Traccia:

Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

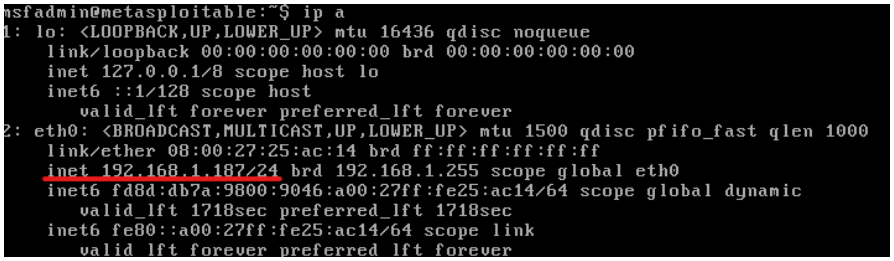
- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati delle scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

- OS fingerprint.

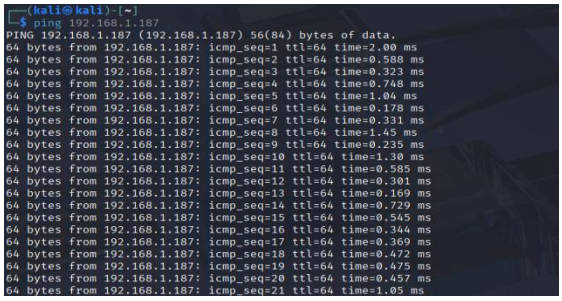
Report Finale

Per prima cosa, controlliamo i diversi IP e facciamo dei ping di prova per verificare che le due macchine Kali e Metasploitable comunichino tra loro.



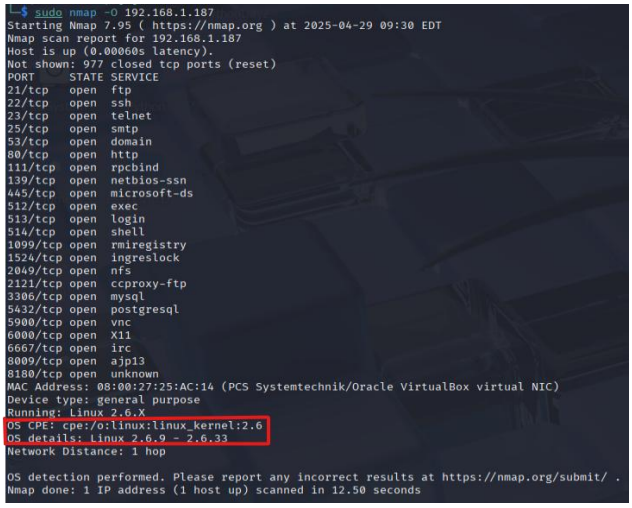
Con il comando <ip a> controlliamo l'ip della Metasploitable che in questo caso è '' 192.168.1.187/24''

A questo punto ''pinghiamo'' su Kali la nostra Metaspliotable – e come possiamo vedere c'è risposta al ping.



Una volta confutata la comunicazione tra le due macchine partiamo con i comandi richiesti nell'esercizio.

Comando: OS fingerprint (Identificazione del sistema operativo)



nmap -O 192.168.1.187

-O: cerca di indovinare il sistema operativo usando tecniche di fingerprinting.

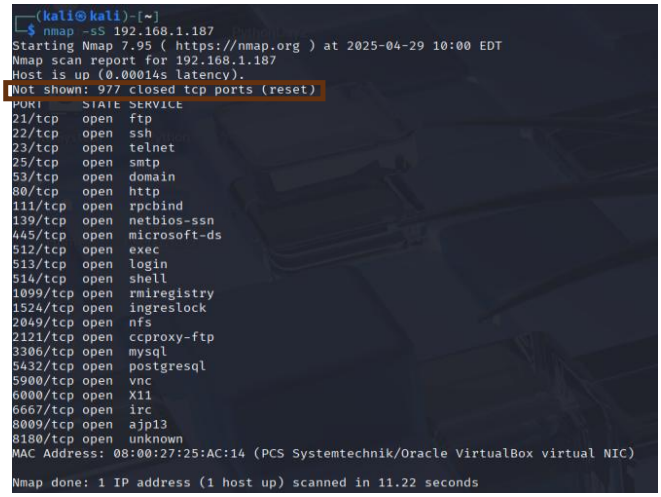
•In questo caso, come da screen, abbiamo scoperto le diverse porte aperte e il sistema operativo evidenziato in rosso:

