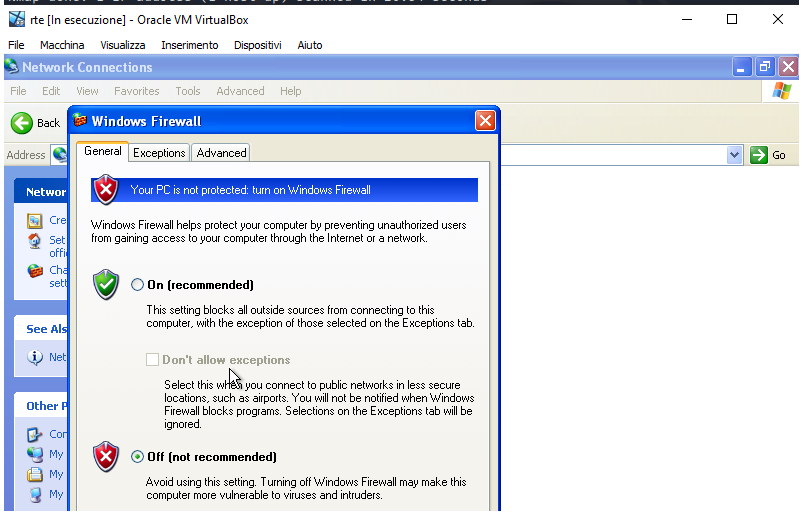
Security Operation

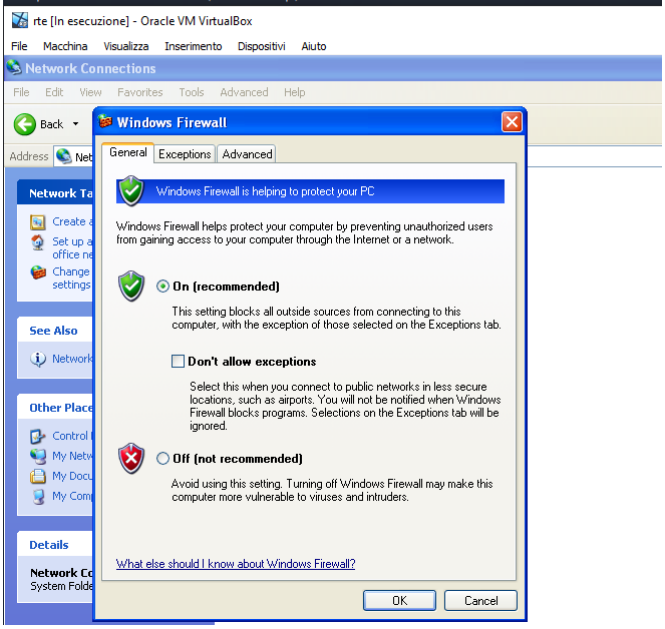
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.240.150 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 11:02 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00018s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft 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 20.54 seconds
```



Disattivando il servizio di Firewall sulla macchina Windows XP abbiamo la possibilità di eseguire una scansione nmap intrusiva come quella del service detection senza essere bloccati o rilevati in alcun modo dal sistema vittima.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.240.150 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 11:03 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 3.23 seconds
```



Riattivando il firewall possiamo notare come la nostra scansione non ha avuto alcun risultato rilevante facendo sembrare la macchina Windows XP spenta.
Quindi il firewall oltre a questo scrive anche nel firewall log informazioni sul tentativo di enumerazione delle porte.

Resoconto log:

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack t

2023-03-20 17:09:01 DROP TCP 192.168.240.100 192.168.240.150 44676 80 60 S 2074903747 0 64240 -
2023-03-20 17:09:01 DROP TCP 192.168.240.100 192.168.240.150 59216 443 60 S 3532713994 0 64240 -
2023-03-20 17:09:03 DROP TCP 192.168.240.100 192.168.240.150 54322 443 60 S 3090834495 0 64240 -
2023-03-20 17:09:03 DROP TCP 192.168.240.100 192.168.240.150 46590 80 60 S 47483243 0 64240 - -
```