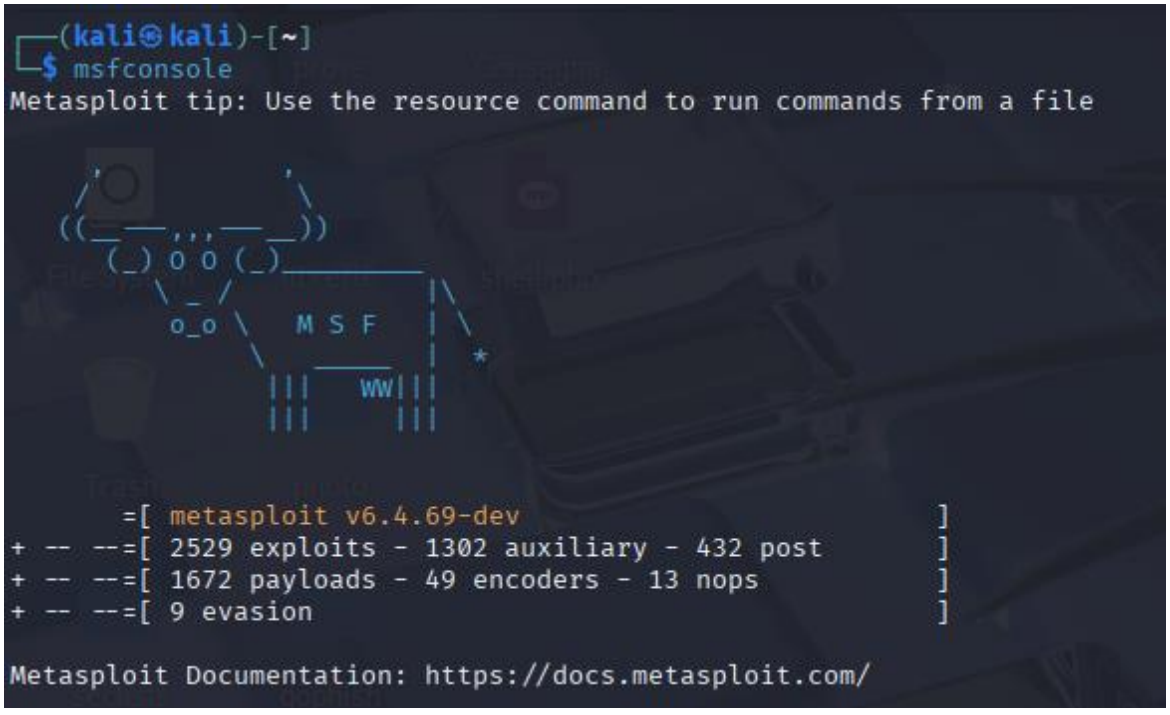
PRATICA S7L2

Traccia: Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40

Fase 1 - Avvio di Metasploit su Kali Linux

Ho aperto il terminale sulla mia macchina Kali Linux e ho avviato il Metasploit Framework digitando msfconsole. Dopo qualche secondo, è comparso il classico ASCII art della mucca con la scritta "MSF", seguita dalle informazioni sulla versione e sulle statistiche del framework.



