ESERCIZIO M5 D3

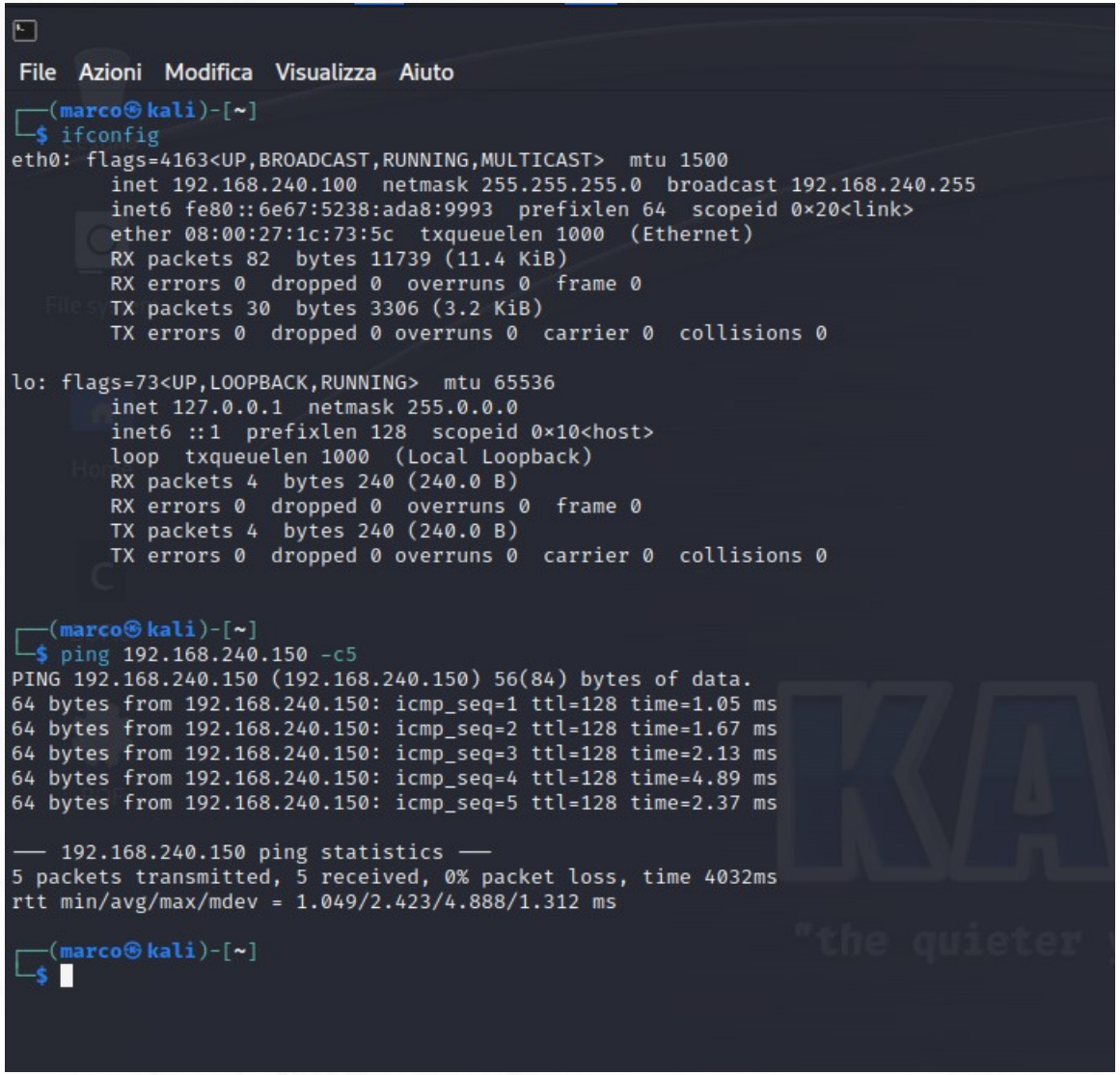
SECURITY OPERATION: AZIONI PREVENTIVE

MESSA A PUNTO LABORATORIO

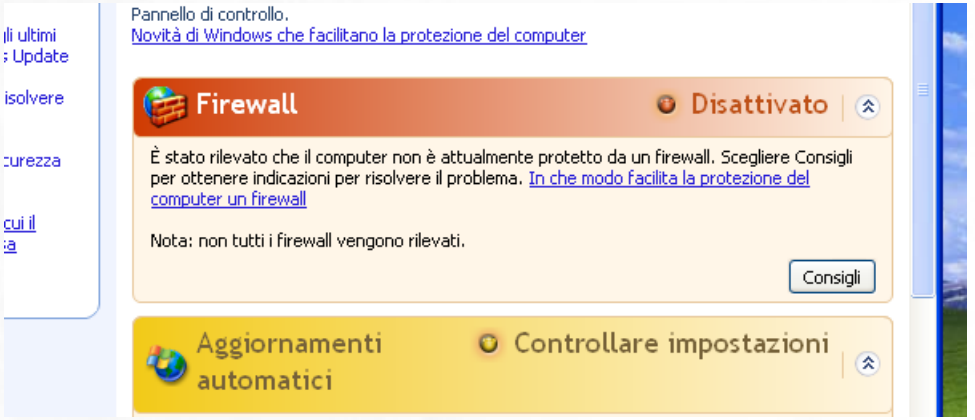
KALI 192.168.240.100

WIN XP 192.168.240.150

TEST DI PING



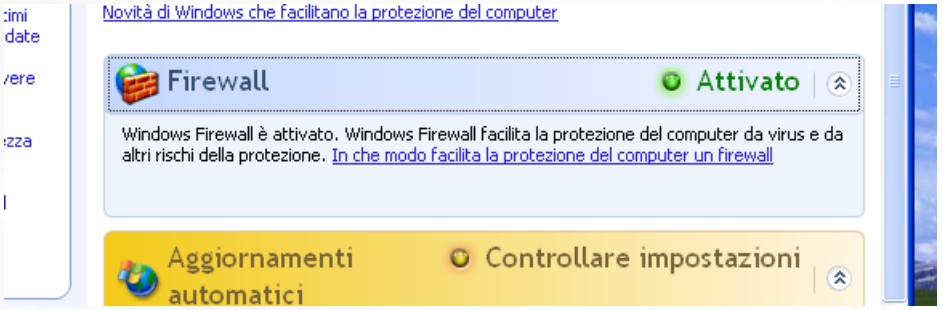
LA MACCHINA WINDOWS XP HA DI DEFAULT IL FIREWALL DISATTIVATO (COME DA IMMAGINE A FIANCO); DI SEGUITO IL RISULTATO DELLA SCANSIONE NMAP (IN BASSO) CHE RIVELA 3 PORTE APERTE CHE POTREBBERO ESSERE VULNERABILI.




```
┌──(marco㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-19 16:08 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00041s 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 21.00 seconds
```

UNA VOLTA ATTIVATO IL FIREWALL SULLA MACCHINA XP SI Può NORATE DALLA SCANSIONE NMAP CHE LE PORTE RISULTANO FILTRATE E QUINDI L'ACCESSO DIVENTA ASSAI ARDUO (SI POTREBBERO VALUTARE STRATEGIE DI AGGIRAMENTO DEL FIREWALL PROBABILMENTE)




```
┌──(marco㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-19 16:17 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 3.21 seconds

┌──(marco㉿kali)-[~]
└─$

┌──(marco㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-21 15:11 CEST
Stats: 0:01:30 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 37.50% done; ETC: 15:14 (0:02:08 remaining)
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 216.76 seconds

┌──(marco㉿kali)-[~]
└─$
```