ESERCIZIO W11D1
SCANSIONI NMAP

Studente: Davide Mirani

Traccia:

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable (target e attaccante devono essere su due reti diverse):

- OS fingerprint
- Syn Scan
- TCP connect
- Version detection

A valle delle scansioni, è prevista la produzione di un report contenente le seguenti info (dove disponibili):

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

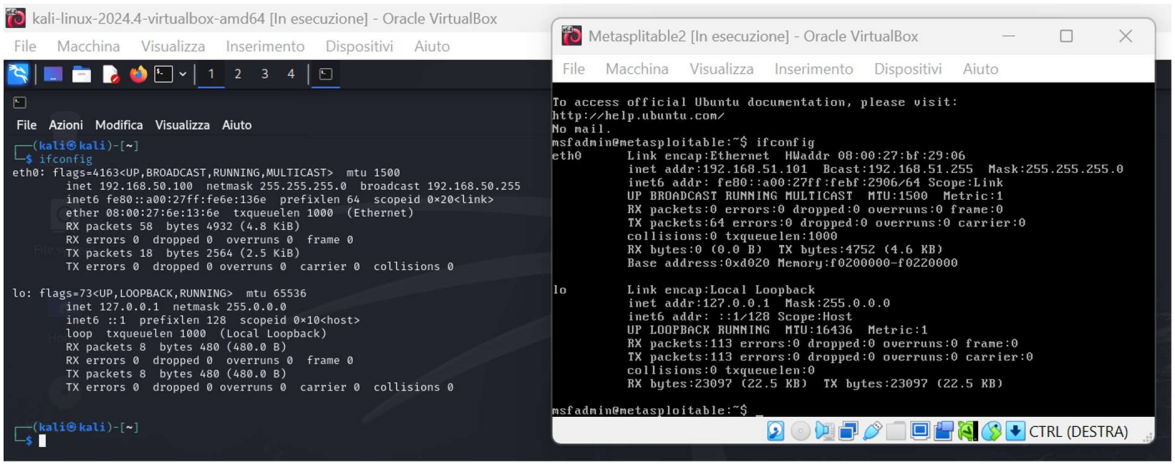
1. Introduzione

L'obiettivo dell'esercizio è eseguire una serie di scansioni Nmap contro una macchina Metasploitable da una macchina Kali Linux, assicurandosi che le due siano configurate su reti diverse.

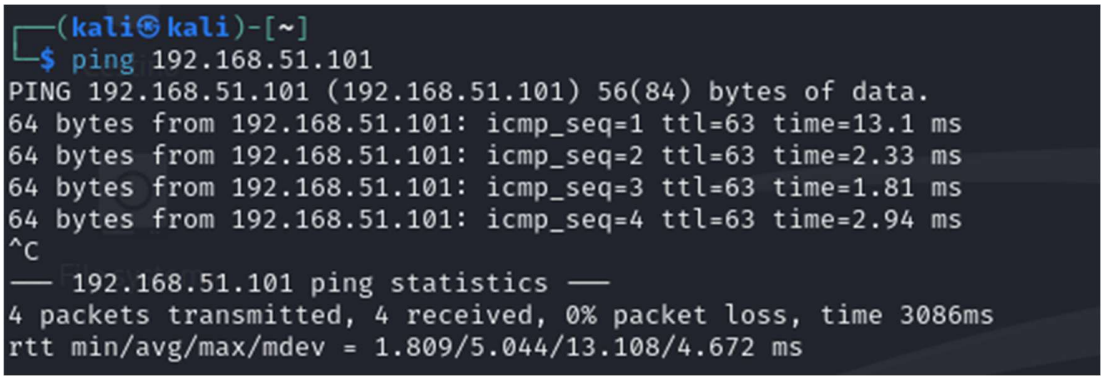
2. Configurazione di rete

- **Kali Linux IP:** 192.168.50.100
- **Metasploitable IP:** 192.168.51.101

Le macchine sono su due reti diverse, come richiesto nella traccia.



