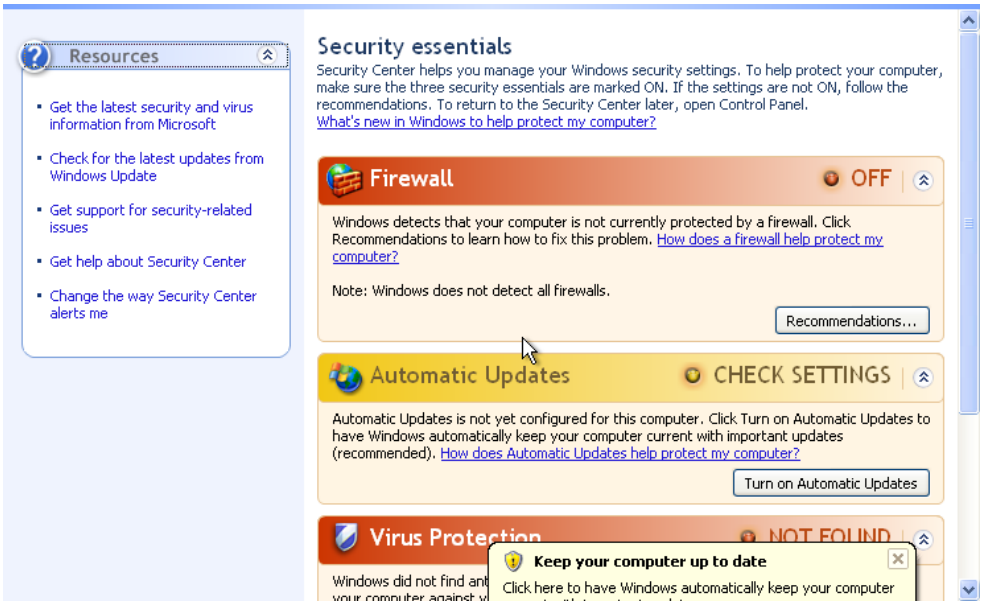
W18D1

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)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 14:30 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00038s latency).
Not shown: 997 closed tcp ports (reset)
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
MAC Address: 08:00:27:18:01:DA (Oracle VirtualBox virtual NIC)
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 20.69 seconds
```

3. Abilitare il Firewall sulla macchina Windows XP

4. Effetuata una seconda scansione con nmap, utilizzando ancora una volta lo switch -sV

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 14:32 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00037s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:18:01:DA (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.95 seconds
```

5. Trovare le eventuali differenze e motivarle.

La differenza tra la prima scansione e la seconda e dettata dal firewall. Quando il firewall spento tutte le porte e i loro relativi servizi sono esposti alla scansione da parte di nmap, contrariamente quando il firewall e attivo scherma tutto il sistema da scansioni esterne impedendo cosi la rivelazione di porte aperte, i servizi presenti su di esse (impedisce anche la scansione del OS della macchina bersaglio).