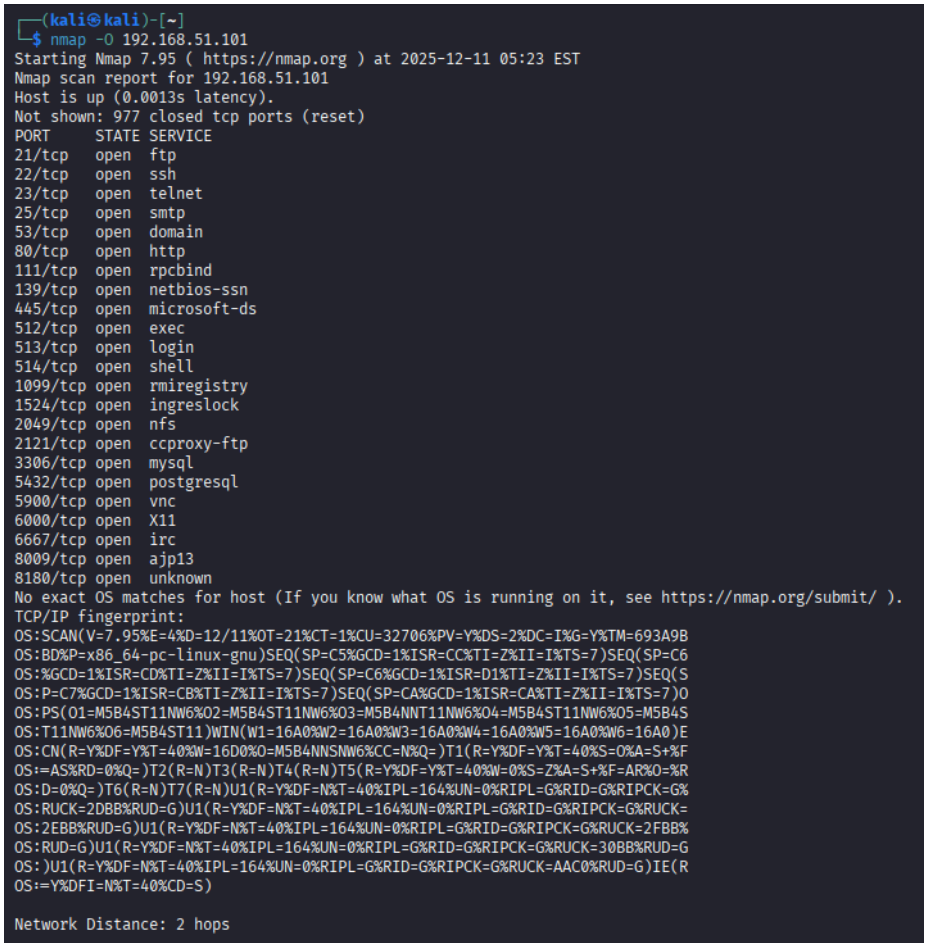
Report di Scansione Nmap

Il presente report documenta l'attività di scansione di rete effettuata sul target **Metasploitable** (**192.168.51.101**) da una macchina **Kali Linux** (**192.168.50.100**). Le due macchine sono posizionate su reti diverse e comunicano attraverso un firewall **pfSense**. L'obiettivo dell'esercizio è identificare il sistema operativo del target, le porte aperte, i servizi in ascolto e confrontare le tecniche di scansione **SYN** e **TCP Connect**.

OS Fingerprinting

L'OS fingerprinting è stato eseguito utilizzando il comando `nmap -O 192.168.51.101` per identificare il sistema operativo del target attraverso l'analisi delle risposte ai pacchetti di rete.

Risultati: La scansione ha rilevato **23** porte aperte su **1000** porte totali scansionate. Tuttavia, dallo screenshot non è visibile un'identificazione esplicita del sistema operativo.



SYN Scan

La **SYN** scan è stata eseguita con il comando `nmap -sS 192.168.51.101`. Questa tecnica utilizza una half-open connection, inviando pacchetti **SYN** senza completare il three-way handshake **TCP**, rendendola più stealth.

Risultati: La scansione ha rilevato **23** porte aperte e **977** porte chiuse (indicate come **reset**). Il tempo di completamento è stato di 13.45 secondi. Le porte chiuse rispondono con pacchetti RST, caratteristico di questa tipologia di scansione.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 05:25 EST
Nmap scan report for 192.168.51.101
Host is up (0.0074s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
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

Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds
```

TCP Connect Scan

La **TCP connect** scan è stata eseguita con il comando `nmap -sT 192.168.51.101`. Questa tecnica completa l'intero **three-way handshake TCP**, stabilendo connessioni complete con le porte del target.

Risultati: La scansione ha rilevato le stesse **23** porte aperte e **977** porte chiuse (indicate come **conn-refused**). Il tempo di completamento è stato di 13.33 secondi.

Differenze tra SYN Scan e TCP Connect Scan:

- **Gestione porte chiuse**: La **SYN** scan riporta **reset** mentre la **TCP connect** riporta **conn-refused**.
- **Completamento connessione**: La **SYN** scan non completa il **three-way handshake** (più stealth), la **TCP connect** invece lo completa.
- **Privilegi richiesti**: La **SYN** scan richiede privilegi **root**, la **TCP connect** può essere eseguita da utenti normali.
- **Porte rilevate**: Entrambe hanno identificato le stesse **23** porte aperte.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 05:25 EST
Nmap scan report for 192.168.51.101
Host is up (0.017s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
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

Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
```

Service Version Detection

La **service version detection** è stata eseguita con il comando `nmap -sV 192.168.51.101` per identificare i servizi in ascolto sulle porte aperte e le loro versioni specifiche.

Questo sarà utile per l'identificazione di eventuali vulnerabilità note.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 05:26 EST
Nmap scan report for 192.168.51.101
Host is up (0.014s 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?
25/tcp   open  smtp?
53/tcp   open  domain       ISC BIND 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
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?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
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        Apache Jserv (Protocol v1.3)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: 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 193.28 seconds
```

Conclusione

Le scansioni effettuate hanno permesso di mappare completamente la superficie di attacco del target **Metasploitable**. Il sistema esegue **Linux Debian/Ubuntu** e presenta **23** servizi esposti, molti dei quali utilizzano versioni obsolete e vulnerabili.

Il confronto tra **SYN** scan e **TCP connect** scan ha evidenziato che entrambe le tecniche rilevano le stesse porte aperte, ma differiscono nel metodo: la **SYN** scan è più stealth e non completa le connessioni TCP, mentre la **TCP connect** è più invasiva ma non richiede privilegi elevati. La presenza di numerosi servizi legacy e versioni software datate conferma la natura volutamente vulnerabile della macchina **Metasploitable**, progettata per scopi didattici di penetration testing.