

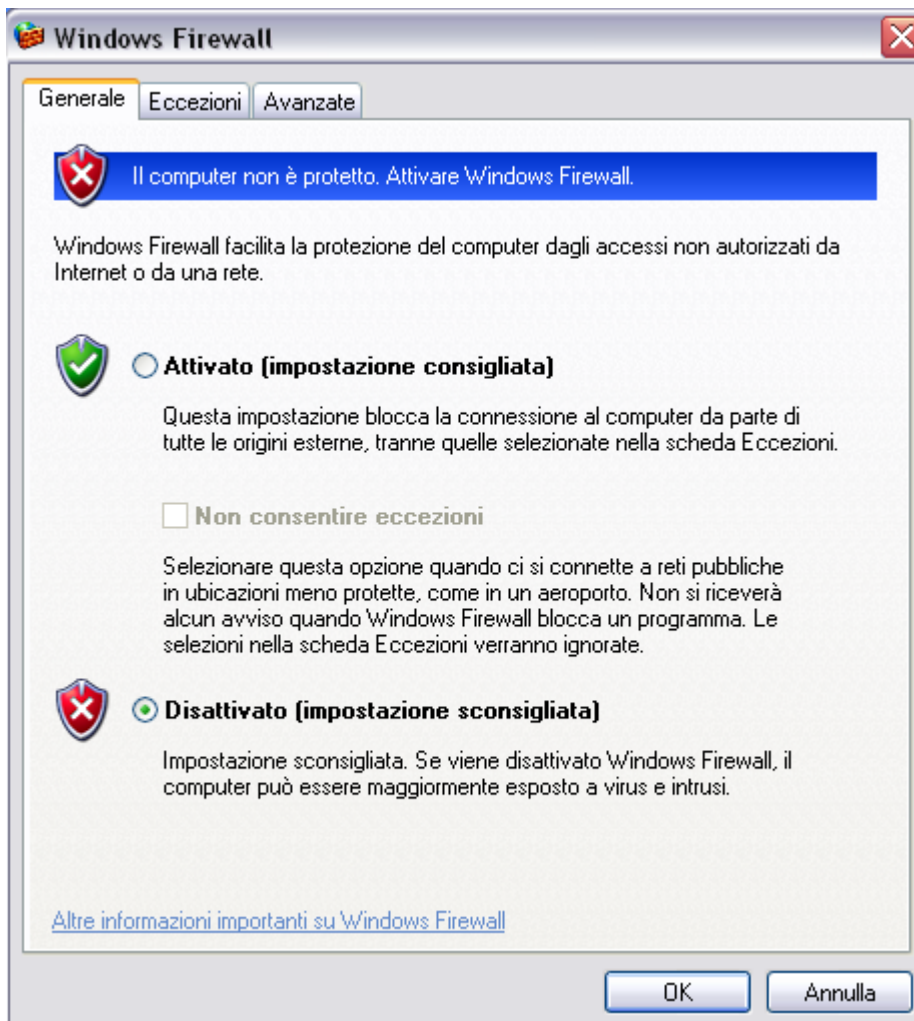
## CONSEGNA U3 S9 L1

Prima di eseguire l'esercizio ho settato correttamente gli indirizzi IP sulle macchine Kali e XP. Poi ho eseguito il **ping** da entrambe per verificare che la connessione fosse attiva e funzionante.

```
(kali㉿kali)-[~]  
$ ping -c3 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=7.58 ms  
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1.41 ms  
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.35 ms  
  
— 192.168.240.150 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2002ms  
rtt min/avg/max/mdev = 1.346/3.444/7.581/2.925 ms
```

```
C:\Documents and Settings\Administrator>ping 192.168.240.100  
Esecuzione di Ping 192.168.240.100 con 32 byte di dati:  
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64  
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64  
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64  
  
Statistiche Ping per 192.168.240.100:  
Pacchetti: Trasmessi = 3, Ricevuti = 3, Persi = 0 (0% persi),  
Tempo approssimativo percorsi andata/ritorno in millisecondi:  
Minimo = 0ms, Massimo = 1ms, Medio = 0ms
```

Poi sulla macchina Windows XP ho disattivato il firewall.



Avvio la scansione di **nmap** con lo switch **-sV** all'indirizzo di XP **192.168.240.150**. con lo switch **-o** dico a **nmap** di salvare l'output della scansione in un file di testo nominato **ReportXP.txt**. Si nota che ci sono diverse porte aperte e vari servizi attivi sulle stesse. Poi col comando **cat** visualizzo a schermo il file di report.

