

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

```
File Azioni Modifica Visualizza Aiuto
(marco@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255
    inet6 fe80::6e67:5238:ada8:9993 prefixlen 64 scopeid 0<link>
    ether 08:00:27:1c:73:5c txqueuelen 1000 (Ethernet)
    RX packets 82 bytes 11739 (11.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30 bytes 3306 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

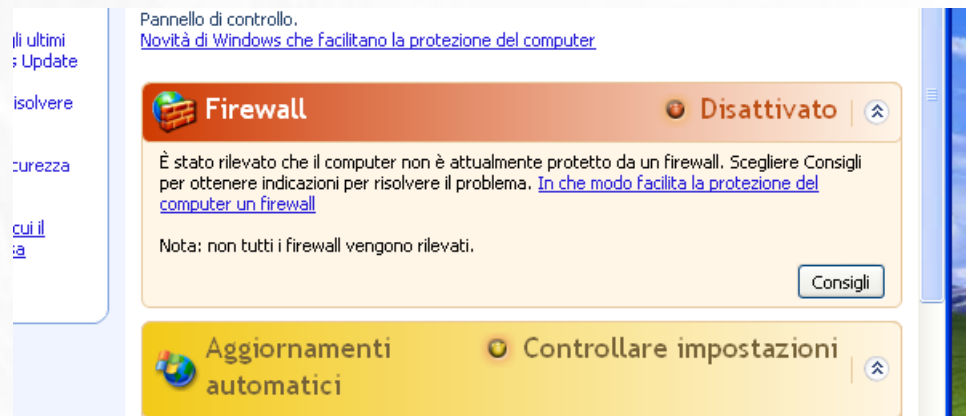
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(marco@kali)-[~]
$ ping 192.168.240.150 -c5
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=1.05 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1.67 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=2.13 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=4.89 ms
64 bytes from 192.168.240.150: icmp_seq=5 ttl=128 time=2.37 ms

— 192.168.240.150 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4032ms
rtt min/avg/max/mdev = 1.049/2.423/4.888/1.312 ms

(marco@kali)-[~]
$
```

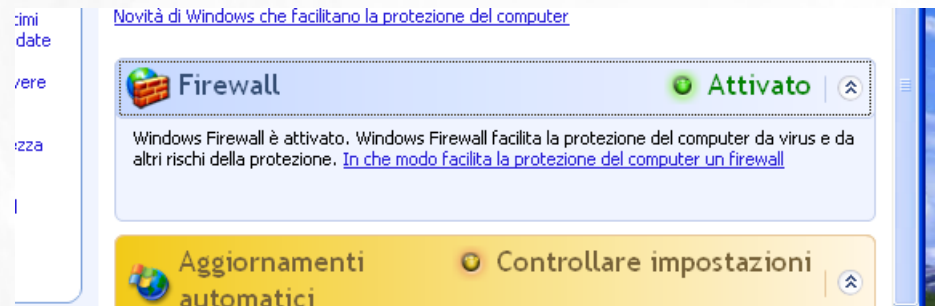
LA MACCHINA WINDOWS XP
HA DI DEFAULT IL FIREWALL
DISATTIVATO (COME DA
IMMAGINE A FIANCO); DI
SEGUITO IL RISULTATO DELLA
SCANSIONE NMAP (IN BASSO)
CHE RIVELA 3 PORTE APERTE
CHE POTREBBERO ESSERE
VULNERABILI.



```
(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 NOTARE 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)-[~]
$
```