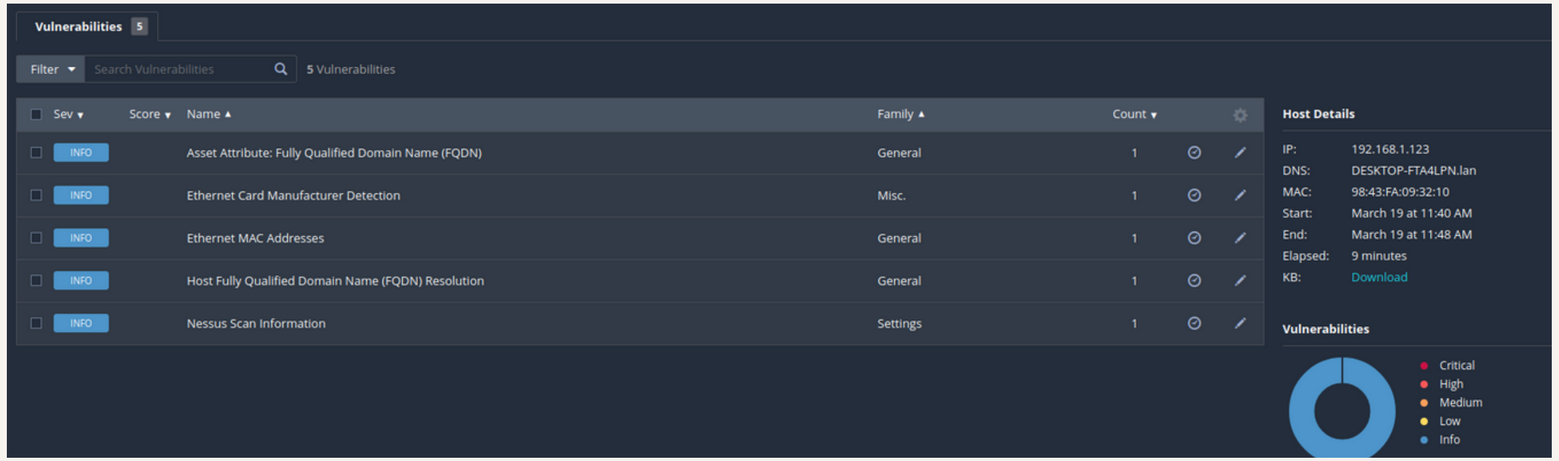
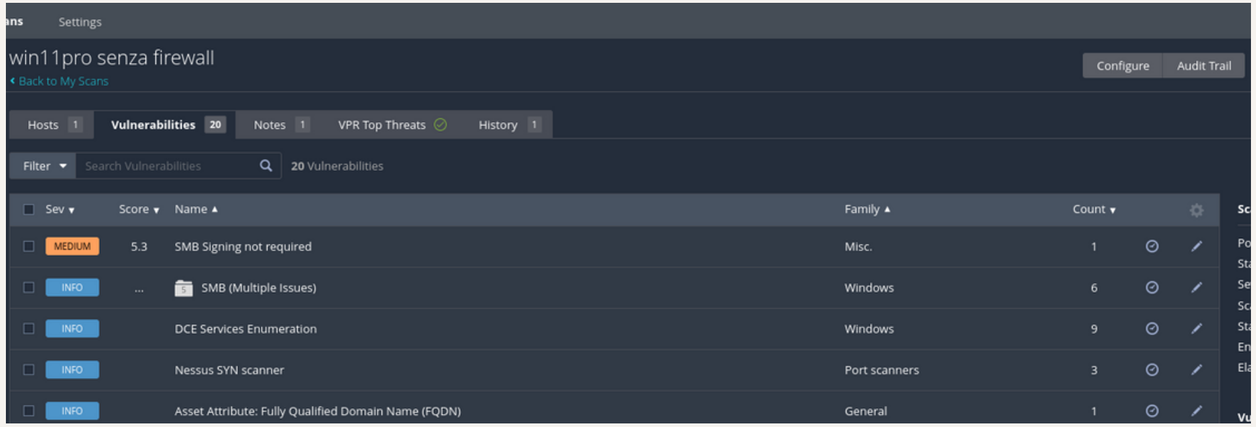
Security Operation: azioni preventive