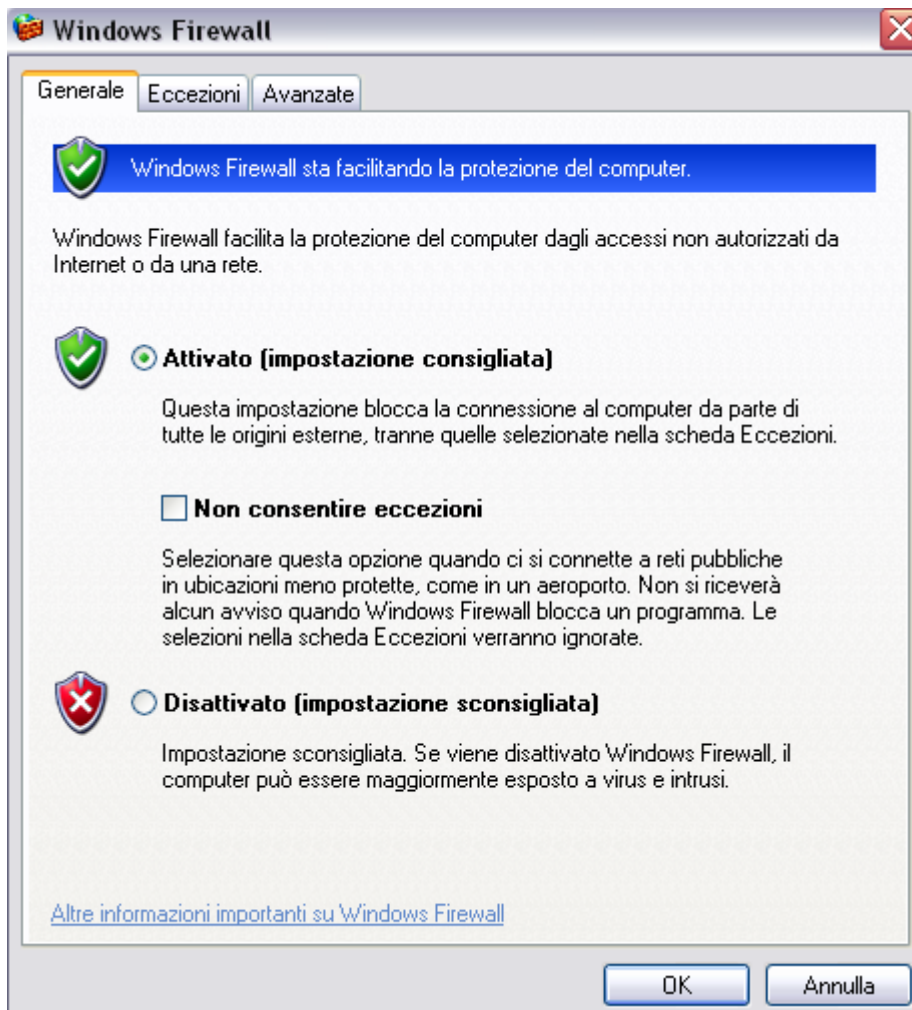
```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o ReportXP.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 14:11 CEST
Nmap scan report for 192.168.240.150
Host is up (0.0025s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        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:window

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.79 seconds

(kali㉿kali)-[~]
$ cat ReportXP.txt
# Nmap 7.94SVN scan initiated Mon Jul 22 14:11:57 2024 as: nmap -sV -o ReportXP.txt 192.168.24
Nmap scan report for 192.168.240.150
Host is up (0.0025s 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:window

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jul 22 14:12:04 2024 -- 1 IP address (1 host up) scanned in 6.79 seconds
```

Adesso attivo il firewall di XP e ripeto la scansione.



Effettuo nuovamente la scansione con **nmap** da Kali. In questa scansione con il firewall abilitato sulla macchina. Creo un nuovo file di report dove salvare le informazioni della scansione chiamato **Report\_FW\_XP.txt**. Tra l'altro **nmap** adesso necessita dello switch **-Pn** affinché la scansione vada a buon fine. Alla fine visualizzo a schermo il file di report.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o Report_FW_XP.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 14:17 CEST
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 3.11 seconds

(kali㉿kali)-[~]
$ nmap -Pn -sV 192.168.240.150 -o Report_FW_XP.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 14:17 CEST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.50% done
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 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/ .
CPU usage: 0.7% address (1 host up) scanned in 201.77 seconds

(kali㉿kali)-[~]
$ cat Report_FW_XP.txt
# Nmap 7.94SVN scan initiated Mon Jul 22 14:17:50 2024 as: nmap -Pn -sV -o Report_FW_XP.txt 19
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 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 at Mon Jul 22 14:21:12 2024 -- 1 IP address (1 host up) scanned in 201.77 seconds
```

Provo poi ad effettuare un'altra scansione più completa con lo switch **-A** per vedere se cambia il risultato e salvo il risultato all'interno del file **Report\_FW\_2\_XP.txt** che successivamente visualizzo sul terminale. Come nella scansione precedente non riesce a trovare nulla.