Fase 2 - Ricerca e selezione del modulo di scansione porte

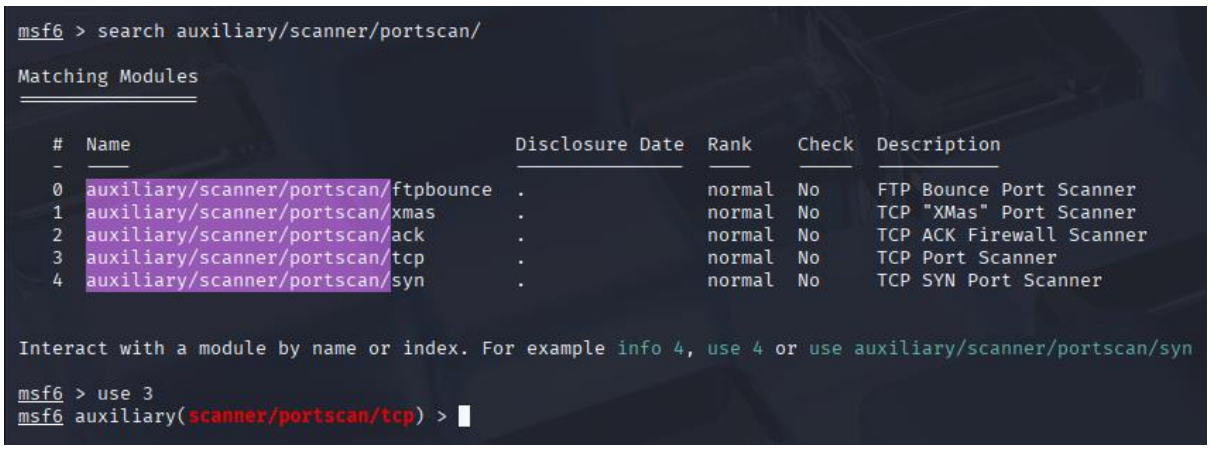
Una volta avviato Metasploit, ho iniziato la fase di ricognizione. Ho cercato i moduli di tipo *auxiliary scanner* dedicati alla scansione delle porte con il comando:

- search auxiliary/scanner/portscan/

Dopo aver valutato le opzioni, ho deciso di utilizzare il modulo **TCP Port Scanner**, che corrispondeva al numero 3 nella lista. Ho quindi eseguito:

- use 3

Questo modulo mi permette di effettuare una scansione diretta delle porte TCP su un target specifico, utile per identificare servizi attivi e potenziali vettori di attacco.



Fase 3 - Configurazione ed esecuzione del modulo scelto

Ho eseguito info -d per visualizzare i dettagli del modulo. Ho studiato le opzioni disponibili, tra cui:

- RHOSTS: host target
- PORTS: intervallo di porte da analizzare
- THREADS: numero di thread concorrenti
- TIMEOUT: timeout di connessione

Il modulo è pensato per identificare servizi TCP attivi.

Ho configurato il modulo per eseguire una scansione sulle porte da 1 a 23 del target 192.168.50.102:

- set RHOSTS 192.168.50.102
- set PORTS 1-23

Questa configurazione mi ha permesso di focalizzarmi sui servizi più comuni, come FTP, SSH e Telnet.

```
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.50.102
RHOSTS => 192.168.50.102
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-23
PORTS => 1-23
msf6 auxiliary(scanner/portscan/tcp) > info

       Name: TCP Port Scanner
     Module: auxiliary/scanner/portscan/tcp
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>
  kris katterjohn <katterjohn@gmail.com>

Check supported:
  No

Basic options:
  Name         Current Setting  Required  Description
  ----         ---------------  --------  -----------
  CONCURRENCY  10               yes       The number of concurrent ports to check per host
  DELAY        0                yes       The delay between connections, per thread, in milliseconds
  JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
  PORTS        1-23             yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS       192.168.50.102   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  THREADS      1                yes       The number of concurrent threads (max one per host)
  TIMEOUT      1000             yes       The socket connect timeout in milliseconds

Description:
  Enumerate open TCP services by performing a full TCP connect on each port.
  This does not need administrative privileges on the source machine, which
  may be useful if pivoting.


View the full module info with the info -d command.
```

Ho avviato la scansione e il modulo ha identificato tre porte aperte sul target:

- **Porta 21** – FTP
- **Porta 22** – SSH
- **Porta 23** – Telnet

La scansione è stata completata con successo su un host. Queste informazioni mi permettono di pianificare le prossime fasi dell'attacco, come l'enumerazione dei servizi o la ricerca di exploit specifici.

```
msf6 auxiliary(scanner/portscan/tcp) > run
[+] 192.168.50.102         - 192.168.50.102:21 - TCP OPEN
[+] 192.168.50.102         - 192.168.50.102:22 - TCP OPEN
[+] 192.168.50.102         - 192.168.50.102:23 - TCP OPEN
[*] 192.168.50.102         - Scanned 1 of 1 hosts (100% complete
[*] Auxiliary module execution completed
```

Fase 4 - Analisi Telnet con Metasploit

Confermata l'apertura della porta Telnet, ho proseguito caricando il modulo auxiliary/scanner/telnet/telnet_version, progettato per rilevare il **banner del servizio Telnet**. Questo passaggio è fondamentale per identificare la versione del software in uso e valutare eventuali vulnerabilità note.

