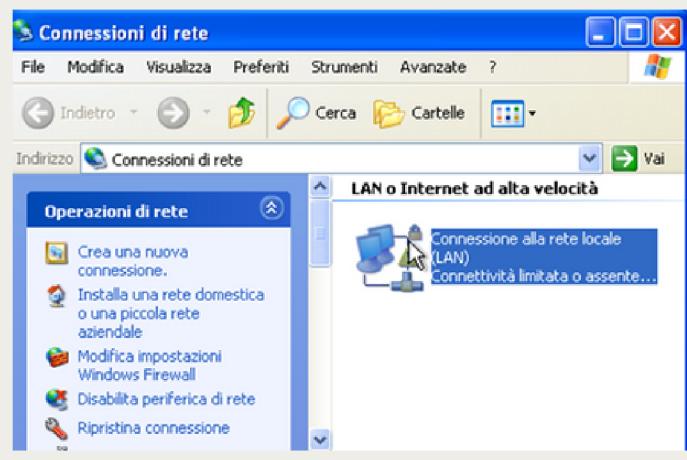


Configurazione IP Windows XP

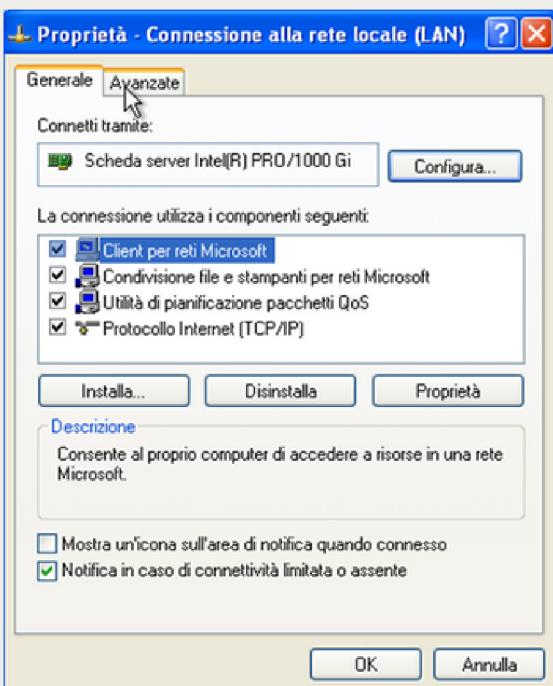


CONFIGURAZIONE IP WINDOWS XP

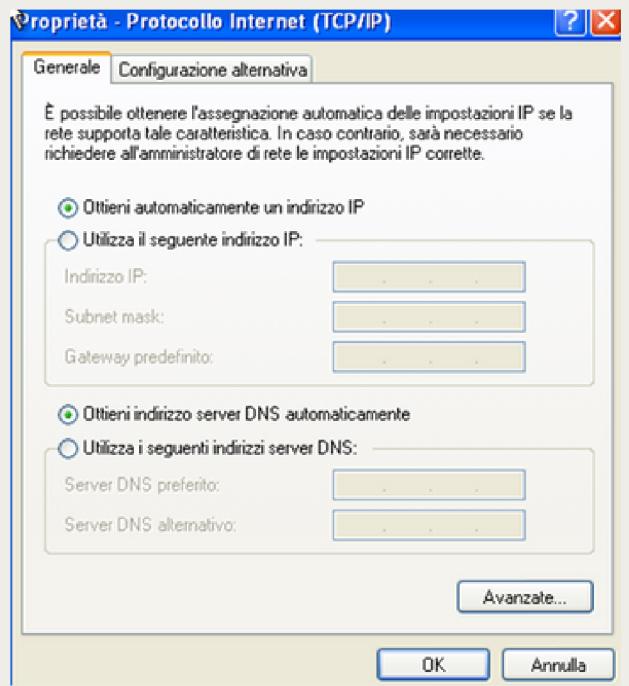
1) ci rechiamo alle impostazioni di rete e selezioniamo la rete locale (**LAN**)



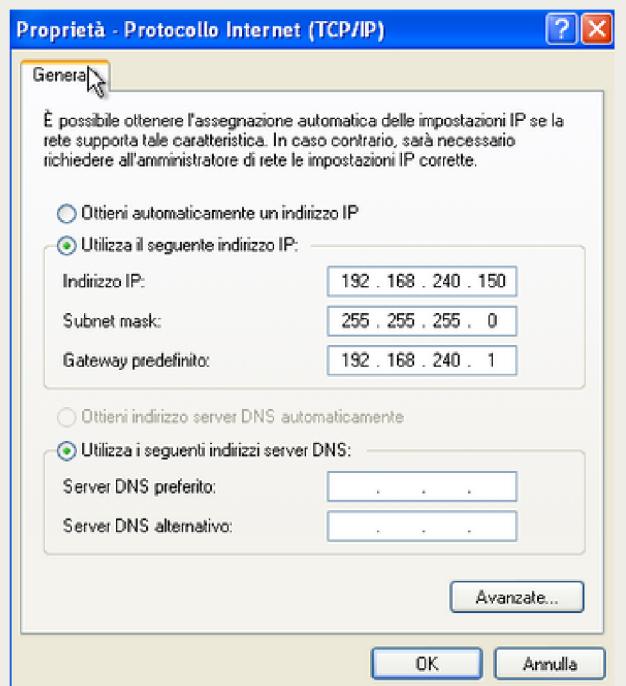
2) apriamo il pannello e selezioniamo protocollo internet (**TCP/IP**)



