Traccia

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)

3. Abilitare il Firewall sulla macchina Windows XP

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

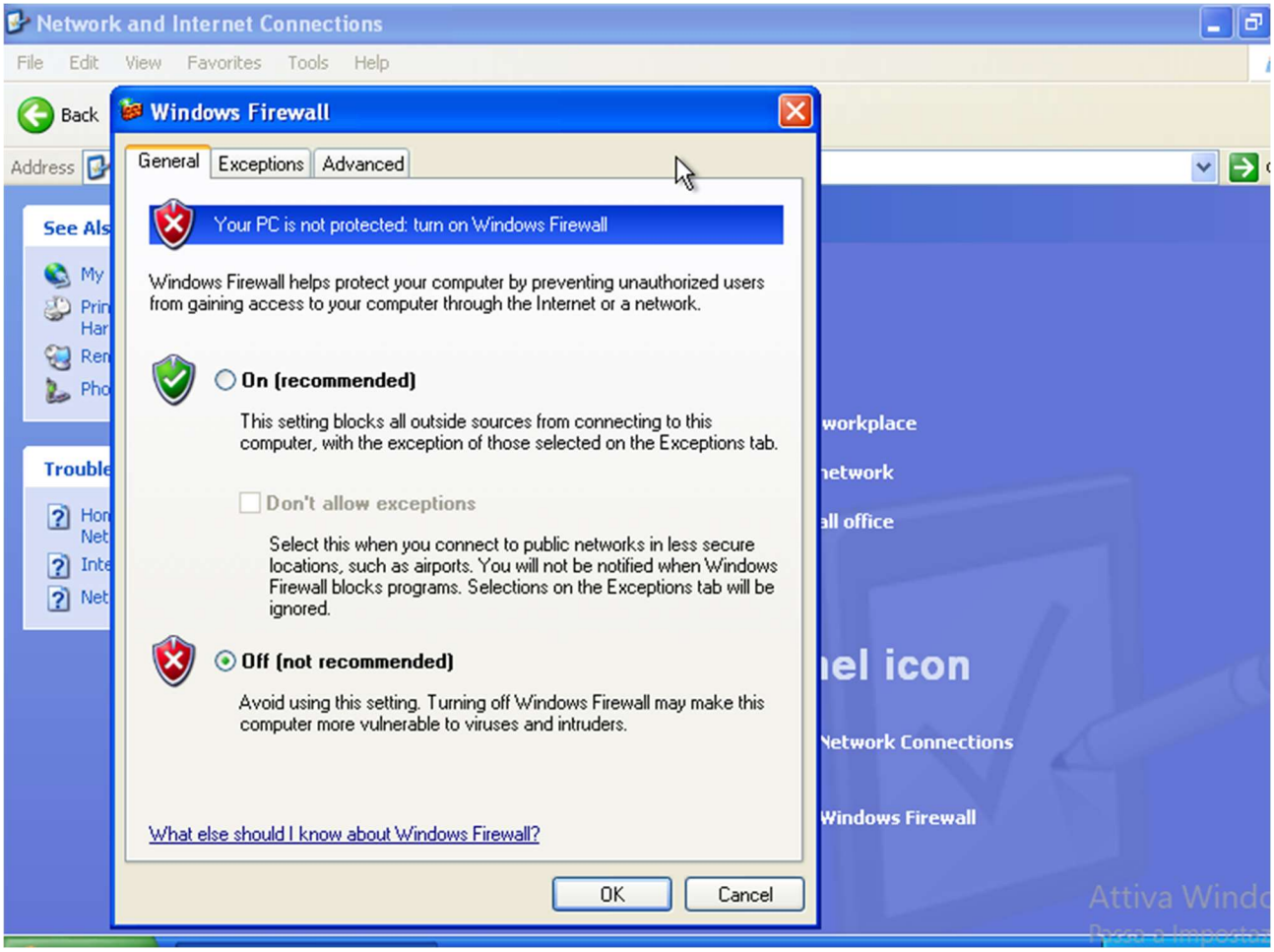
5. Trova le eventuali differenze e motivarle

Bonus:

Monitorare i log di Windows durante queste operazioni.