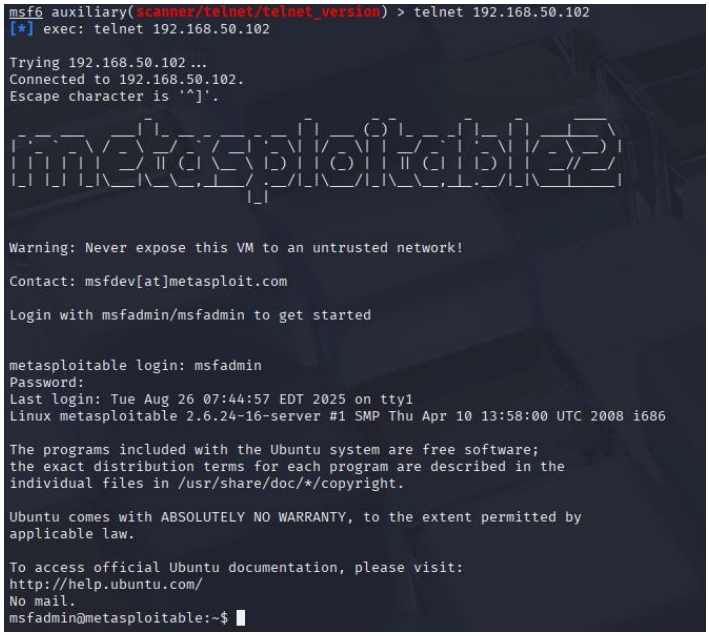
```
msf6 > search auxiliary/scanner/telnet/telnet_version

Matching Modules
================

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/telnet_version  .                normal  No     Telnet Service Banner Detection


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version

msf6 > use 0
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Ho impostato RHOSTS sul target e verificato le opzioni disponibili (RPORT, TIMEOUT, THREADS), lasciando i valori di default per una scansione semplice e diretta. Il modulo ha eseguito correttamente il rilevamento, fornendo informazioni utili per le fasi successive di exploit.

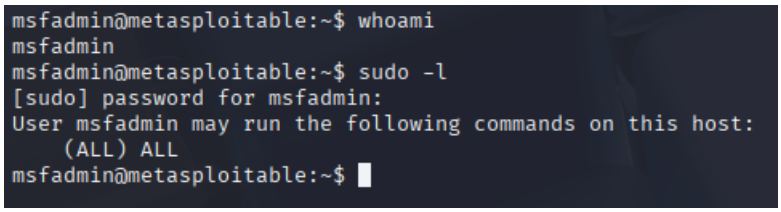
Fase 5 - Accesso remoto e privilege escalation su Metasploitable2

ho utilizzato il modulo auxiliary/scanner/telnet/telnet_version per rilevare il banner del servizio e confermare la presenza del demone Telnet attivo su **192.168.50.102**.

A quel punto, ho stabilito una connessione diretta via Telnet e ho effettuato l'autenticazione con le credenziali predefinite **msfadmin:msfadmin**, ottenendo accesso alla macchina **Metasploitable2.**



Una volta dentro, ho eseguito whoami per confermare l'identità dell'utente e sudo -l per verificare i privilegi. Il risultato ha mostrato che l'utente **msfadmin** può eseguire **qualsiasi comando come root**, aprendo la strada a una **privilege escalation completa**. Questo accesso amministrativo rappresenta un punto cruciale nel processo di compromissione, permettendo il controllo totale del sistema target.



Conclusione dell'esercizio

L'esercizio ha mostrato come, partendo da una semplice scansione TCP, sia stato possibile identificare servizi attivi, accedere via Telnet alla macchina Metasploitable2 e ottenere privilegi amministrativi. Questo scenario evidenzia l'importanza della protezione dei servizi esposti e della gestione sicura delle credenziali, offrendo un esempio pratico di compromissione in ambiente controllato.