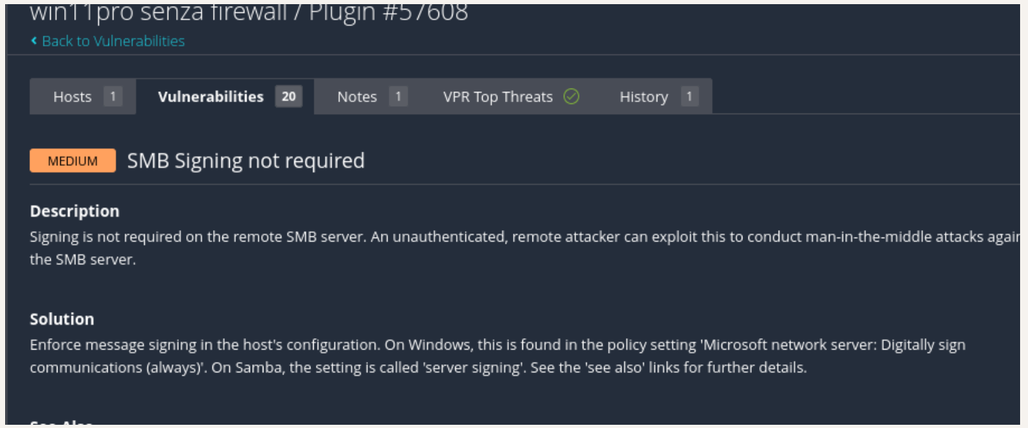
Ieri pomeriggio mi ero dilettato a mandare qualche scansione con Nessus sull'host di win11 dapprima col firewall attivo, poi disattivandolo.

Scansione con Nessus su host Win11 con Firewall attivo



Scansione con Nessus su host Win11 con Firewall disattivato: ho denotato la presenza di una vulnerabilità di crititcità media





Ho anche mandato una Scansione con nmap sull'host Win11 con firewall attivo

```
┌──(kali㉿kali)-[~]
└─$ nmap -v -A 192.168.1.123 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 08:09 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 08:09
Completed Parallel DNS resolution of 1 host. at 08:09, 0.00s elapsed
Initiating Connect Scan at 08:09
Scanning 192.168.1.123 [1000 ports]
Completed Connect Scan at 08:09, 5.86s elapsed (1000 total ports)
Initiating Service scan at 08:09
NSE: Script scanning 192.168.1.123.
Initiating NSE at 08:09
Completed NSE at 08:09, 5.00s elapsed
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Nmap scan report for 192.168.1.123
Host is up (0.049s latency).
All 1000 scanned ports on 192.168.1.123 are in ignored states.
Not shown: 990 filtered tcp ports (no-response), 10 filtered tcp ports (host-unreach)

NSE: Script Post-scanning.
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.40 seconds
```

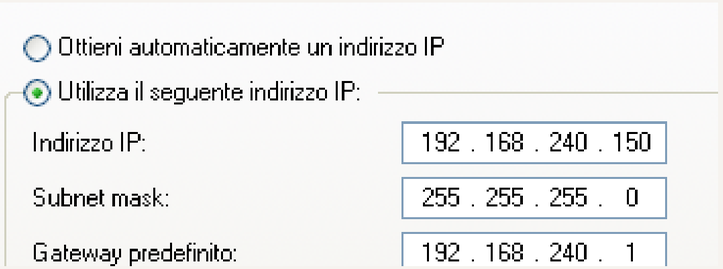
L'opzione -Pn è stata utilizzata per disabilitare la scansione del ping (altrimenti il firewall bloccava anche il ping), per forzare l' indirizzo IP target in "up".

Il risultato indica che l'host è "up", ma che tutte le 1000 porte TCP scansionate sono in stato "ignored", il che significa che non sono state né aperte né chiuse, ma sono state filtrate e non hanno dato risposta alla scansione.

Esercizio con WinXP

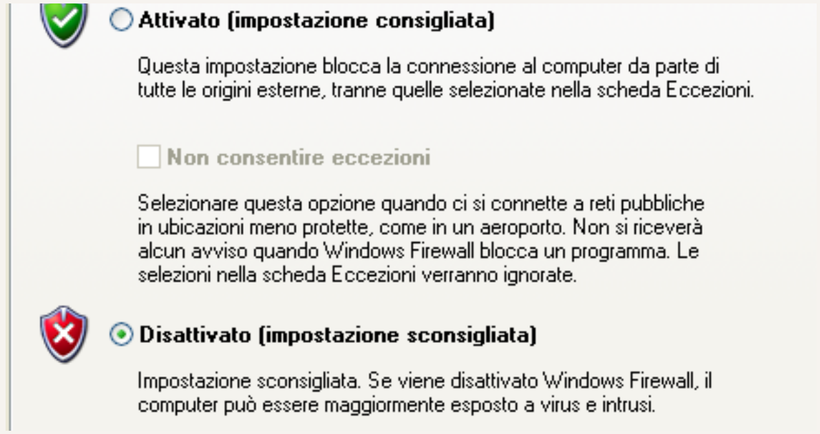
Ping delle macchine

```
# The loopback network interfac
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.100/24
gateway 192.168.240.1
```



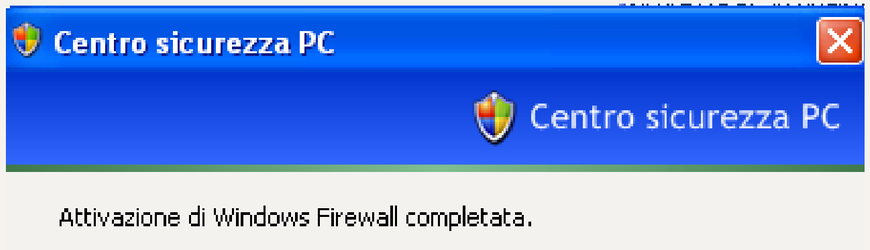

```
└─$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=1.54 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=2.42 ms
^C
── 192.168.240.150 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.535/1.975/2.415/0.440 ms
```

