S5L2

Report

Questo report documenta le scansioni effettuate con Nmap sui target Metasploitable e Windows. Le scansioni includono l'identificazione del sistema operativo, la rilevazione delle porte aperte e dei servizi attivi con le relative versioni.

Target: Metasploitable

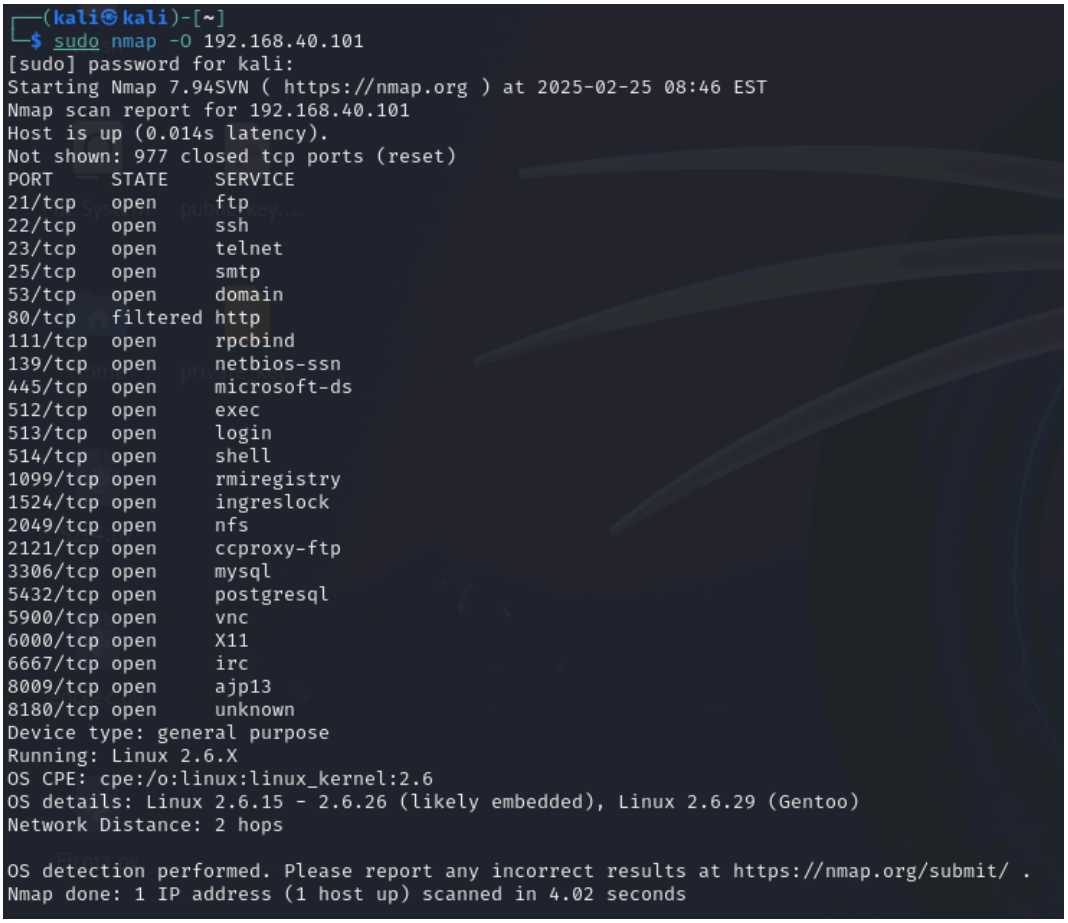
IP Target: 192.168.40.101

Sistema Operativo Rilevato: Linux 2.6.15 - 2.6.26 - 2.6.29

Scansioni Eseguite:

