

SCANSIONE NMAP SU WINDOWS XP

```
File Actions Edit View Help
(kali㉿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::a00:27ff:feb6:96ed prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b6:96:ed txqueuelen 1000 (Ethernet)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 2424 (2.3 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 0x10<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

(kali㉿kali)-[~]
$ ping 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=2.85 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1.33 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.27 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=1.29 ms
^C
— 192.168.240.150 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 1.267/1.685/2.854/0.675 ms

(kali㉿kali)-[~]
$ nmap -sV -o report_prima_scansione 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 12:33 CET
Nmap scan report for 192.168.240.150
Host is up (0.065s 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 20.11 seconds
```

Dopo aver modificato l'IP della macchina Windows Xp con l'IP 192.168.240.150 e disattivato il Firewall e dopo aver modificato l'IP della macchina Kali con IP 192.168.240.100 è stata avviata la scansione con Nmap -sV sono stati trovati le seguenti porte aperte:

- 135 / TCP
- 139 / TCP
- 445 / TCP

```
(kali@kali)-[~]  
$ nmap -sV -o report_seconda_scansione 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 12:55 CET  
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 3.18 seconds  
  
(kali@kali)-[~]  
$
```

Dopo aver modificato l'IP della macchina Windows Xp con l'IP 192.168.240.150 e attivato il Firewall e quella della macchina di Kali IP 192.168.240.100 è stata avviata una seconda scansione con Nmap -sV e questa volta non è stata trovata nessuna porta aperta;

ANALISI DOPO LE DUE SCANSIONI NMAP -sV

Differenze evidenti:

Numero di porte aperte:

Prima scansione: 3 porte aperte

Seconda scansione: 0 porte aperte

Servizi accessibili:

Prima scansione:

HTTP (80/tcp)

NetBIOS (139/tcp)

Microsoft-DS (445/tcp)

Seconda scansione

Nessuna porta rilevata aperta in quanto il Firewall blocca la scansione;

MOTIVAZIONI

Il firewall di Windows XP blocca l'accesso alle porte non espressamente autorizzate.

Le altre porte, come 139 (NetBIOS) e 445 (Microsoft-DS), sono bloccate dal firewall.

Il firewall di Windows XP è efficace nel limitare l'accesso alle porte e ai servizi sulla macchina.

Disattivare il firewall rende la macchina più vulnerabile ad attacchi informatici.

È importante configurare il firewall correttamente per consentire solo l'accesso ai servizi necessari.