

S9-L1

Come vedremo dalla prossima slide le principali differenze sono sostanzialmente che con il firewall attivato riesco ad ottenere poche informazioni riguardo alla macchina xp. Mentre se disattiviamo il firewall possiamo vedere informazioni fondamentali come: le porte aperte e i servizi attivi con le loro versioni, inoltre possiamo anche vedere il sistema operativo e le sue informazioni correlate.

File Actions Edit View Help

Nmap done: 1 IP address (1 host up) scanned in 25.20 seconds

**(root@kali)-[/home/kali]**

# nmap -sV 192.168.50.103

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-04-22 14:28 CEST

Nmap scan report for 192.168.50.103

Host is up (0.0016s latency).

All 1000 scanned ports on 192.168.50.103 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 45.68 seconds

**(root@kali)-[/home/kali]**

# nmap -sV 192.168.50.103

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-04-22 14:29 CEST

Nmap scan report for 192.168.50.103

Host is up (0.0020s latency).

Not shown: 997 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 XP microsoft-ds
---------	------	--------------	-----------------------------------

MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)

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 21.16 seconds

**(root@kali)-[/home/kali]**

#