Ci assicuriamo che il firewall sulla macchina WinXP sia disattivo e mandiamo la prima scansione con nmap salvando l'output nel file "NOfirewall"




```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -oN NOfirewall
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 09:22 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0015s 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 20.61 seconds
```

Attivazione del firewall su WinXP



Mandiamo la seconda scansione con nmap su winXP col firewall attivo

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -oN SIfirewall
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 09:45 EDT
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 3.22 seconds
```

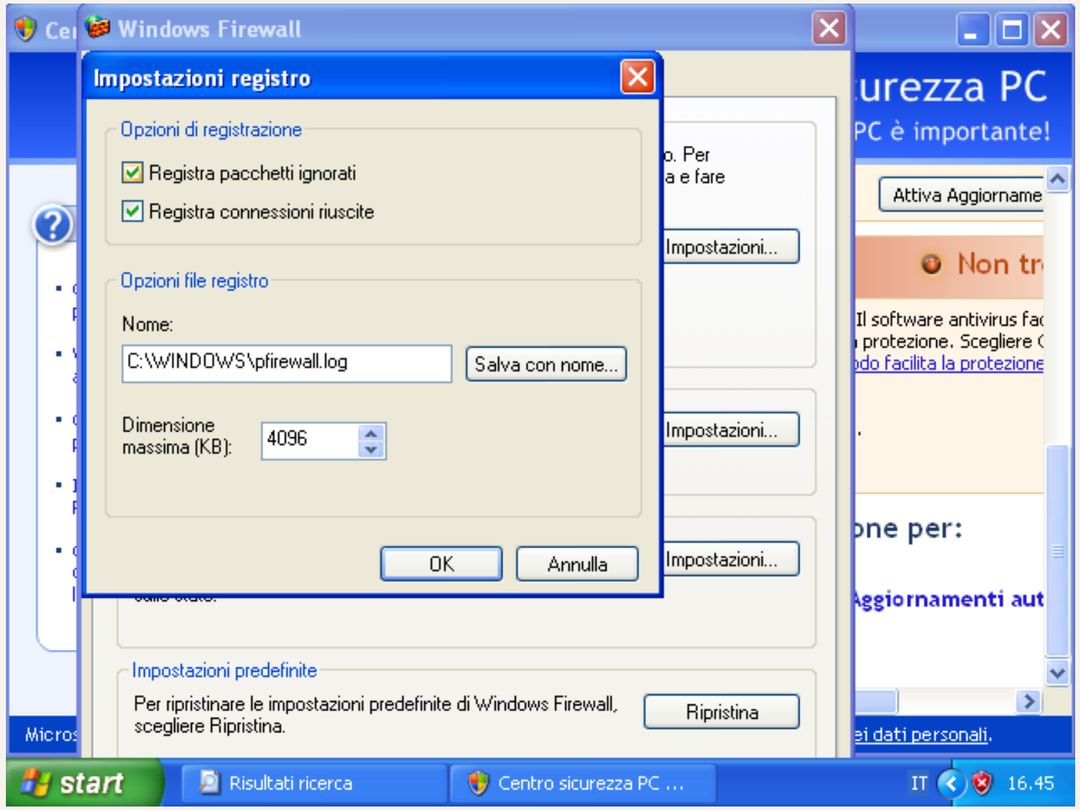
Di seguito la differenza tra gli output delle due scansioni:

```
┌──(kali㉿kali)-[~]
└─$ cat SIfirewall
# Nmap 7.93 scan initiated Mon Mar 20 09:45:23 2023 as: nmap -sV -oN SIfirewall 192.168.240.150
# Nmap done at Mon Mar 20 09:45:26 2023 -- 1 IP address (0 hosts up) scanned in 3.22 seconds

┌──(kali㉿kali)-[~]
└─$ cat NOfirewall
# Nmap 7.93 scan initiated Mon Mar 20 09:22:55 2023 as: nmap -sV -oN NOfirewall 192.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.0015s 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 at Mon Mar 20 09:23:15 2023 -- 1 IP address (1 host up) scanned in 20.61 seconds
```

- il file "**SIfirewall**" non contiene alcuna informazione utile, in quanto non è stato rilevato alcun host attivo.
- il file "**NOfirewall**" include una descrizione dettagliata dei servizi scoperti sulla macchina, ovvero: i numeri di porta aperti, gli stati dei servizi. le informazioni sulle versioni, la rilevazione dell'host, il tempo di latenza e le informazioni sul sistema operativo.

Ciò suggerisce che il firewall potrebbe essere attivo sulla macchina, impedendo a Nmap di rilevare l'host e la sua configurazione.

Per trovare i cambiamenti nei log è necessario anzitutto cambiare le impostazioni del registro spuntando la registrazione dei pacchetti ignorati e delle connessioni riuscite



Dopo aver avviato la scansione con Nmap i log verranno salvati sul file "pfirewall" nella directory Windows