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: linux 2.6.9 – 2.6.33

- **Perché si usa:** Identifica il sistema operativo in esecuzione su un host remoto (es. Windows, Linux, etc.).
- **Come funziona:** Analizza il comportamento della macchina in risposta a pacchetti TCP/IP particolari.

Comando: Syn Scan (scansione più veloce e discreta)



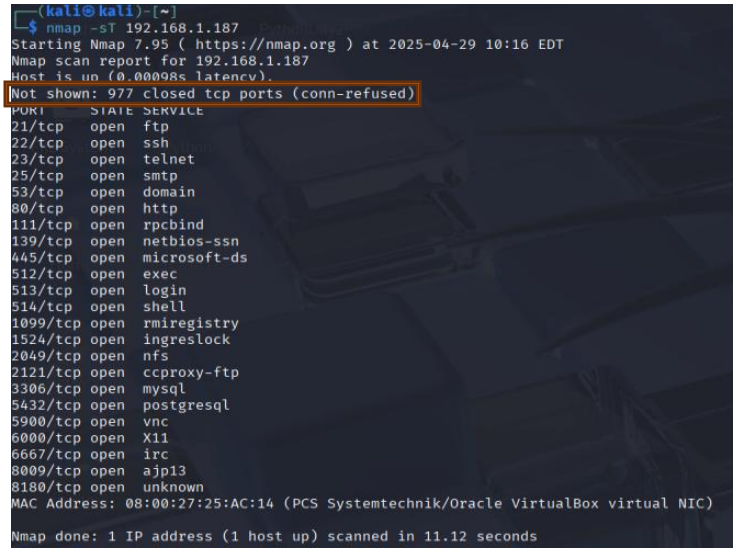
nmap -sS 192.168.1.187

-sS: Syn scan, detta anche "half-open scan", invia solo pacchetti SYN.

È rapida e furtiva (molti firewall la rilevano con più difficoltà).

- **Perché si usa:** È il tipo di scansione più veloce e discreto per identificare porte aperte.
- **Come funziona:** Invia un pacchetto SYN (inizio handshake) e legge la risposta, senza completare la connessione (stealth scan).

TCP Connect Scan (per inviare pacchetti raw)



nmap -sT 192.168.1.187

-sT: usa la chiamata di sistema completa connect() per aprire le connessioni TCP.

È **più facile da rilevare**, ma non richiede privilegi di root.

- **Perché si usa:** È usato quando non hai i permessi per inviare pacchetti raw (es. senza privilegi di root).
- **Come funziona:** Esegue il normale handshake TCP completo (SYN, SYN-ACK, ACK).

Differenze tra i due comandi -sS -sT

Nel risultato della riga quattro del comando -sS notiamo:

- Not Shown: 977 closed tcp ports (reset) – ovvero 977 porte chiuse che non vengono mostrate.

-sS (SYN scan): È una **scansione "half-open"**, cioè Nmap invia solo un pacchetto SYN per vedere se la porta è aperta. Se è chiusa, riceve un pacchetto **RST (reset)** in risposta. → Mostrato come **(reset)** evidenziato nello screenshot (in arancione)

