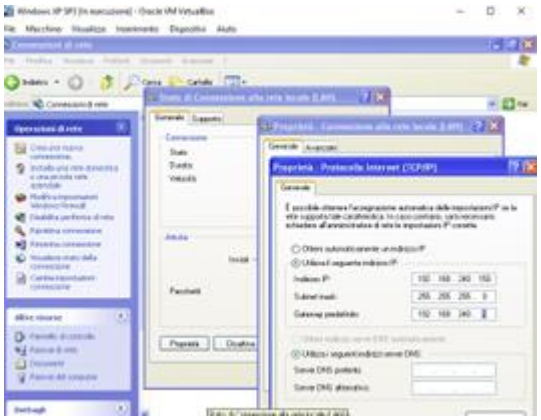
Traccia: Esercizio Le azioni preventive Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato. La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato. L'e sercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno.

Per prima cosa, soddisfiamo i requisiti del laboratorio, impostando gli IP delle macchine come richiesto.



Accertiamoci che il Firewall di Windows sia disattivato e lanciamo la scansione verso il nostro target con lo switch –sV. La scansione ci riporta 3 servizi in ascolto rispettivamente sulle porte TCP 135,139,445.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org )
Nmap scan report for 192.168.240.150
Host is up (0.68s 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 20.89 seconds
```

Attiviamo il Firewall di Windows XP e procediamo nuovamente alla scansione.

Attiviamo il Firewall di Windows XP e procediamo nuovamente alla scansione.

Il risultato della scansione indica che la macchina potrebbe essere spenta o, se è accesa, potrebbe bloccare l'host discovery di nmap. Il suggerimento è di usare il parametro –Pn per bypassare il ping. Sembra evidente che il firewall stia bloccando il traffico ICMP (ping). Procediamo quindi utilizzando lo switch –Pn per saltare il ping e andare direttamente alla scansione dei servizi.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org )
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 3.51 seconds
```

Utilizzando lo switch –Pn, la scansione bypassa il ping e procede direttamente alla scoperta dei servizi. Questa volta, tutte le porte sembrano essere filtrate, nel senso che non hanno risposto alle richieste dello scanner. È chiaro che il firewall sta bloccando l'accesso alle porte. Una porta è considerata filtrata quando lo scanner non riceve alcuna risposta; in questo caso, non possiamo determinare con certezza se una porta filtrata sia aperta o chiusa, anche se sappiamo che sulle porte 135, 139 e 445 ci sono servizi in ascolto.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.92 ( https://nmap.org )
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 215.00 seconds

┌──(kali㉿kali)-[~]
└─$
```

Il firewall di Windows XP sta effettivamente bloccando la scansione dei servizi attivi sulla macchina Windows XP dall'esterno. Siamo consapevoli che questi servizi sono vulnerabili, poiché li abbiamo sfruttati durante i test con Metasploit nella Unit 2. Pertanto, possiamo affermare che il firewall sta riducendo proattivamente i rischi di attacchi esterni, rendendo inaccessibili le porte 135, 139 e 445 TCP, su cui sono in ascolto i servizi.