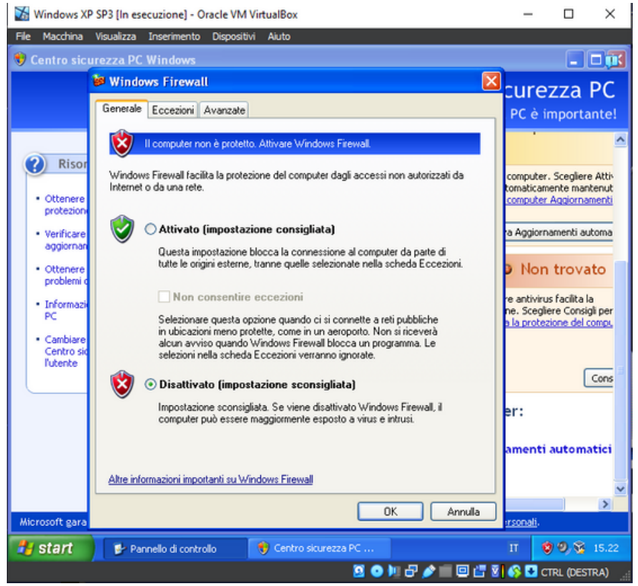
PRATICA S9/L1

Security Operation: azioni preventive

In questo esercizio andremo a testare le differenze tra una scansione con Nmap su Windows XP con firewall disattivato e una con il firewall attivo

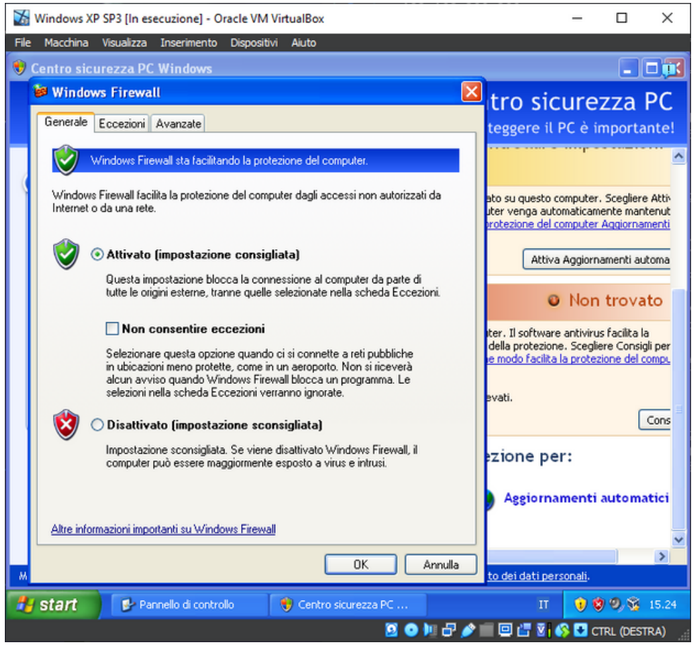
Come possiamo vedere il firewall di windows non è attivo. Eseguendo una scansione con Nmap possiamo notare come sia possibile individuare tutti i servizi attivi e la loro versione. Questo perchè il firewall è un componente di sicurezza informatica progettato per monitorare, filtrare e controllare il traffico di rete.




```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.200.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 09:23 EST
Nmap scan report for 192.168.200.200
Host is up (0.00031s 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 20.52 seconds
```

Attivando il firewall non è più possibile individuare tramite scansione di Nmap i servizi attivi sulla macchina, anche utilizando il comando -Pn che blocca l'invio del ping che funzionando tramite protocollo ICMP può creare problemi.
Si evince che utilizzare il firewall sia prezioso per garantire la sicurezza del sistema perchè funge da prima barriera contro potenziali attacchi.




```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.200.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 09:24 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 3.14 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sV 192.168.200.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 09:26 EST
Stats: 0:02:58 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 82.00% done; ETC: 09:30 (0:00:36 remaining)
Nmap scan report for 192.168.200.200
Host is up.
All 1000 scanned ports on 192.168.200.200 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 214.54 seconds
```