3. Raggiungibilità della macchina (ping)



4. Risultati delle scansioni

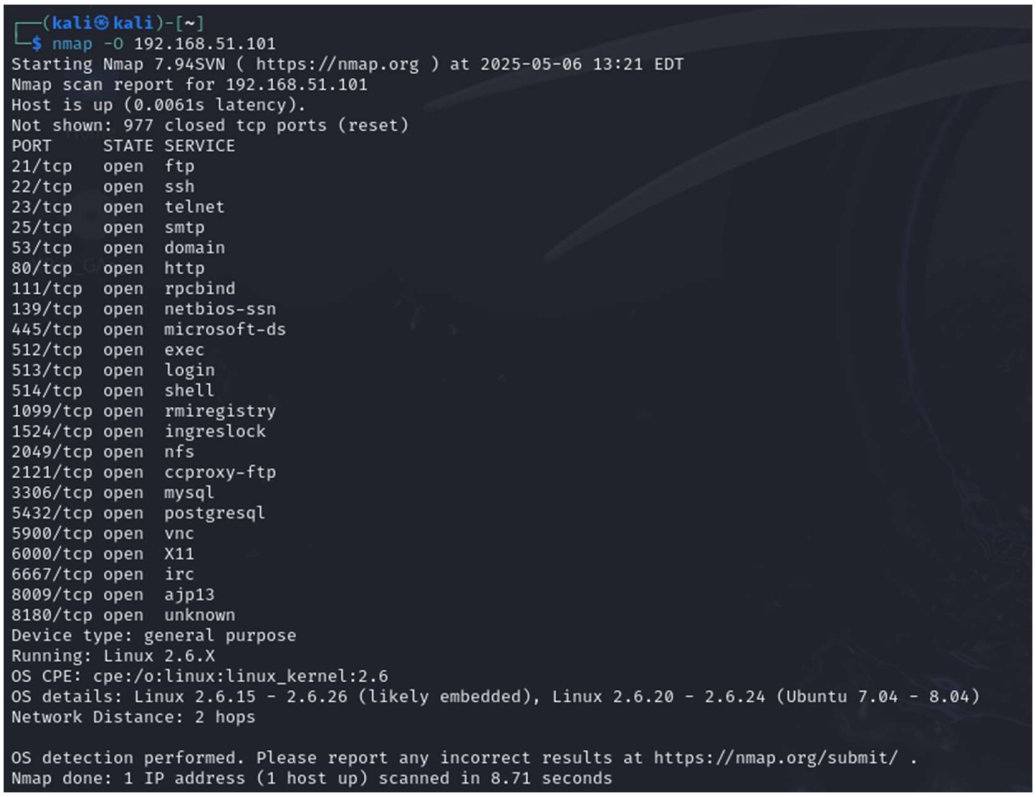
Porta	Servizio	Stato (sS)	Stato (sT)	Versione (sV)
21	ftp	open	open	vsftpd 2.3.4
22	ssh	open	open	OpenSSH 4.7p1 Debian 8ubuntu1
23	telnet	open	open	Linux telnetd
25	smtp	open	open	Postfix smtpd
53	domain	open	open	ISC BIND 9.4.2
80	http	open	open	Apache httpd 2.2.8
111	rpcbind	open	open	2 (RPC #100000)
139	netbios-ssn	open	open	Samba smbd 3.X - 4.X
445	microsoft-ds	open	open	Samba smbd 3.X - 4.X
512	exec	open	open	netkit-rsh rexecd
513	login	open	open	?
514	shell	open	open	Netkit rshd
1099	rmiregistry	open	open	GNU Classpath grmiregistry
1524	ingresslock	open	open	Metasploitable root shell
2049	nfs	open	open	2-4 (RPC #100003)

2121	ccproxy-ftp	open	open	?
3306	mysql	open	open	MySQL 5.0.51a-3ubuntu5
5432	postgresql	open	open	PostgreSQL DB 8.0 - 8.3.7
5900	vnc	open	open	VNC (protocol 3.3)
6000	X11	open	open	(access denied)
6667	irc	open	open	UnrealIRCd
8009	ajp13	open	open	Apache Jserv (Protocol v1.3)
8180	http (tomcat)	open	open	Apache Tomcat/Coyote JSP engine 1.1

5. OS Fingerprint

- Tipo dispositivo: General purpose
- OS CPE: cpe:/o:linux:linux_kernel:2.6
- Dettagli: Linux 2.6.15 – 2.6.26 (probabilmente Ubuntu 7.04 – 8.04)
- Network distance: 2 hops
- Tempo di scansione: 8.71 secondi

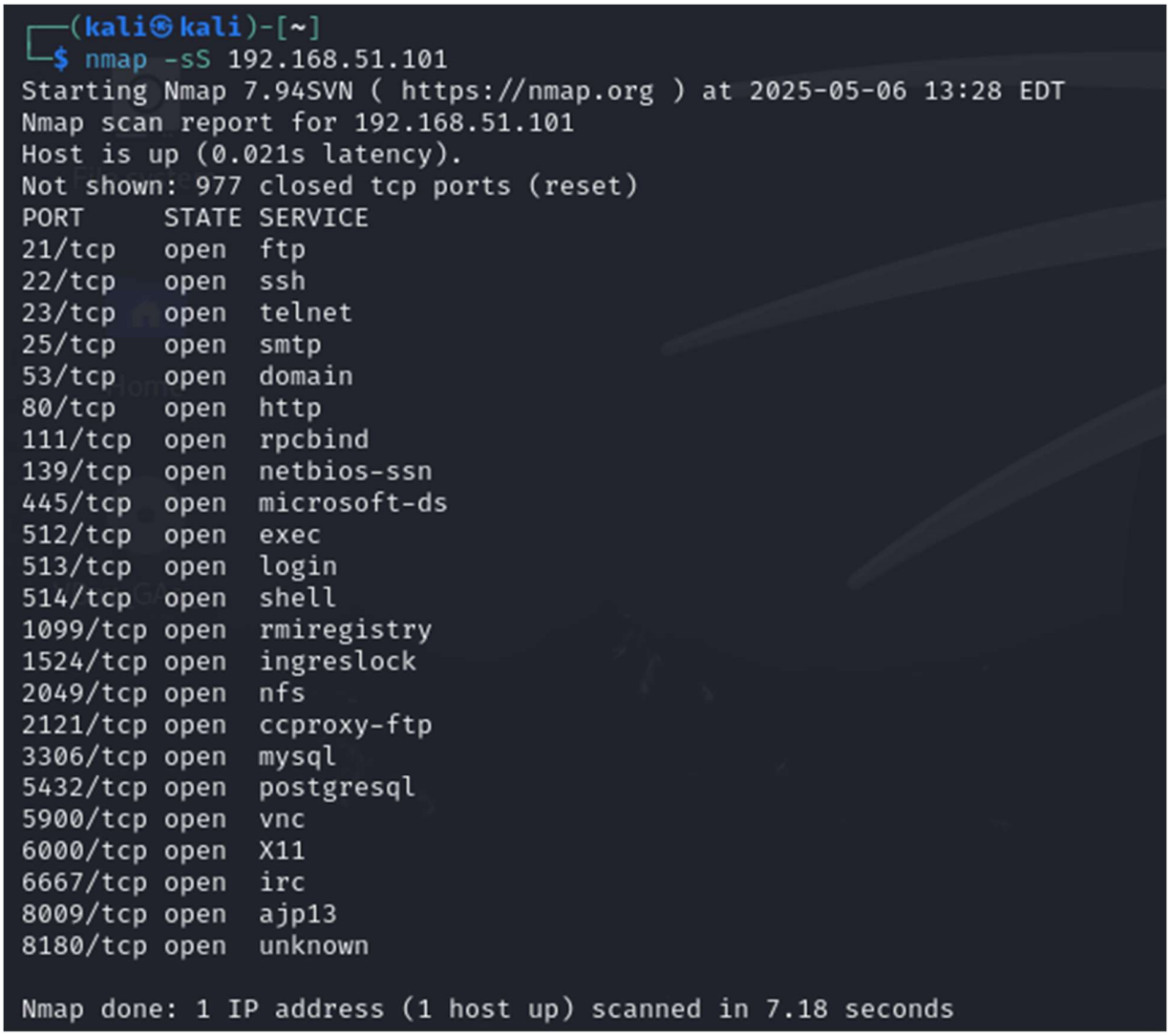
Screenshot OS Fingerprint (nmap -O):



6. Scansione SYN (nmap -sS)

Tempo di scansione: 7.18 secondi

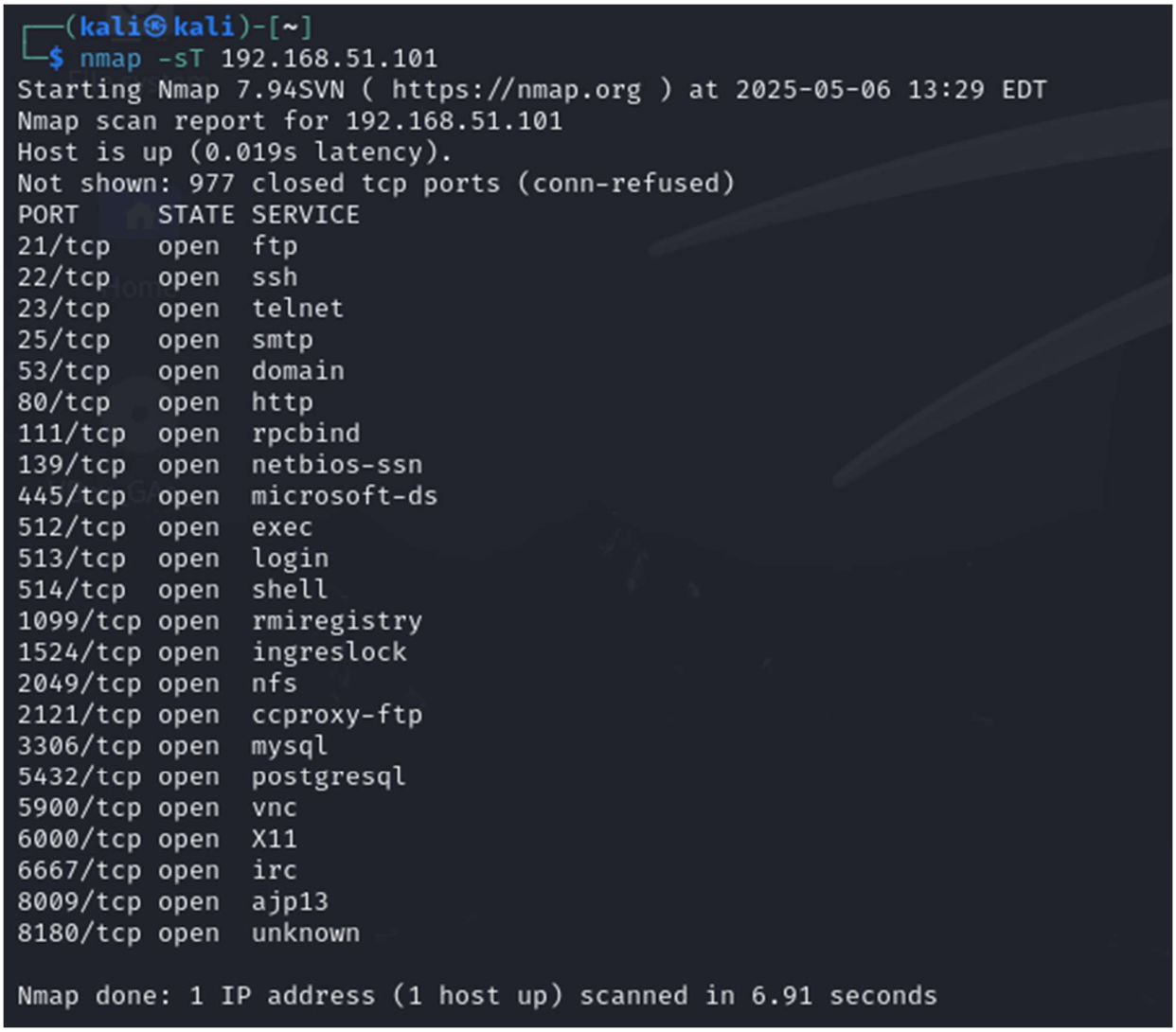
Screenshot della scansione SYN:



7. Scansione TCP Connect (nmap -sT)

Tempo di scansione: 6.91

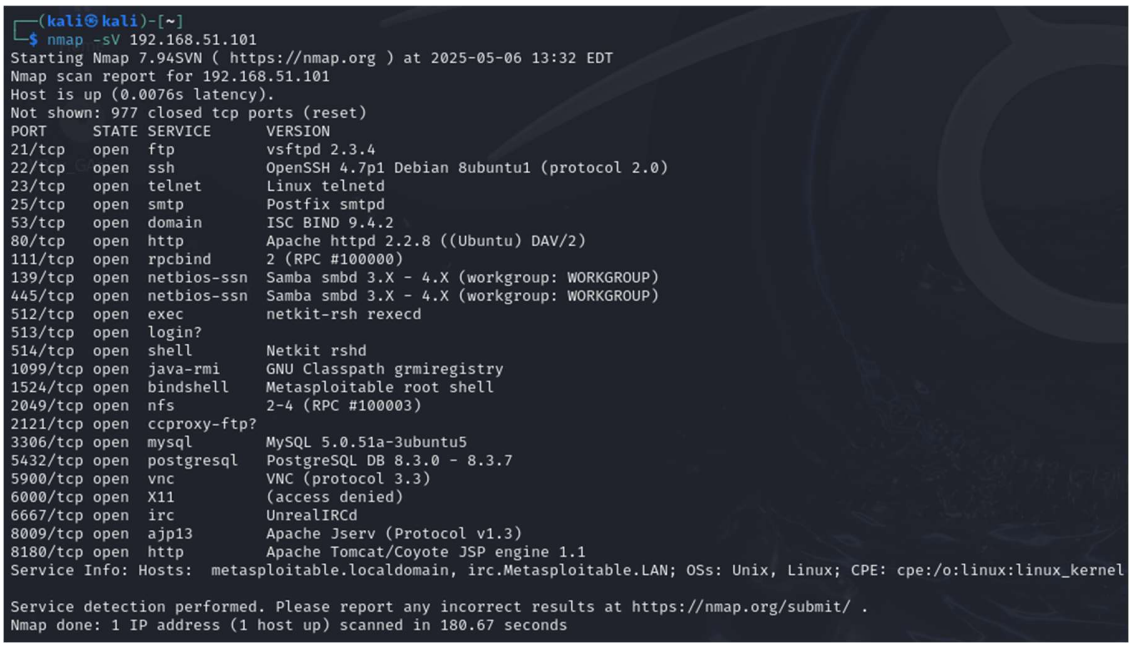
Screenshot della scansione TCP connect:



8. Rilevamento versioni (nmap -sV)

Tempo di scansione: 180.67 secondi

Screenshot rilevamento versione dei servizi:



9. Differenze tra scansioni SYN e TCP Connect

La scansione SYN (`-sS`) è più veloce e meno rilevabile dai firewall/IDS perché non completa la stretta di mano TCP.
La scansione TCP Connect (`-sT`) invece stabilisce una connessione completa ed è più facilmente tracciabile.
In questo caso i risultati delle due scansioni sono identici, variando solo nei tempi.

10. Conclusioni

La macchina Metasploitable presenta molte porte aperte e servizi vulnerabili.
L'identificazione precisa delle versioni tramite `-sV` ha permesso di confermare la natura deliberatamente vulnerabile del sistema target.