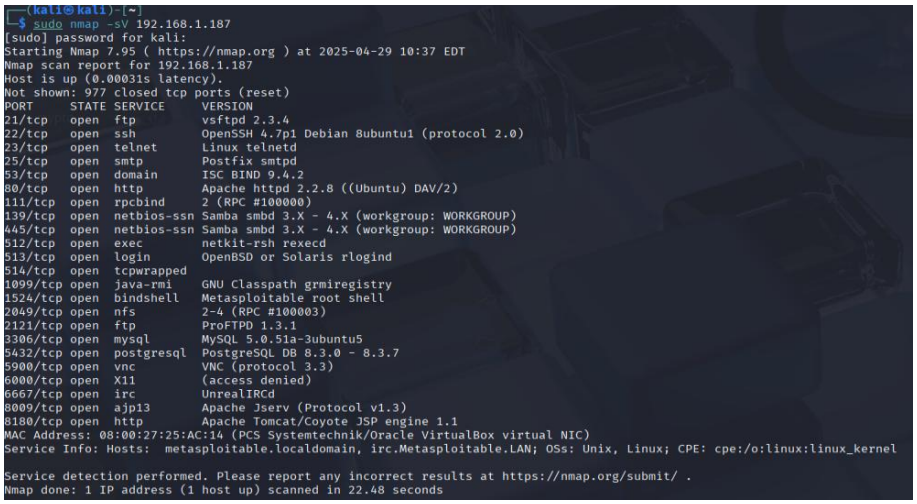
Mentre nel risultato del comando nmap -sT notiamo:

- Not Shown: 977 closed tcp ports (conn-refused) – indicazione che se la porta è chiusa, il sistema target rifiuta la connessione, e quindi si ottiene un **Connection Refused (conn-refused).**

-sT (TCP connect scan): È una **scansione completa**, che utilizza la funzione connect () del sistema operativo per aprire una vera connessione TCP. Se la porta è chiusa, il sistema target rifiuta la connessione, e quindi si ottiene un **Connection Refused**. → Mostrato come **(conn-refused)** evidenziato nello screenshot (in arancione).

Anche le tempistiche di risposta tra i due comandi sono diverse, il comando nmap -sS oltre ad essere più veloce è anche più ‘’stealth’’ e lascia meno log nei target. Nonostante il metodo diverso, **entrambi hanno elencato le stesse porte aperte** e indicano che 977 porte erano chiuse (ma non mostrate in dettaglio).

Version Detection (servizi in esecuzione delle porte aperte)



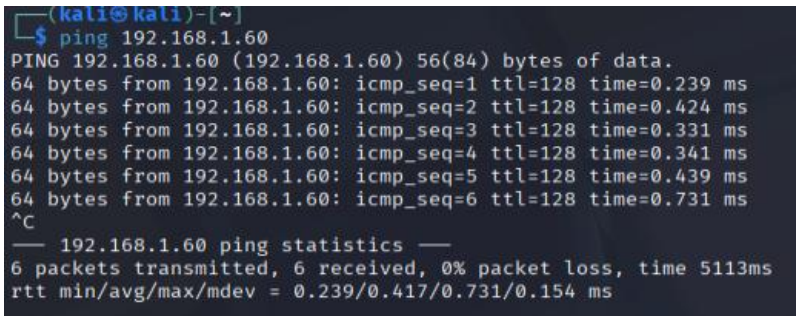
sudo nmap -sV 192.168.1.187

-sV: cerca di determinare le **versioni dei servizi** in esecuzione sulle porte aperte.

- **Perché si usa:** Identifica il tipo e la versione precisa dei servizi in esecuzione su una porta
- **Come funziona:** Interroga le porte aperte e analizza le risposte dei servizi.

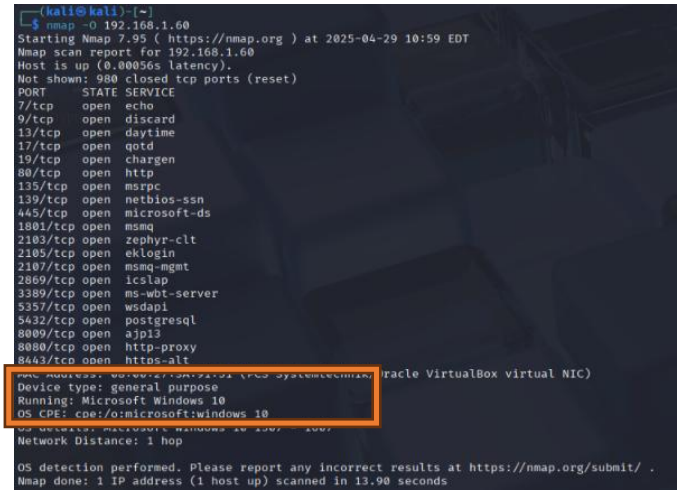
Sintesi finale: il target presenta numerosi servizi attivi, alcuni dei quali obsoleti e a rischio. L'implementazione tempestiva di contromisure (chiusura porte inutilizzate, aggiornamenti, cifratura dei servizi) porterà ad un significativo innalzamento della postura di sicurezza complessiva.