```
(kali@kali)-[~]
$ nmap -Pn -A 192.168.240.150 -o Report_FW_2_XP.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 15:22 CEST
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 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 206.91 seconds

(kali@kali)-[~]
$ cat Report_FW_2_XP.txt
# Nmap 7.94SVN scan initiated Mon Jul 22 15:22:27 2024 as: nmap -Pn -A -o Report_FW_2_XP.txt 1
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 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 at Mon Jul 22 15:25:54 2024 -- 1 IP address (1 host up) scanned in 206.91 seconds
```

Provando ad effettuare la scansione con lo switch -O si riesce, anche a firewall attivo, ad ottenere informazioni sul sistema operativo della macchina target. (In questo caso Windows XP SP2)

```
(kali@kali)-[~]  
$ sudo nmap -Pn -O 192.168.240.150 -o Report_FW_3_XP.txt  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 17:39 CEST  
Nmap scan report for 192.168.240.150  
Host is up (0.0012s latency).  
All 1000 scanned ports on 192.168.240.150 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 08:00:27:2C:4C:74 (Oracle VirtualBox virtual NIC)  
Device type: specialized|general purpose  
Running: AKCP embedded, General Dynamics embedded, Microsoft Windows 2000|2003|XP  
OS CPE: cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_server_2003 cpe:/o:microsoft:windows_xp::sp2  
Too many fingerprints match this host to give specific OS details  
Network Distance: 1 hop  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 22.48 seconds
```

Verifico con **wireshark** il traffico di rete, mi accorgo che con il firewall attivo sulla macchina Windows, molte delle trasmissioni avviate da **nmap** per la verifica dei servizi attivi sulle porte vengono rifiutate per motivi di sicurezza. (le righe evidenziate in rosso)

Source	Destination	Protocol	Length	Info
192.168.240.100	192.168.240.150	TCP	74	44550 → 1025 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T...
192.168.240.100	192.168.240.150	TCP	74	54984 → 5900 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T...
192.168.240.100	192.168.240.150	TCP	74	44558 → 1720 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T...
192.168.240.100	192.168.240.150	TCP	74	43632 → 110 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS...
192.168.240.100	192.168.240.150	TCP	74	38884 → 587 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS...
192.168.240.100	192.168.240.150	TCP	74	55812 → 22 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSv...
192.168.240.100	192.168.240.150	TCP	74	33306 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS...
192.168.240.100	192.168.240.150	TCP	74	35216 → 995 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS...
192.168.240.100	192.168.240.150	TCP	74	58826 → 1723 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T...
192.168.240.100	192.168.240.150	TCP	74	44678 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS...
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 44678 → 445 [SYN] Seq=0 Win=32120 Len=0 ...
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 58826 → 1723 [SYN] Seq=0 Win=32120 Len=0...
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 35216 → 995 [SYN] Seq=0 Win=32120 Len=0 ...
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 33306 → 443 [SYN] Seq=0 Win=32120 Len=0 ...
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 55812 → 22 [SYN] Seq=0 Win=32120 Len=0 M...
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 38884 → 587 [SYN] Seq=0 Win=32120 Len=0 ...
192.168.240.100	192.168.240.150	TCP	74	44686 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS...
192.168.240.100	192.168.240.150	TCP	74	58826 → 1723 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T...

Source	Destination	Protocol	Length	Info
192.168.240.100	192.168.240.150	TCP	74	59840 → 7025 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T...
192.168.240.100	192.168.240.150	TCP	74	50244 → 646 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS...
192.168.240.100	192.168.240.150	TCP	74	54422 → 1066 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T...
192.168.240.100	192.168.240.150	TCP	74	46978 → 1081 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T...
192.168.240.100	192.168.240.150	TCP	74	50954 → 999 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS...
192.168.240.100	192.168.240.150	TCP	74	40996 → 15660 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM ...
192.168.240.100	192.168.240.150	TCP	74	51006 → 30718 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM ...
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 45052 → 5925 [SYN] Seq=0 Win=32120 Len=0...
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 50684 → 5051 [SYN] Seq=0 Win=32120 Len=0...
192.168.240.100	192.168.240.150	TCP	74	50684 → 5051 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS...

## Conclusioni

Nonostante le porte con servizi attivi sulla rete, quando il firewall sulla macchina Windows è disattivato siano poche, comunque l'aver attivato il firewall protegge notevolmente di più la macchina da attacchi esterni. Inoltre, si dà il caso che sulle macchine più obsolete, come per esempio Windows /, Vista, XP, quelle poche porte aperte possono permettere a qualche malintenzionato di sfruttare delle vulnerabilità che permettono di avere accesso e pieno controllo sulla macchina target.