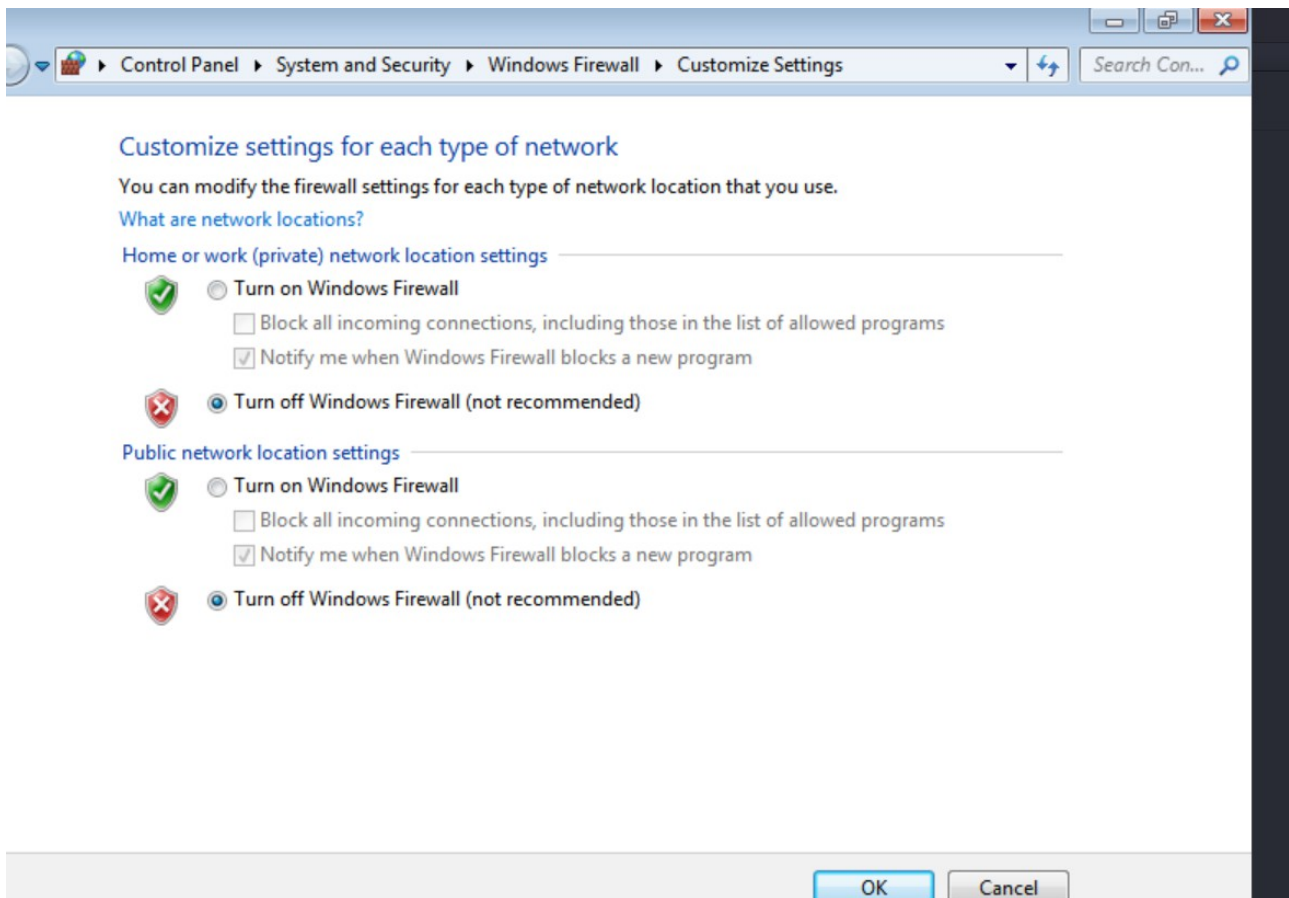


W18D1

1 - Firewall disattivato su windows 7



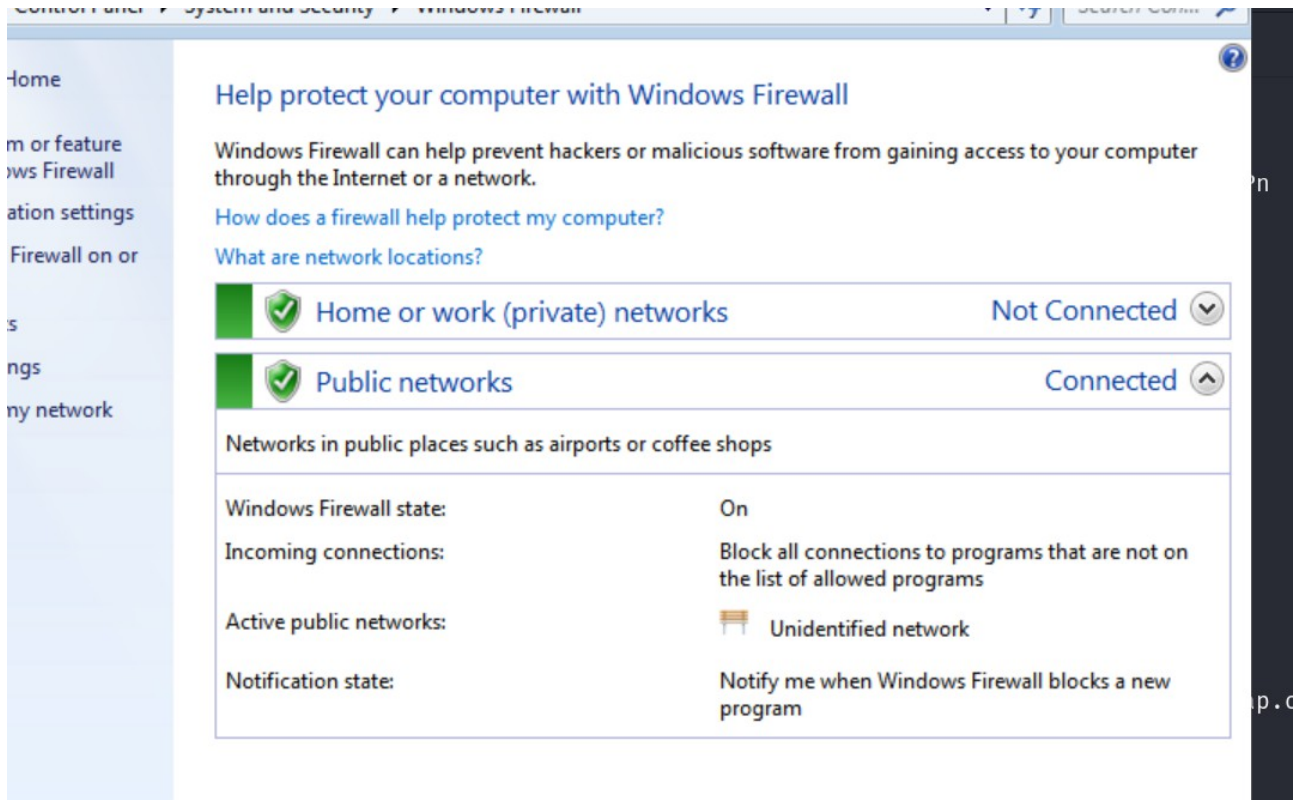
2-Scansione con Nmap -sV -O

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)~[~/Desktop]
$ sudo nmap -sV -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 13:24 EDT
Stats: 0:00:40 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 13:26 (0:00:52 remaining)
Nmap scan report for 192.168.50.102
Host is up (0.00099s latency).
Not shown: 991 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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc          Microsoft Windows RPC
49153/tcp  open  msrpc          Microsoft Windows RPC
49154/tcp  open  msrpc          Microsoft Windows RPC
49155/tcp  open  msrpc          Microsoft Windows RPC
49156/tcp  open  msrpc          Microsoft Windows RPC
49157/tcp  open  msrpc          Microsoft Windows RPC
MAC Address: 08:00:27:F8:BB:04 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.50 seconds

(kali@kali)~[~/Desktop]
$
```

3 - Attivazione firewall su windows 7



4 - Scansione Nmap -sV -p

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 13:18 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 3.37 seconds

(kali@kali)-[~/Desktop]
$ nmap -sV -Pn- 192.168.50.102
Unknown -P option -Pn-.
QUITTING!

(kali@kali)-[~/Desktop]
$ nmap -sV -Pn 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 13:19 EDT
Stats: 0:02:58 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 82.00% done; ETC: 13:22 (0:00:36 remaining)
Nmap scan report for 192.168.50.102
Host is up.
All 1000 scanned ports on 192.168.50.102 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 214.69 seconds

(kali@kali)-[~/Desktop]
$
```

Si può notare come il Firewall stia bloccando la scansione di Nmap. Di conseguenza possiamo dire che il Firewall sta riducendo i rischi da possibili attacchi esterni. Rendendo inaccessibili informazioni fondamentali per eventuali attacchi.