1. Quali log vengono modificati? (se vengono modificati)

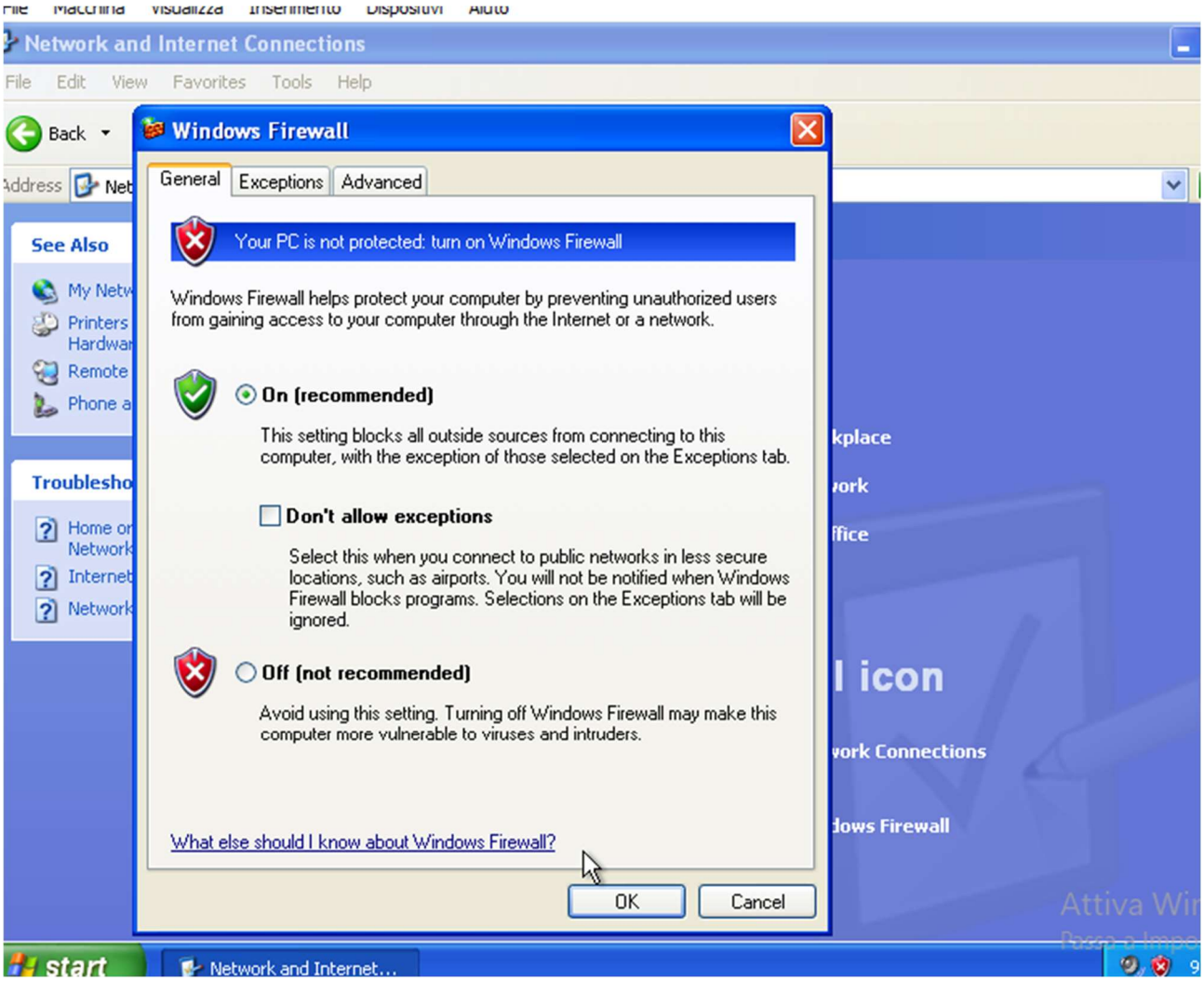
2. Cosa si riesce a trovare?



