PRATICA M2/S1/L2
CS0225IT
MIRKO GERIA

Introduzione

L'esercizio di oggi ci chiede:
Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

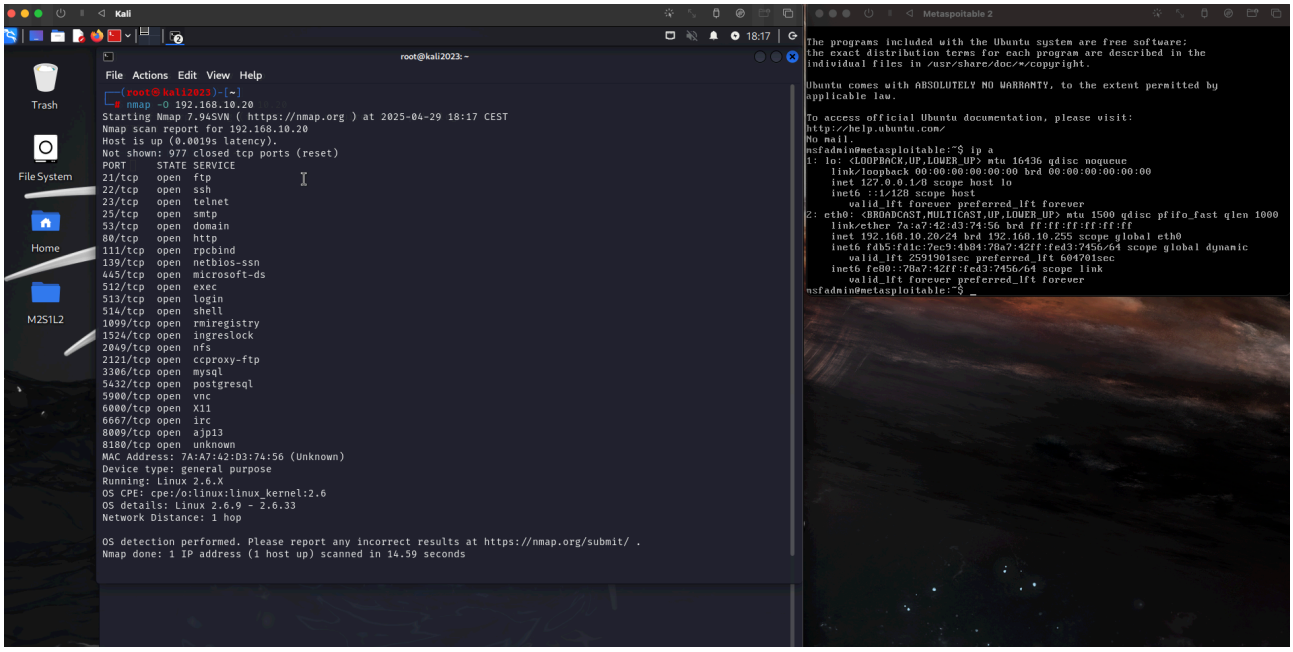
- OS fingerprint.
- Syn Scan.
- TCP connect – trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

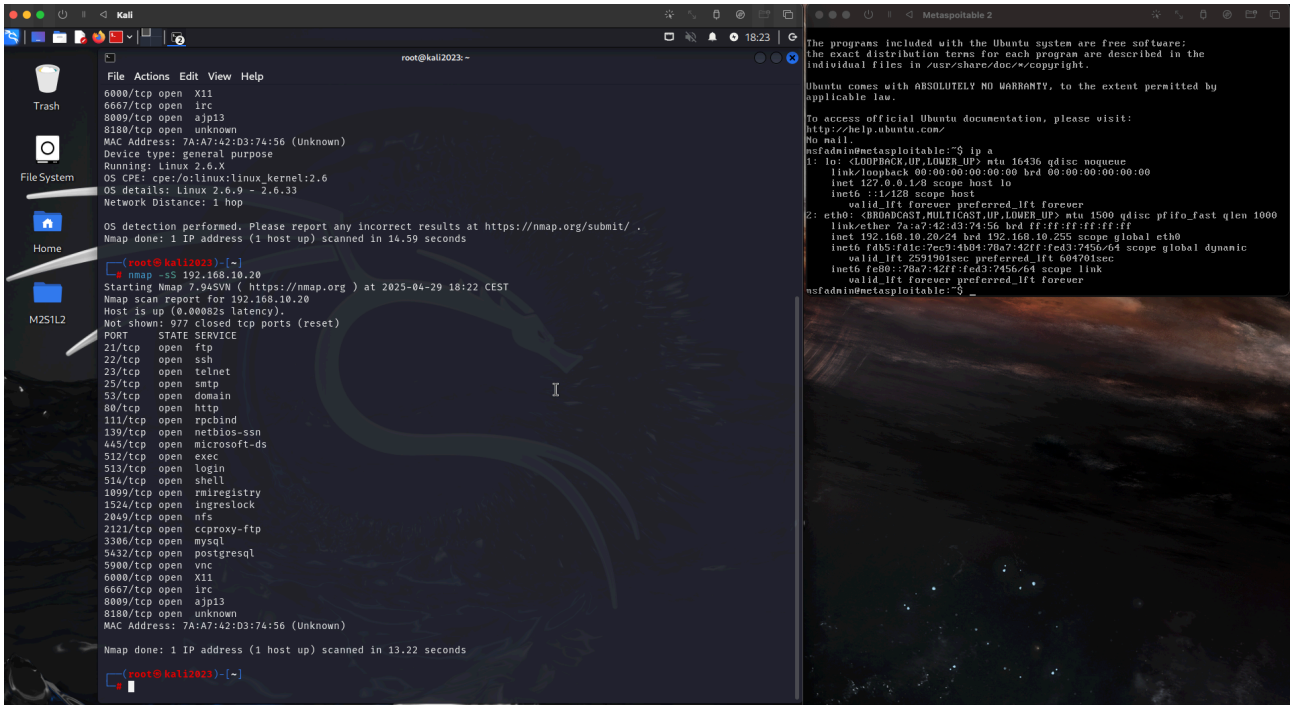
- OS fingerprint.

Descrizione del procedimento

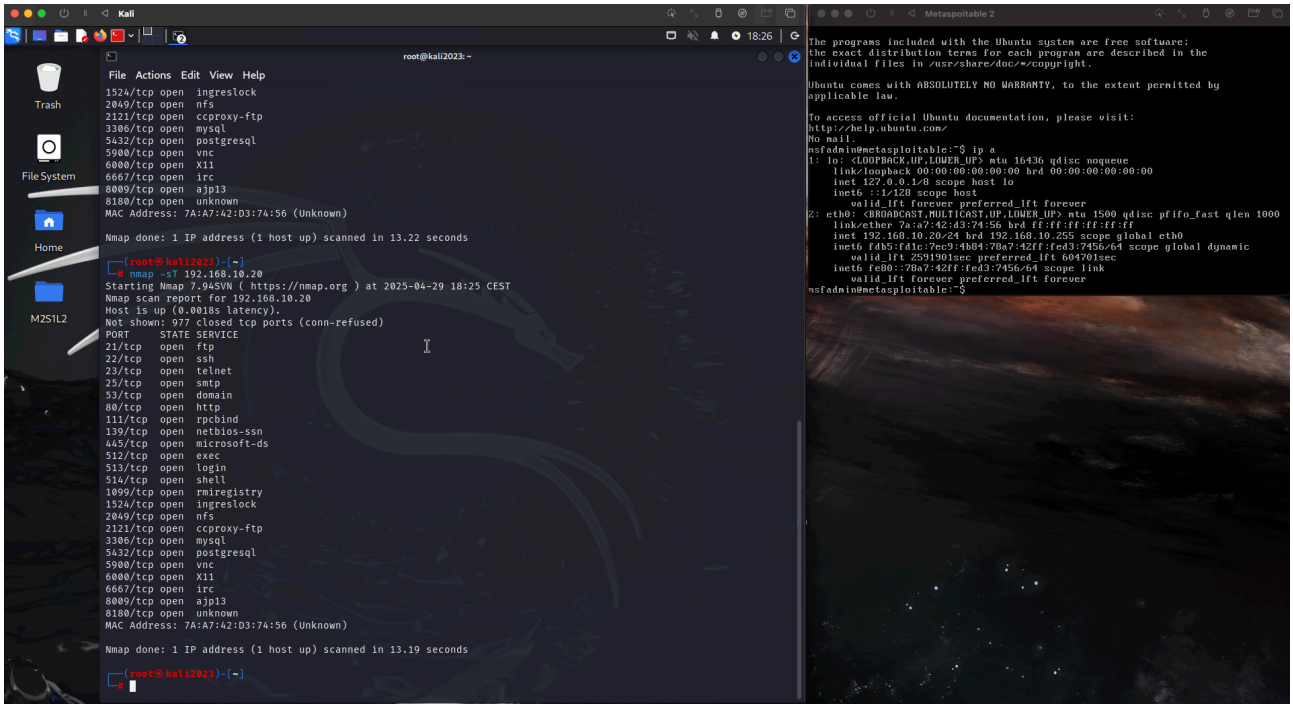
Usiamo Kali linux 192.168.10.10 per eseguire la scansione OS su metasploitable 192.168.10.20 con il comando ‘sudo nmap -O 192.168.10.20’ e avremo questo risultato:



Per la SYN Scan usiamo il comando ‘nmap -sS 192.168.10.20’ e avremo questo risultato:

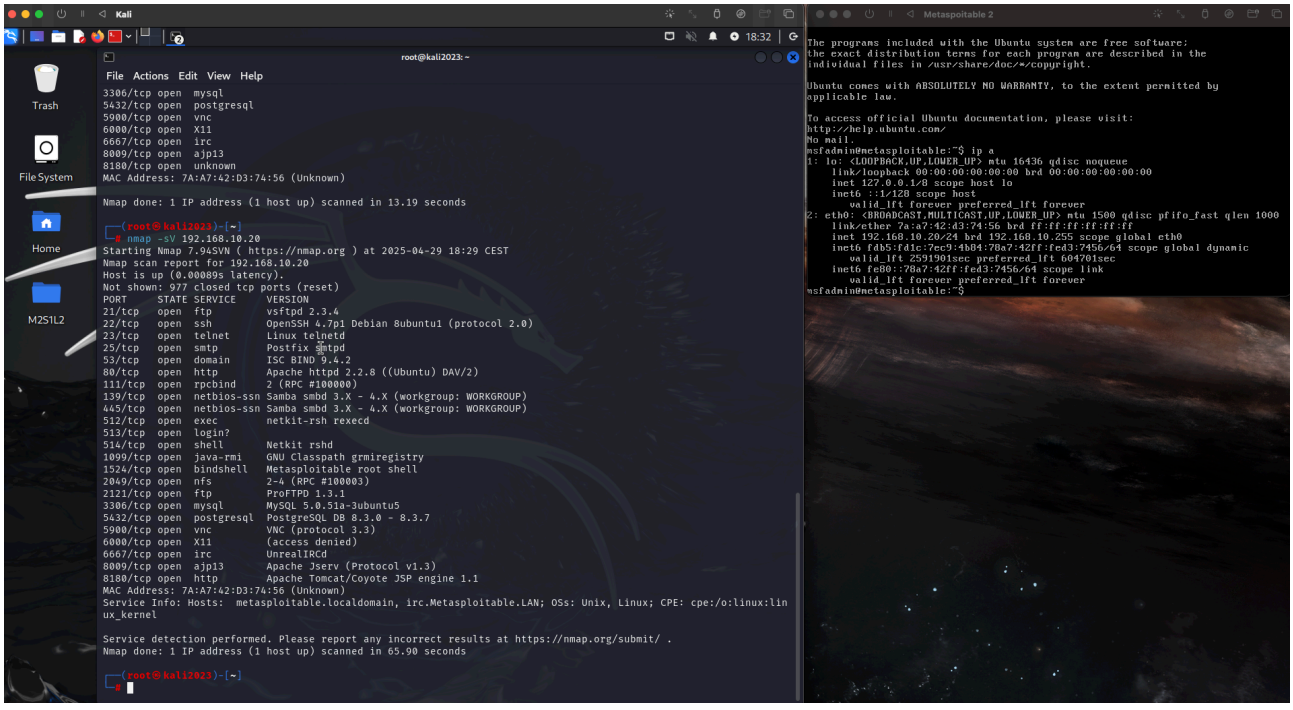


Per la TCP Connect Scan usiamo il comando ‘nmap –sT 192.168.10.20’ e avremo questo risultato:

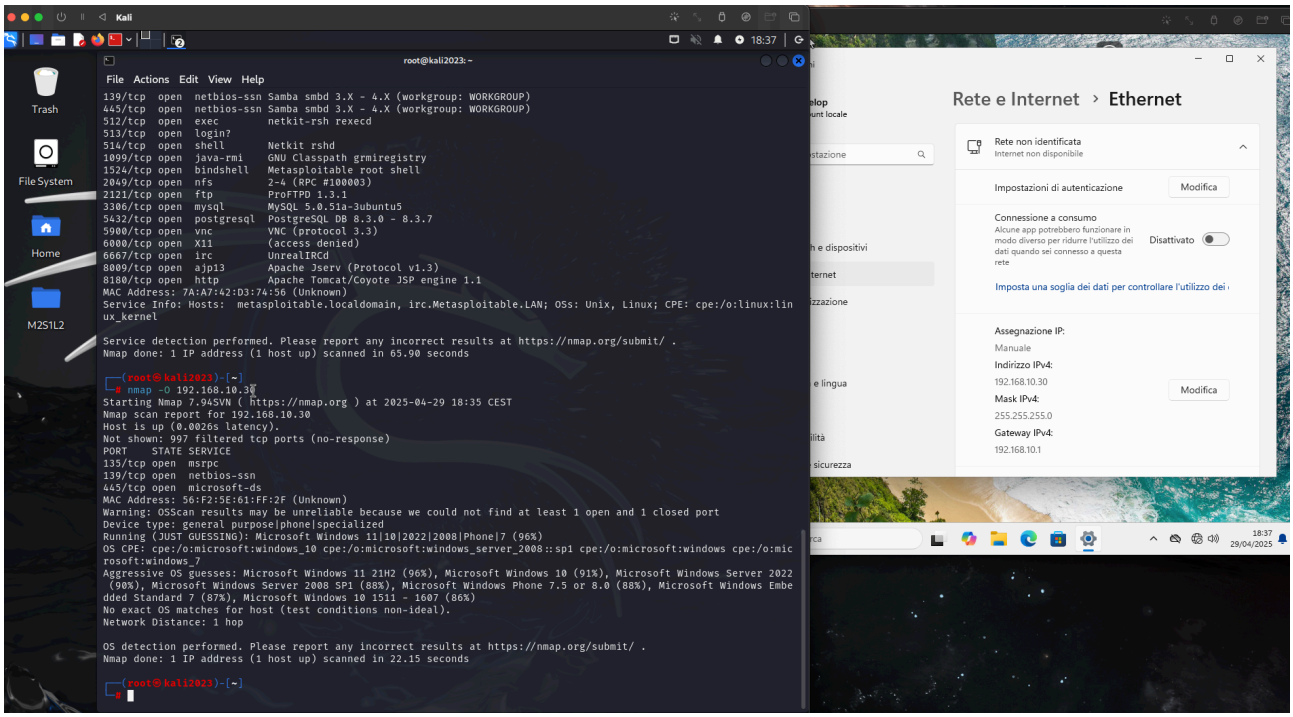


Dove non notiamo differenze con SYN Scan

Per la Version detection usiamo il comando ‘map –sT 192.168.10.20’ e avremo questo risultato:



Fatto cio ci spostiamo a scansionare la VM Windows 11 192.168.10.30 dove eseguiamo solo la scansione OS, tramite Kali linux 192.168.10.10, con il comando 'sudo nmap –O 192.168.10.30' e avremo questo risultato:



Dalla scansione su metasploitabale 192.168.10.20 possiamo evincere quanto segue:

- IP: 192.168.10.20
- OS: Linux 2.6.9 – 2.6.33
- 23 Porta aperte:

PORTA	OPEN/CLOSED
21/tcp	open
22/tcp	open
23/tcp	open
25/tcp	open
53/tcp	open
80/tcp	open
111/tep	open
139/tcp	open

445/tcp	open
512/tcp	open
513/tcp	open
514/tcp	open
1099/tcp	open
1524/tcp	open
2049/tcp	open
2121/tcp	open
3306/tcp	open
5432/tcp	open
5900/tcp	open
6000/tcp	open
6667/tcp	open
8009/tcp	open
8180/tcp	open

- **Servizi in ascolto con versione:**

SERVIZIO	VERSIONE
ftp	vsftpd 2.3.4
ssh	OpenSSH 4.7p1 Debian 8ubuntui (protocol
telnet	Linux telnetd
smtp	Postfix Smtpd
domain	ISC BIND 9.4.2
http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
rpebind	2 (RPC #100000)
netbios-ssn	Samba smbd 3. - 4.X (workgroup:
netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
exec	netkit-rsh rexecd
login?	
shell	Netkit rshd
java- rmi	GNU Classpath grmiregistry
bindshell	Metasploitable root shell
nfs	2-4 (RPC #100003)
ftp	ProFTPD 1.3.1

mysql	MySOL 5.0.51a-3ubuntu5
postgresql	PostgreSQL DB 8.3.0 - 8.3.7
vnG	VNC (protocol 3.3)
X11	(access denied)
irc	UnrealIRCd
ajp13	Apache Jserv (Protocol v1.3)
http	Apache Tomcat/Coyote JSP engine 1.1

-

Mentre dalla scansione fatta su Windows 11 possiamo evincere quanto segue:

- IP: 192.168.10.30
- OS: Microsoft Windows 11 21H2 (96%)

Autori e contatti

Mirko Geria
mirkogeria@gmail.com
+39 33318*****