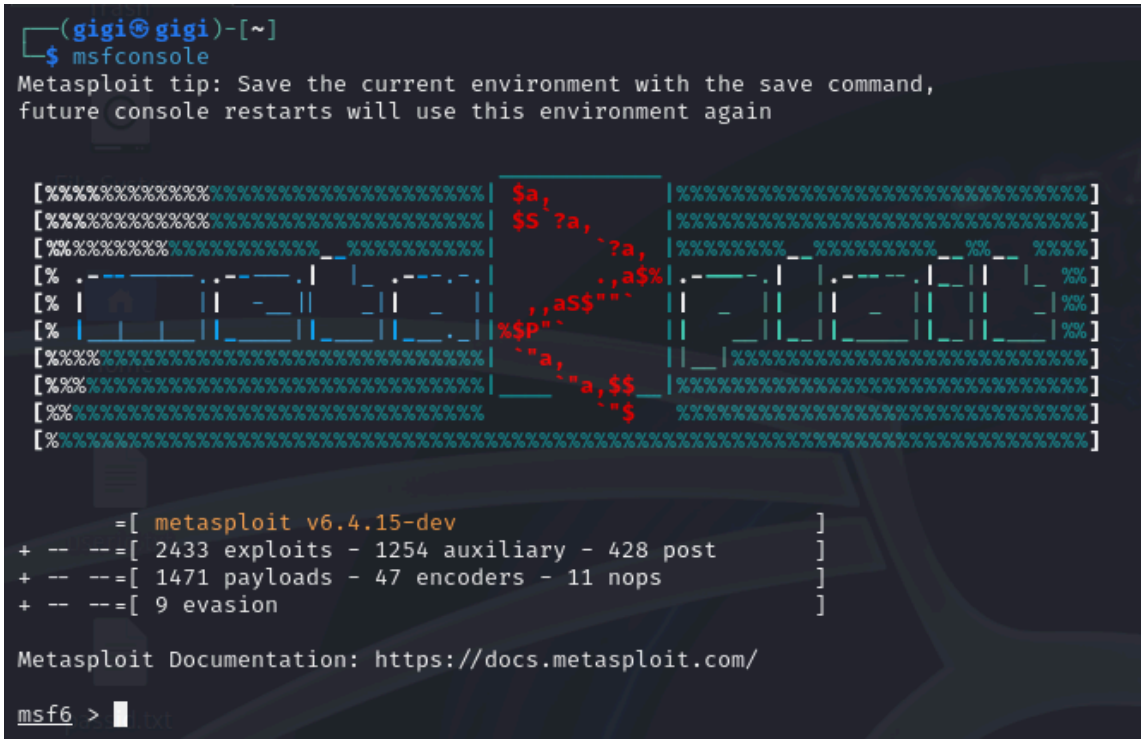
EXPLOIT TELNET CON MSFCONSOLE

Marco Malizia, 09.07.2024

Macchine utilizzate: Kali Linux - Metasploitable2

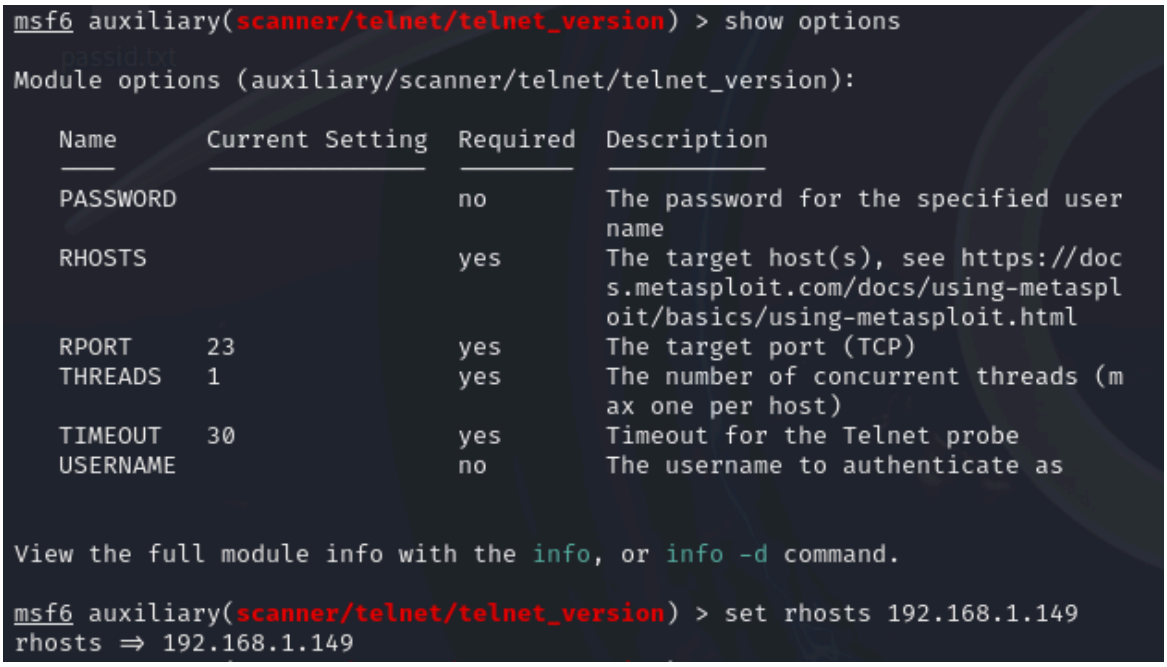
Configurazione rete interna con IP Kali (192.168.1.150) e Meta (192.168.1.149)

- Avviare MSFCONSOLE sul terminal di Kali



- Eseguendo il comando <search telnet _version> andiamo a filtrare la ricerca per ottenere risultati piu' vicini possibili alle nostre necessita', selezioniamo il secondo risultato visto che rappresenta esattamente cio' che stiamo cercando.

- Dopo aver impostato il modulo eseguiamo <show options> per visualizzare a schermo i dati richiesti. Come possiamo vedere e' richiesto anche l'indirizzo IP del target, percio' eseguiamo <set rhost IPTARGET> che in questa situazione e' quello appartenente alla macchina Metasploit, ovvero 192.168.1.149.



- Ora che abbiamo inserito tutti i dati richiesti, possiamo eseguire il comando <run> oppure <exploit> e come vediamo dallo screenshot, abbiamo ottenuto cio' che cercavamo, le credenziali per poter accedere al portale tramite telnet.

- Eseguendo il comando <telnet 192.168.1.149> possiamo accedere al portale di login di Metasploit, dove inserendo le credenziali trovate prima con MSFCONSOLE possiamo accedere.