SECURITY OPERATION

- FIREWALL DI WINDOWS XP -

ESERCIZIO S9/L1

L’ESERCIZIO DI OGGI CONSISTE NEL VERIFICARE IN CHE MODO L’ATTIVAZIONE DEL FIREWALL IMPATTA IL RISULTATO DI UNA SCANSIONE DEI SERVIZI DALL’ESTERNO.

1. Andiamo a configurare le nostre macchine come richiesto con i seguenti indirizzi IP:
   - Macchina Windows XP: 192.168.240.150
   - Macchina Kali: 192.168.240.100

2. Andiamo ad eseguire le scansioni, utilizzando NMAP per verificare i servizi attivi e le porte dalla macchina Kali su quella di Windows XP, utilizzando lo switch –sV per la service detection
   - Scansione con il firewall attivo sulla macchina di Windows XP
   - Scansione con il firewall non attivo sulla macchina di Windows XP

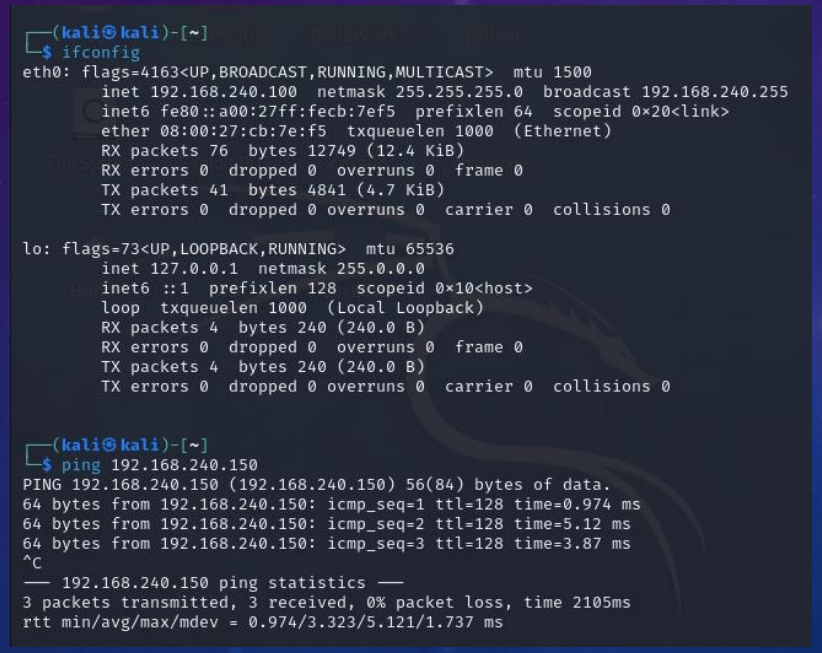
3. Evidenziare le differenze delle due scansioni effettuate

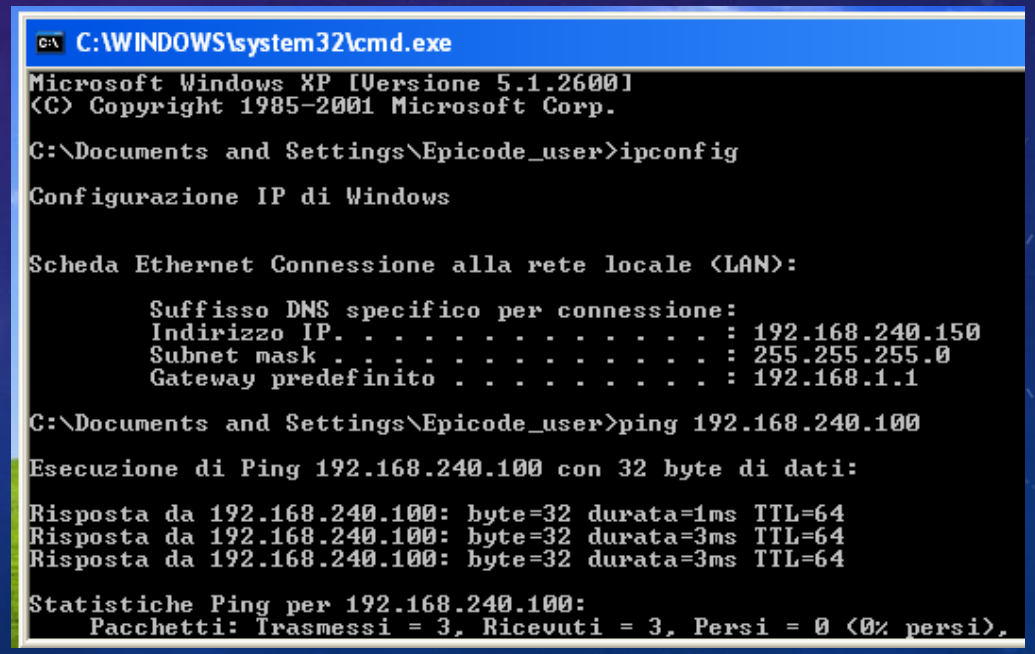
1. CONFIGURIAMO LE NOSTRE MACCHINE COME RICHIESTO CON I SEGUENTI INDIRIZZI IP:

- Macchina windows XP: 192.168.240.150
- Macchina kali: 192.168.240.100

Verifichiamo con il comando ‘ifconfig’ su kali e ‘ipconfig’ su windows xp le impostazioni di rete

Facciamo un ping per verificare che le macchine comunicano tra di loro, utilizzando il comando ‘ping «ipmacchinatarget»’

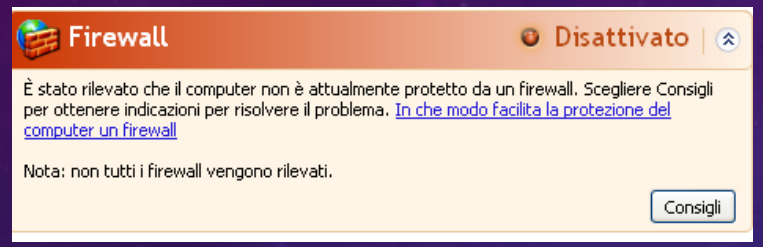




2. ESEGUIAMO LE SCANSIONI, UTILIZZANDO NMAP SULLA MACCHINA TARGET WINDOWS XP

Per effettuare la scansione utilizziamo il comando ‘nmap’ e lo switch ‘–sV’ per la service detection
Facciamo prima una scansione con il firewall disattivato e poi ripetiamo la scansione con il firewall attivo

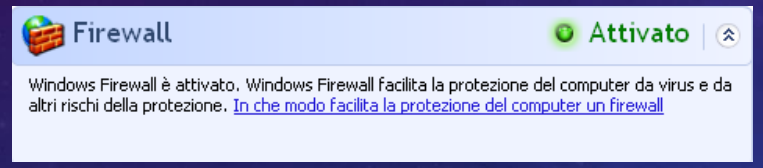
- Scansione con il firewall disattivato




```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 07:25 EST
Nmap scan report for 192.168.240.150
Host is up (0.00094s 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 20.75 seconds
```

- Scansione con il firewall attivo




```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 07:28 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 3.16 seconds
```

Il ping viene bloccato e quindi non riusciamo ad effettuare la scansione, proviamo ad utilizzare il comando ‘nmap –sV –pN «iptarget» per effettuare una scansione senza la risposta del ping, anche in questo caso non otteniamo molte informazioni utili.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 07:28 EST
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)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 221.75 seconds
```

3.DIFFERENZE DELLE DUE SCANSIONI EFFETTUATE

- Come possiamo vedere con il firewall disattivato, nmap riesce ad identificare le porte aperte sul sistema, indicando quali porte ci sono in ascolto per le connessioni in entrata, inoltre trova anche i servizi in esecuzione su ciascuna porta aperta, con i rispettivi versioni specifiche di software. Inoltre riusciamo ad ottenere anche le informazioni sul sistema operativo della macchina target.
- Con il firewall attivo le richieste di scansione vengono bloccate, non lasciando l'accesso ad informazioni sulle porte e servizi, ne ad altre informazioni sulla macchina.

CONCLUSIONI

E' estremamente importante avere un firewall attivo su un qualsiasi sistema operativo in uso, poiché ci aiuta a proteggere il sistema sia da attacchi di rete sia da malware, bloccando i tentativi di accesso non autorizzati e filtrando il traffico dannoso. Il firewall filtra il traffico in base alle porte e ai protocolli, aiutando cosi a prevenire exploit che potrebbero sfruttare vulnerabilità nei servizi di rete. Riduce anche i rischi di attacchi da remoto, limitando i servizi e le porte accessibili dall'esterno. Quindi è importante avere sempre il software del firewall aggiornato e configurato correttamente.