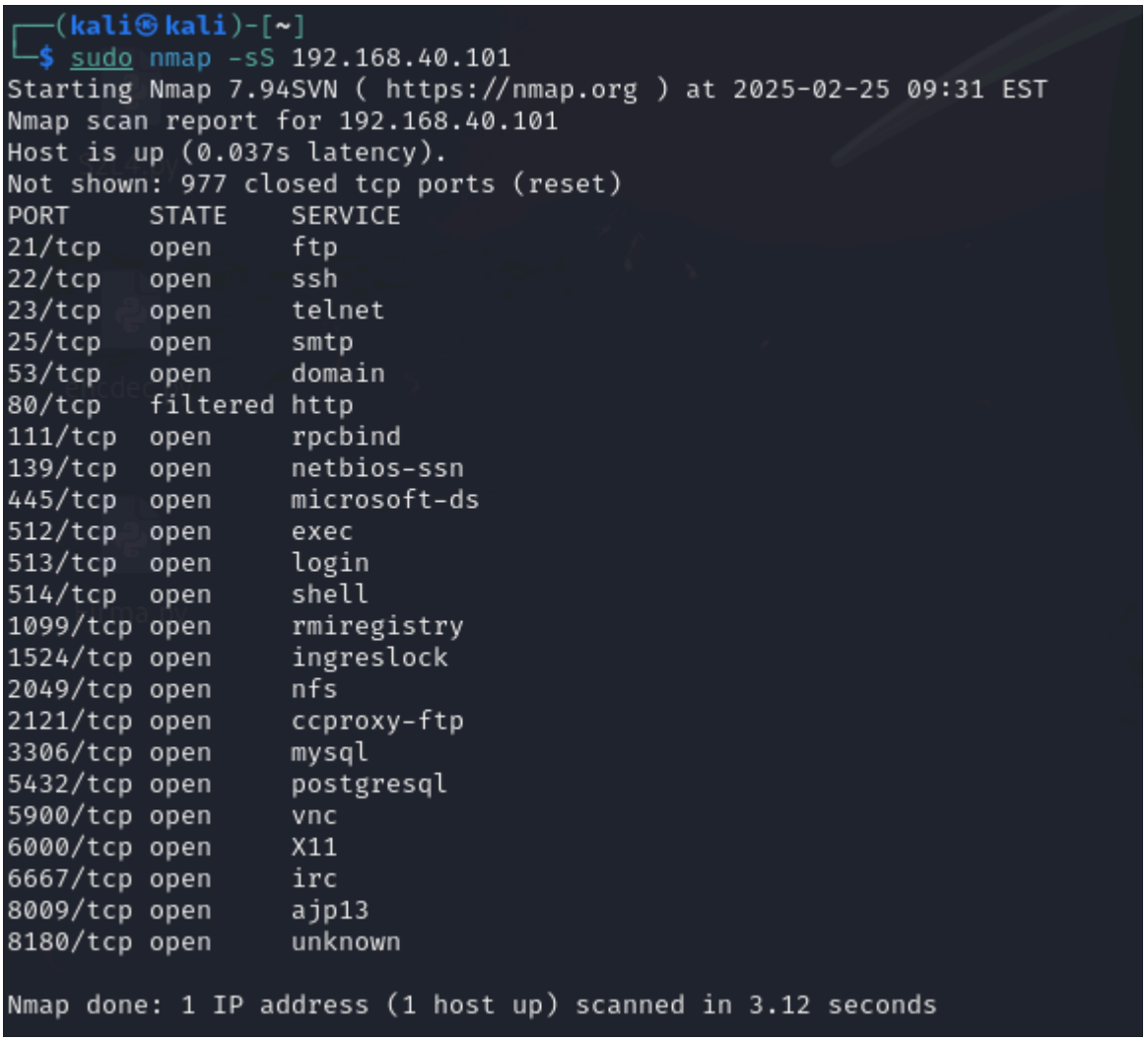
OS Fingerprint:

Comando: sudo nmap -O 192.168.40.101



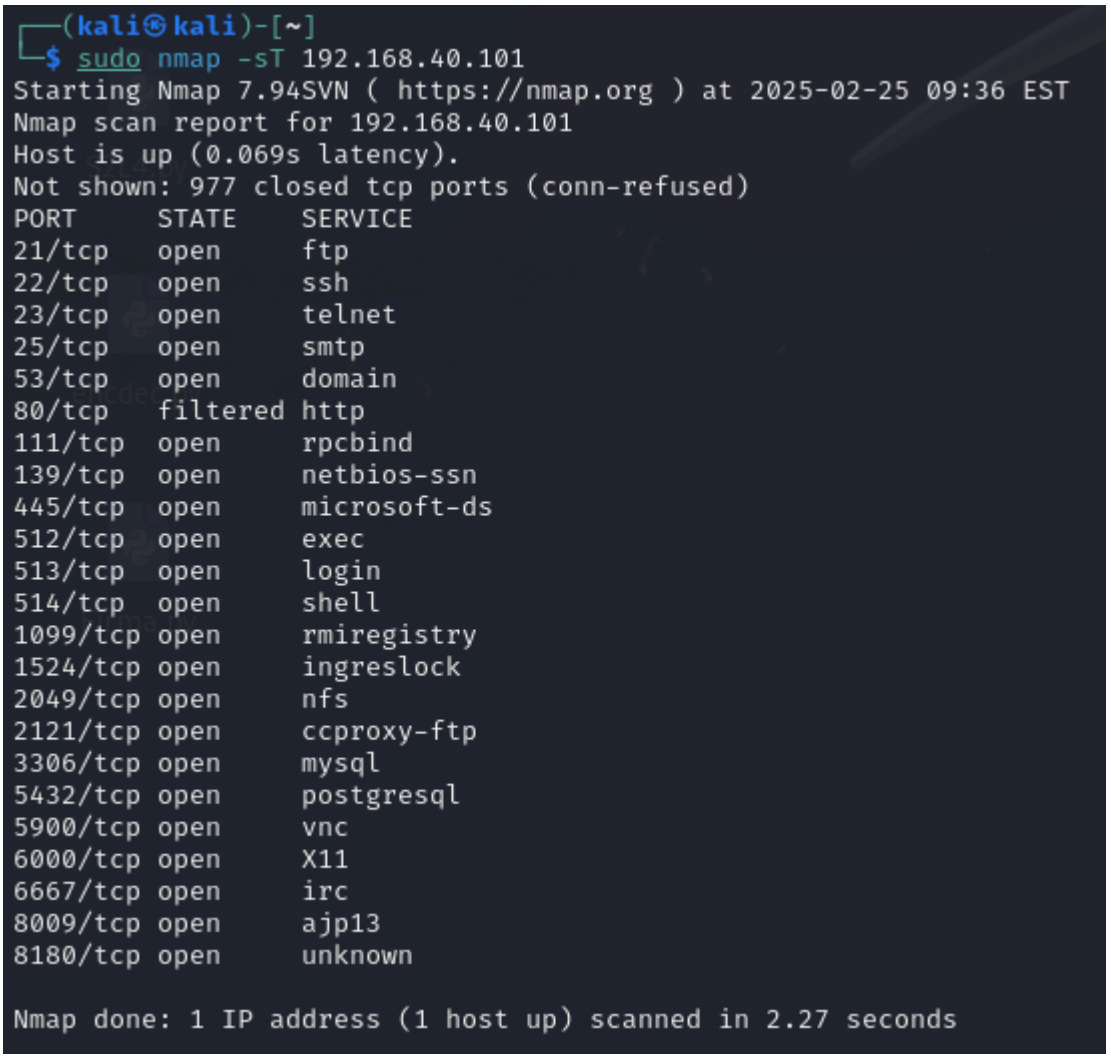
SYN Scan:

Comando: sudo nmap -sS 192.168.40.101



TCP Connect Scan:

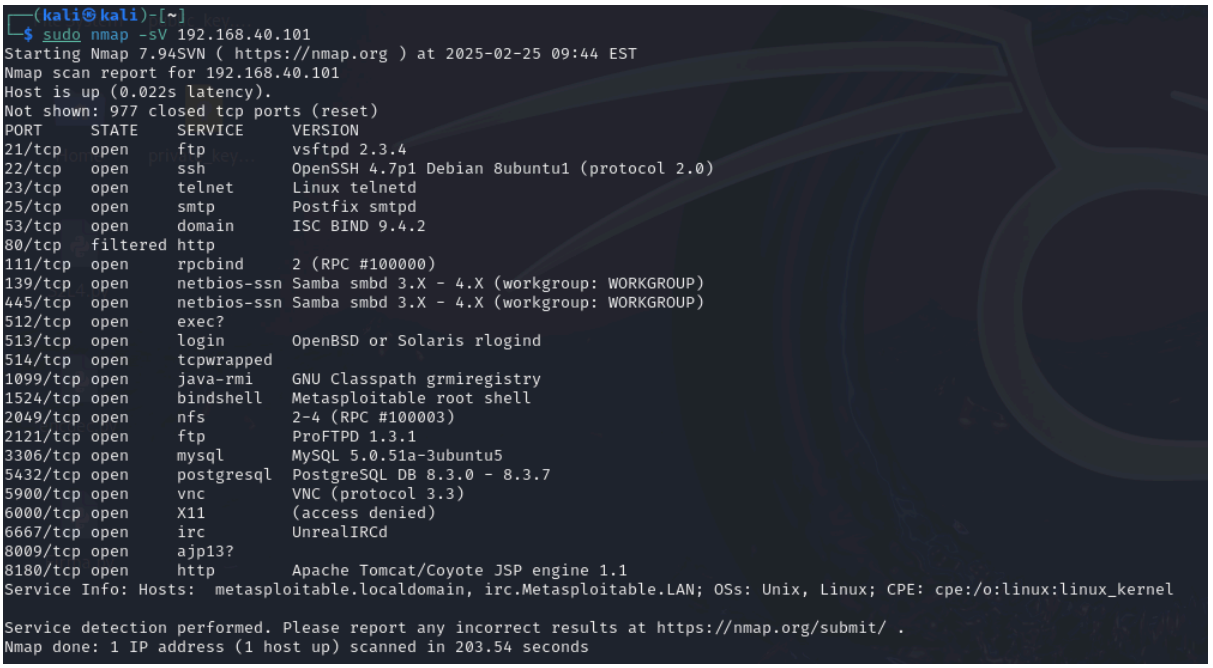
Comando: sudo nmap -sT 192.168.40.101



Differenze: con SYN Scan: non ci sono differenze rispetto alla scansione SYN

Version Detection:

Comando: sudo nmap -sV 192.168.40.101



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.40.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 09:44 EST
Nmap scan report for 192.168.40.101
Host is up (0.022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE     VERSION
21/tcp   open     ftp         vsftpd 2.3.4
22/tcp   open     ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet      Linux telnetd
25/tcp   open     smtp        Postfix smtpd
53/tcp   open     domain      ISC BIND 9.4.2
80/tcp   filtered http
111/tcp  open     rpcbind     2 (RPC #100000)
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open     exec?
513/tcp  open     login       OpenBSD or Solaris rlogind
514/tcp  open     tcpwrapped
1099/tcp open     java-rmi    GNU Classpath grmiregistry
1524/tcp open     bindshell   Metasploitable root shell
2049/tcp open     nfs         2-4 (RPC #100003)
2121/tcp open     ftp         ProFTPD 1.3.1
3306/tcp open     mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc         VNC (protocol 3.3)
6000/tcp open     X11         (access denied)
6667/tcp open     irc         UnrealIRCd
8009/tcp open     ajp13?
8180/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 203.54 seconds
```

Nmap Scan Report

Comando: sudo nmap -sS -O -sV -oX reportscan.xml 192.168.40.101 && xsltproc reportscan.xml -o reportscan.html

Nmap Scan Report - Scanned at Tue Feb 25 09:22:19 2025

Scan Summary | **192.168.40.101**

Scan Summary

Nmap 7.94SVN was initiated at Tue Feb 25 09:22:19 2025 with these arguments:
/usr/lib/nmap/nmap -sS -O -sV -oX reportscan.xml 192.168.40.101

Verbosity: 0; Debug level 0

Nmap done at Tue Feb 25 09:25:34 2025; 1 IP address (1 host up) scanned in 194.45 seconds

192.168.40.101

Address

- 192.168.40.101 (ipv4)

Ports

The 977 ports scanned but not shown below are in state: **closed**

- 977 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [1])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4	
22	tcp	open	ssh	syn-ack	OpenSSH	4.7p1 Debian 8ubuntu1	protocol 2.0
23	tcp	open	telnet	syn-ack	Linux telnetd		
25	tcp	open	smtp	syn-ack	Postfix smtpd		
53	tcp	open	domain	syn-ack	ISC BIND	9.4.2	
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
512	tcp	open	exec	syn-ack			
513	tcp	open	login	syn-ack			
514	tcp	open	tcpwrapped	syn-ack			
1099	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
1524	tcp	open	bindshell	syn-ack	Metasploitable root shell		
2049	tcp	open	nfs	syn-ack		2-4	RPC #100003
2121	tcp	open	ftp	syn-ack	ProFTPD	1.3.1	
3306	tcp	open	mysql	syn-ack	MySQL	5.0.51a-3ubuntu5	
5432	tcp	open	postgresql	syn-ack	PostgreSQL DB	8.3.0 - 8.3.7	
5900	tcp	open	vnc	syn-ack	VNC		protocol 3.3
6000	tcp	open	X11	syn-ack			access denied
6667	tcp	open	irc	syn-ack	UnrealIRCd		
8009	tcp	open	ajp13	syn-ack			
8180	tcp	open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **42330/udp** (**closed**)
- OS match: **Linux 2.6.15 - 2.6.26 (likely embedded)** (**100%**)
- OS match: **Linux 2.6.29 (Gentoo)** (**100%**)

Misc Metrics (click to expand)

Metric	Value
Ping Results	echo-reply
System Uptime	603 seconds (last reboot: Tue Feb 25 09:15:31 2025)
Network Distance	2 hops
TCP Sequence Prediction	Difficulty=194 (Good luck!)
IP ID Sequence Generation	All zeros

Target: Windows

IP Target: 192.168.50.151

Scansioni Eseguite:

OS Fingerprint: