Esercitazione W11D1 - Pratica 1

Nmap

Fabio Benevento - 16/01/2024

Traccia

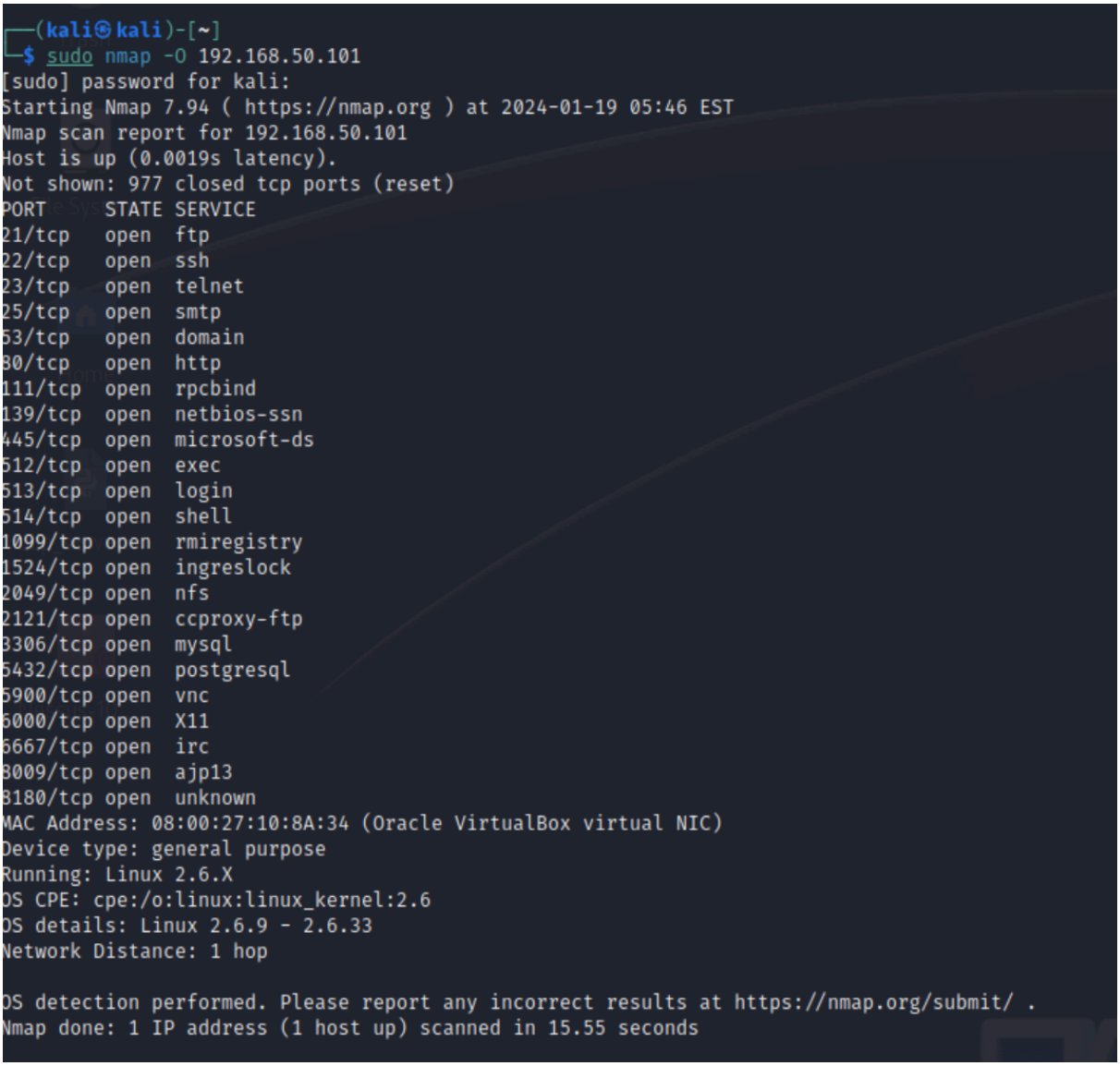
Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:
- OS fingerprint
- Syn Scan
- TCP connect (trovate differenze tra i risultati della scansioni TCP connect e SYN?)
- Version detection

Implementazione

Nelle seguenti pagine sono illustrati i comandi utilizzati per ricavare le informazioni richieste.
Entrambe le macchine sono collocate sulla stessa sottorete (192.168.50.x) con indirizzi rispettivamente di 192.168.50.100 per Kali Linux e di 192.168.50.101 per Metasploitable

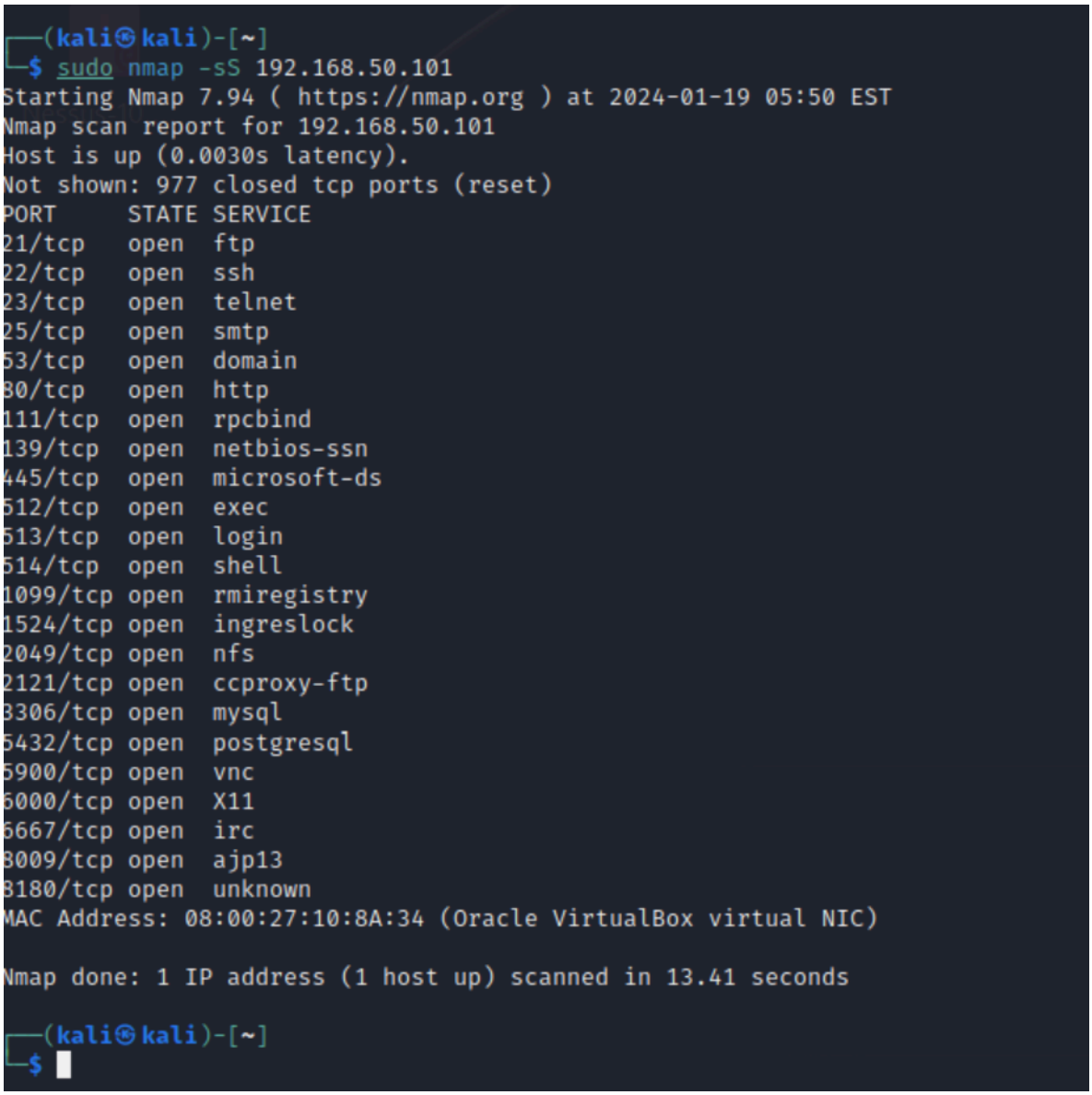
OS Fingerprinting (-O)

Tramite l'opzione -O è possibile individuare la versione del sistema operativo che viene stampata in basso al termine della scansione dei servizi come mostrato nell'immagine sottostante.



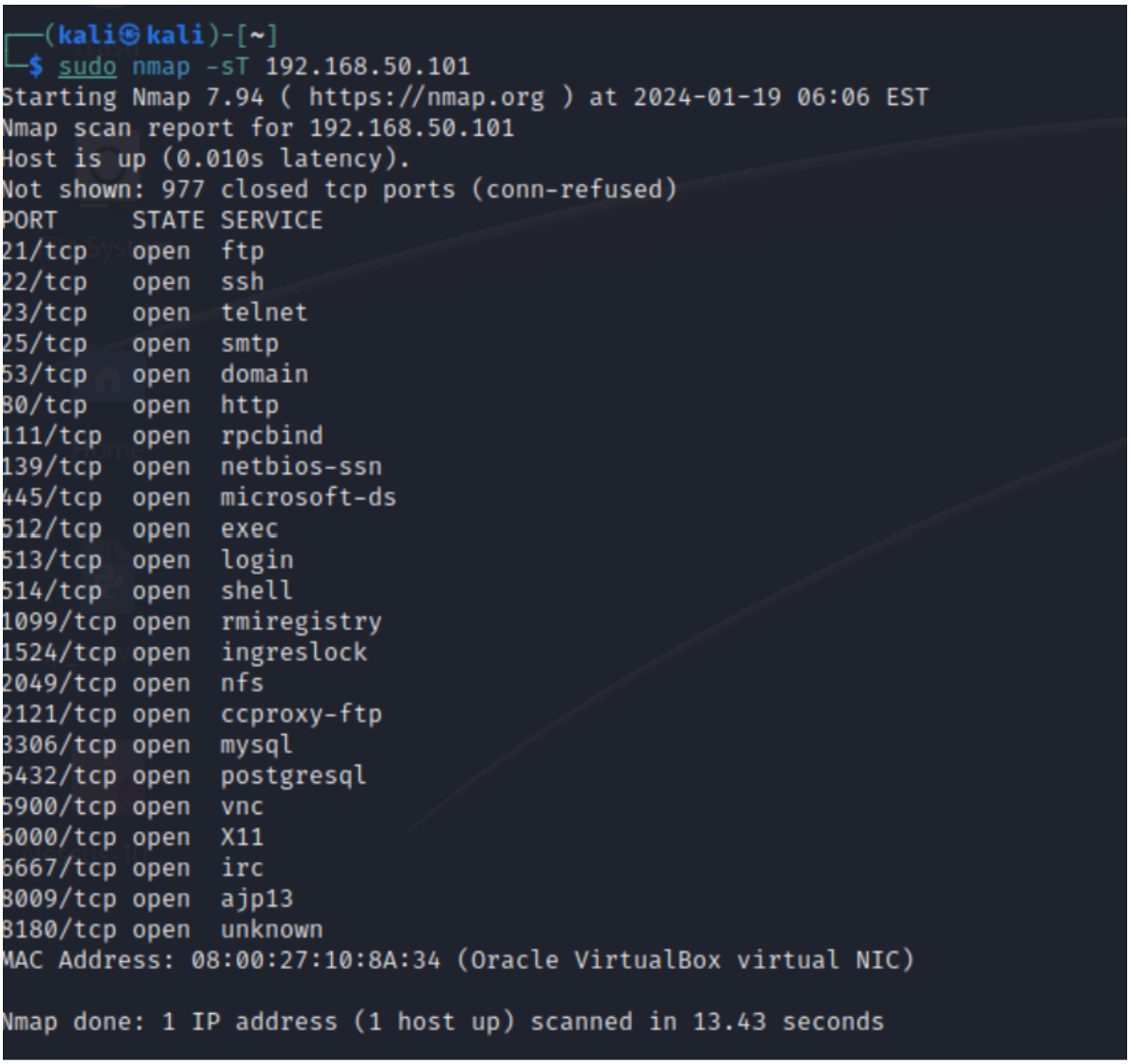
Syn Scan (-S)

Tramite l'opzione -S è possibile effettuare la scansione senza effettuare la connessione completa con three-way handshake



TCP Connect (-T)

Con l'opzione -T invece la scansione viene effettua instaurando una connessione con three-way handshake e risulta quindi più invasiva.



Version detection (-V)

Per il version detection ho utilizzato l'opzione specifica -V. In questo caso, ove possibile, nmap indica la versione del tool che espone il servizio.

Report finale

Di seguito il report in forma tabellare con le informazioni trovate

Fonte	Kali Linux - IP: 192.168.50.100		
Target	Metasploitable - IP: 192.168.50.101		
Tipo di scan	Nmap (varie modalità)		
Numero servizi trovati		12	
Porta	**Servizio**	**Versione**	**Descrizione**
21	ftp	vsftpd 2.3.4	server FTP per scambio file
22	ssh	OpenSSH 4.7p1	connessione sicura remota

23	telnet	Linux telnetd	connessione host remoto
25	smtp	Postfix smtpd	invio posta elettronica
53	domain	ISC Bind 9.4.2	dns
80	http	Apache 2.2.8	server web
111	rpc-bind	2	comunicazione tra processi RPC
139	netbios-ssn	Samba 3.x - 4.x	com. reti locali - sessione
445	microsoft-ds	Samba 3.x - 4.x	condivisione risorse
512	exec	netkit-rsh rexeccd	remote shell (progetto netkit)
513	login		remote shell (progetto netkit)
514	shell	netkit-rsh	remote shell (progetto netkit)
1099	java-rmi	GNU classpath gmiregistry	invocazione metodi remoti
1524	bindshell	Metasploitable root shell	shell remota (hacking)
2049	nfs	2-4	condivisione file
2121	ftp	ProFTP 1.3.1	server FTP per scambio file
3306	mysql	5.0.51a	database relazionale
5432	postgresql	8.3.0 - 8.3.7	database relazionale
5900	vnc	protocol 3.3	controllo desktop remoto
6000	X11		motore grafico di Linux
6667	irc	UnrealIRCd	chat
8009	ajp13	Apache jserv (prot. 1.3)	servlet
8081	http	Apache Tomcat 1.1	server web