3) una volta aperto possiamo iniziare ad immettere l'ip da noi deciso



4) immettiamo
l'IP: 192.168.240.150
S.Mask: 255.255.255.0
gateway: 192.168.240.1



Configurazione IP

Kali Linux



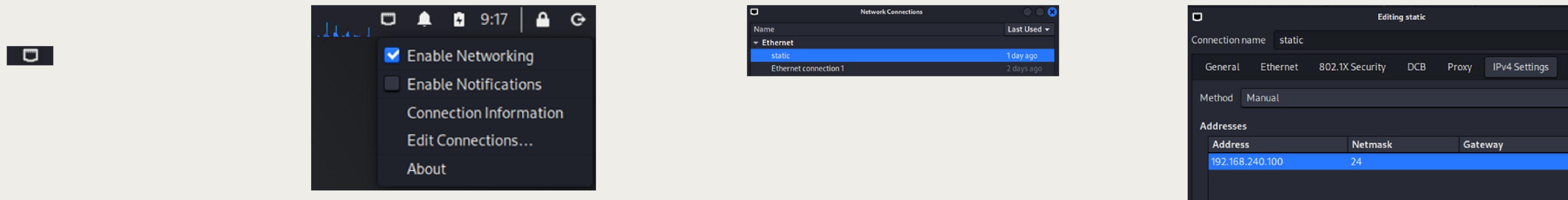
CONFIGURAZIONE IP KALI LINUX

1) Dal Desktop clicchiamo in alto a destra sull'iconcina di rete

2) Uscirà una piccola tabella e clicchiamo **Edit Connections**

3) Selezioniamo la voce **static**

4) immettiamo
l'IP: 192.168.240.100
NetMask: 24



5) dalla shell restartiamola scheda di rete con il comando:
sudo /etc/init.d/networking restart

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

Nmap
Firewall Off



NMAP SENZA FIREWALL

Eseguiamo una scansione con nmap utilizzando kali verso la macchina Windows XP con il comando

```
nmap -sV 192.168.240.150 -oN scan1
```

Questo comando farà una scansione di un host specifico cercando di identificare i servizi in esecuzione e le loro versioni, e salva i risultati in un file chiamato scan1.

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -oN scan1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 15:42 CEST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.240.150
Host is up (0.0012s 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 20.92 seconds
```



NMAP SENZA FIREWALL

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -oN scan1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 15:42 CEST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.240.150
Host is up (0.0012s 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 20.92 seconds
```

siamo riusciti ad identificare delle porte vulnerabili:

135 è una porta di per la comunicazione remota utilizzata dal servizio Microsoft DCE/RPC (Distributed Computing Environment / Remote Procedure Call), noto anche come "MSRPC". le vulnerabilità note: **Blaster worm, DoS e Buffer Overflow in DCOM**.

139 è una porta per la condivisione di file e stampanti su reti locali. utilizzata dal servizio NetBIOS Session Service, che è una parte del protocollo NetBIOS (Network Basic Input/Output System).

vulnerabilità note: **Brute Force attack, Accesso non autorizzato e Spoofing**.

445 è una porta per la condivisione di file e risorse di rete senza la necessità di NetBIOS. utilizzata dal protocollo Microsoft-DS (Directory Services) e SMB (Server Message Block).

Vulnerabilità note: **Eternal blue, Smb relay attacks, Information disclosure**.



Nmap Firewall On



NMAP CON FIREWALL

Eseguiamo una scansione con nmap utilizzando kali verso la macchina Windows XP con il comando

```
nmap -sV 192.168.240.150 -oN scan1
```

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -oN scan1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 15:56 CEST
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 3.17 seconds
```

Differenze:

Quando il firewall di Windows XP è attivato, vengono applicate delle regole predefinite che bloccano le connessioni in entrata su queste porte, rendendole non accessibili dall'esterno. Il firewall controlla e filtra il traffico di rete, impedendo alle connessioni non autorizzate di raggiungere questi servizi.

Quando il firewall di Windows XP è disattivato, non ci sono restrizioni sulle connessioni di rete in entrata e in uscita. Di conseguenza, le porte 135, 139 e 445 risultano aperte e accessibili perché i servizi associati (come DCOM, NetBIOS e SMB) sono in esecuzione e ascoltano su queste porte.