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.11.113
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-05 16:21 CET
Nmap scan report for 192.168.11.113
Host is up (0.0012s 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 21.32 seconds

┌──(kali㉿kali)-[~]
└─$
```

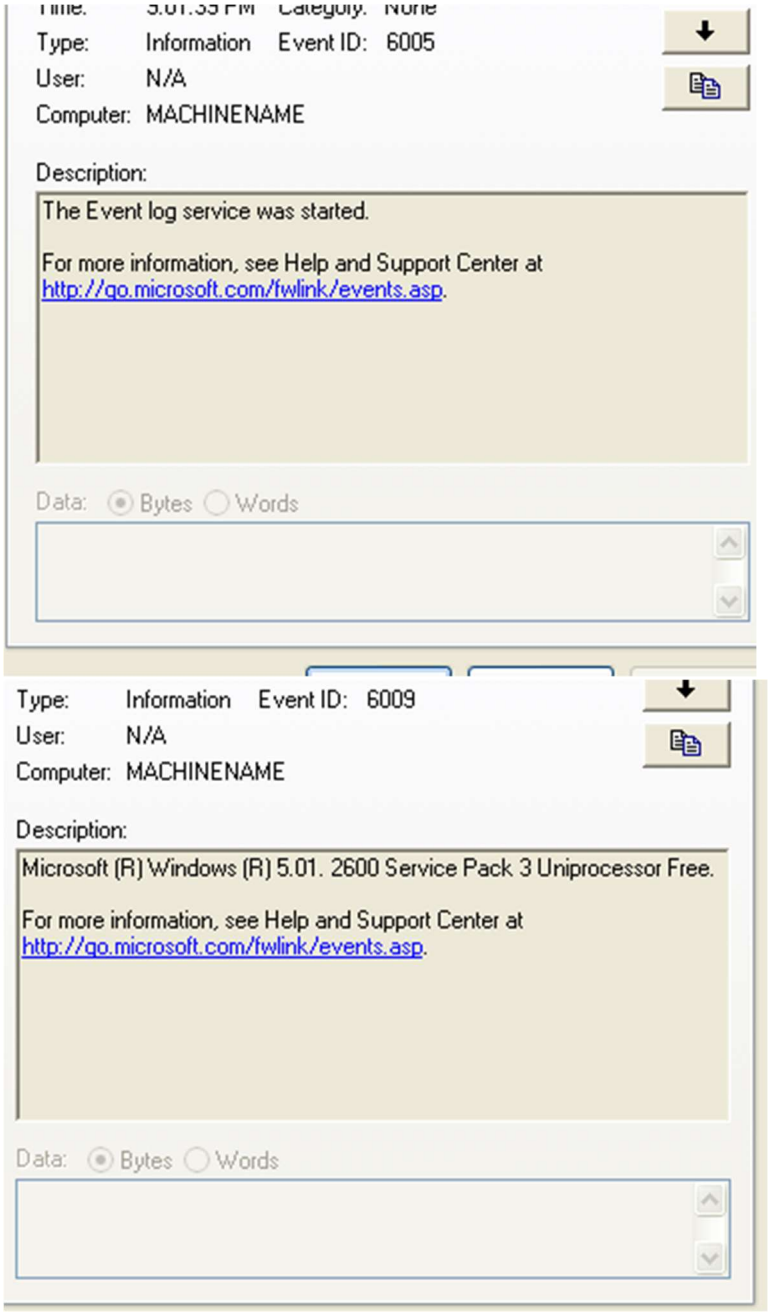



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.11.113
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-05 16:23 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.47 seconds

┌──(kali㉿kali)-[~]
└─$
```

Le differenze riguardano i servizi rilevati durante le scansioni. Con il Firewall disattivato, nmap rileva un numero maggiore di servizi e versioni. Con il Firewall attivato, i servizi sono nascosti o non raggiungibili, quindi nmap non riesce a rilevarli tutti o a identificarne le versioni correttamente.

Bonus



Nei log del Firewall di Windows, si potrebbero trovare voci relative alle connessioni bloccate o permessi concessi in base alle regole del Firewall. Nei log delle connessioni di rete, si potrebbero trovare informazioni sulle connessioni in entrata e in uscita durante le scansioni con nmap. Ciò potrebbe aiutare a capire meglio come il Firewall influisce sul traffico di rete e sulle operazioni di scansione.