Security Operation: Azioni Preventive

Traccia

- Cambiare IP delle due macchine come di seguito:
  Windows XP: 192.168.240.150
  Kali: 192.168.240.100
- Con Firewall disattivato effettuare una scansione con nmap con switch -sV e -o
- Ripetere la stessa scansione con Firewall attivo
- Trovare e motivare le differenze

Cambio Indirizzi IP

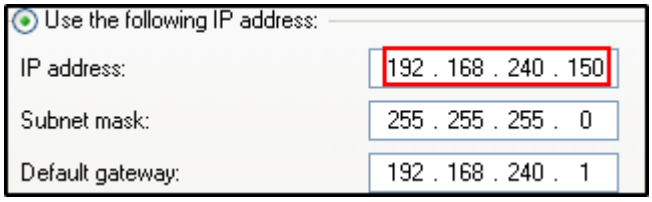
Kali

```
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
netmask 255.255.255.0
network 192.168.240.0
broadcast 192.168.240.255
gateway 192.168.240.1
```

Windows XP



Scansione nmap con Firewall disattivato

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.240.150 -o ./NoFirewallScan
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 14:57 CET
Nmap scan report for 192.168.240.150
Host is up (0.00021s 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 20.81 seconds
```

Scansione nmap con Firewall attivo

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.240.150 -o ./FirewallScan
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 15:00 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 3.11 seconds
```

Differenze

La differenza principale è che il firewall blocca le richieste di ping non permettendo ad nmap di capire se l'host è up o down

Possiamo saltare il ping con nmap usando il parametro -Pn

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -Pn -sV 192.168.240.150 -o ./FirewallScanPn
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 15:02 CET
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 222.69 seconds
```

In questo caso lo scan avviene ma tutte le porte risultano filtrate perchè non c'è nessuna risposta per via del firewall