E la seguente sul target Windows: OS fingerprint.



Come sempre controlliamo che le due macchine pinghino tra loro.

In questo caso l'ip di Windows è 192.168.1.60.



Andiamo ora ad usare il comando OS Fingerprint: nmap -O 192.168.1.60 – verificando il sistema operativo che come possiamo constatare nello screenshot di sinistra, il risultato del comando, conferma il OS della nostra VM, in questo caso Windows 10.

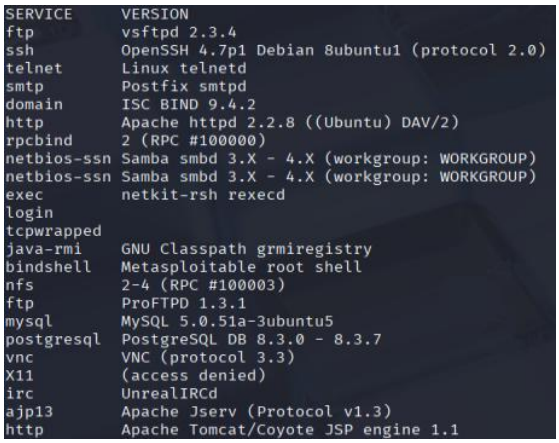
Conclusioni

IP Target: 192.168.1.187
Sistema Operativo:
Sistema Rilevato: Linux 2.6.x
Dettagli: Linux 2.6.9 - 2.6.33
MAC Address: 08:00:27:25:AC:14
Vendor NIC: PCS Systemtechnik / Oracle VirtualBox (virtual NIC)

Porte Aperte e Servizi:

21/tcp - open - ftp
22/tcp - open - ssh
23/tcp - open - telnet
25/tcp - open - smtp
53/tcp - open - domain
80/tcp - open - http
111/tcp - open - rpcbind
139/tcp - open - netbios-ssn
445/tcp - open - microsoft-ds
512/tcp - open - exec
513/tcp - open - login
514/tcp - open - shell
1099/tcp - open - rmiregistry
1524/tcp - open - ingreslock
2049/tcp - open - nfs
2121/tcp - open - ccproxy-ftp
3306/tcp - open - mysql
5432/tcp - open - postgresql
5900/tcp - open - vnc
6000/tcp - open - X11
6667/tcp - open - irc
8009/tcp - open - ajp13
8180/tcp - open - unknown

Servizi aperti con Versione:



```
SERVICE     VERSION
ftp         vsftpd 2.3.4
ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
telnet      Linux telnetd
smtp        Postfix smtpd
domain      ISC BIND 9.4.2
http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
rpcbind     2 (RPC #100000)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
exec        netkit-rsh rexecd
login
tcpwrapped
java-rmi    GNU Classpath grmiregistry
bindshell   Metasploitable root shell
nfs         2-4 (RPC #100003)
ftp         ProFTPD 1.3.1
mysql       MySQL 5.0.51a-3ubuntu5
postgresql  PostgreSQL DB 8.3.0 - 8.3.7
vnc         VNC (protocol 3.3)
X11         (access denied)
irc         UnrealIRCd
ajp13       Apache Jserv (Protocol v1.3)
http        Apache Tomcat/Coyote JSP engine 1.1
```

Le scansioni effettuate tramite Nmap sono state eseguite con l'obiettivo di identificare e documentare le caratteristiche principali degli host attivi all'interno della rete analizzata.
In particolare, l'attività ha permesso di raccogliere informazioni relative agli indirizzi IP, ai sistemi operativi rilevati, alle porte aperte e ai servizi in ascolto con le relative versioni.

Questi dati costituiscono la base informativa necessaria per una successiva fase di analisi nel nostro caso di pentesting.