PROGETTO S7-L2

SCOPO: Usare Metasploit per sfruttare la vulnerabilità relativa a Telnet sulla macchina Metasploitable.configurando l'IP di kali con 192.168.1.25 e l'IP della di Metasploitable con 192.168.1.40 .

Prima di passare alla fase Applicativa prendiamo un pò di tempo per capire che cosa è Metasploit e che cosa è Telnet.

1-) Metasploit

È un framework open-source usato per il penetration testing e lo sviluppo di exploit.fornisce una vasta gamma di exploit(quasi 2000) e numerosi vettori di attacco che possono essere utilizzati contro diversi sistemi e technologie. Può anche essere utilizzato per creare ed automatizzare i propri exploit.

Metasploit fornisce anche una gamma di 600 payload,que sono porzione di codice o dati all'interno di un pacchetto di dati o di un programma che esegue una specifica azione quando attivo.

2-) Telnet

È uno dei servizi attivi su Metasploitable, è un protocolo che consente di stabilire una connessione remota a un dispositivo per interagire con esso tramite la linea di comando.

A come scopo di inviare informazioni,comprese le credenziali di acceso,in modo non crittografatto. E questo lo rendo vulnerabile agli attacchi di intercettazione e sniffing.

PROGETTO S7-L2

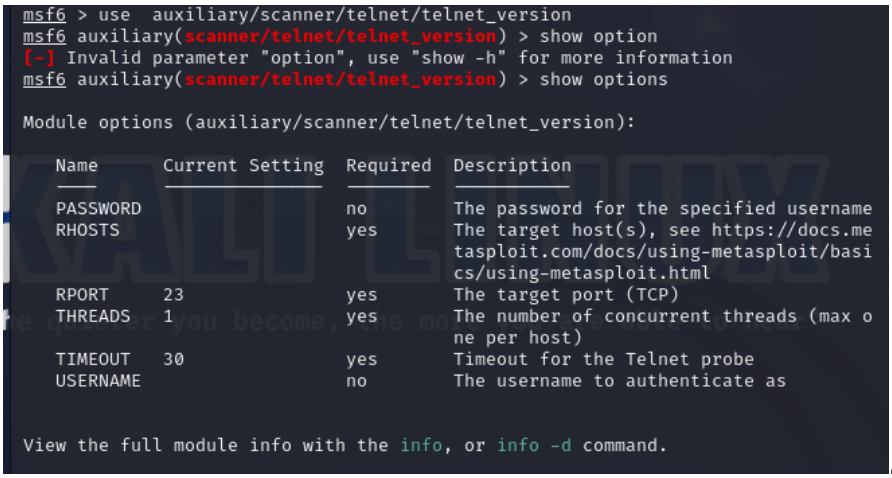
3-) Fase di Applicazione

In questa fase descriviamo come abbiamo processo per sfruttare il servizio vulnerabile Telnet

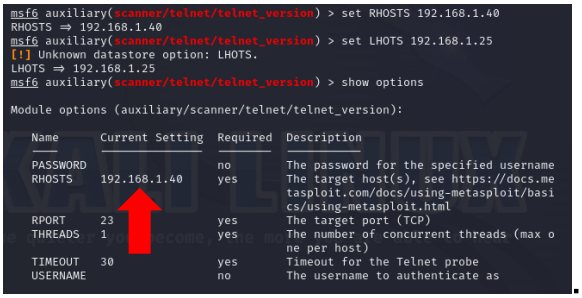
Abbiamo attivato la console di Metasploit con il comando msfconsole,

Poi abbiamo avviato la ricerca con il comando search telnet_version.

Di seguito abbiamo usato il comando use seguide del path di telnet,per usare il payload di telnet. E poi inserendo show options per gli opzioni e abbiamo ottenuto il risultato seguente.



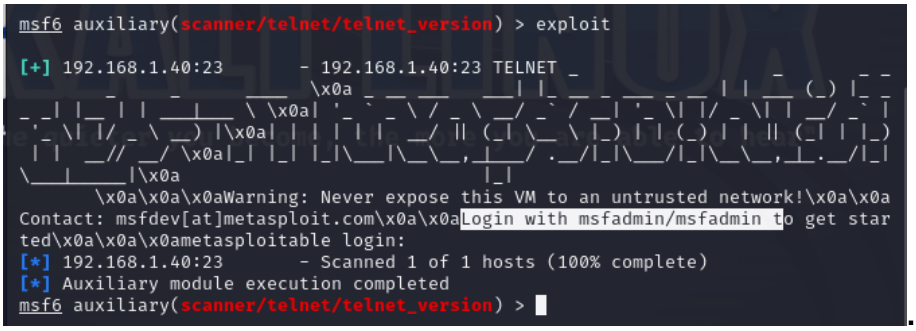
Dopo questo abbiamo inserito l'indirizzo IP di Metasploitable usando il comando set seguito dell'indirizzo IP di Metasploitable. E abbiamo ottenuto il risultato che segue:



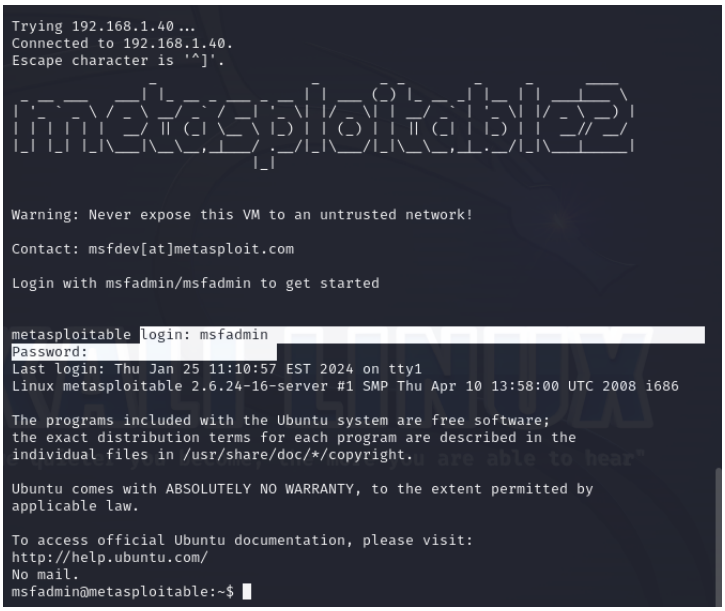
Possiamo vedere qui che l'indirizzo IP è ben stato inserito come indicato con la freccia rossa.

PROGETTO S7-L2

Poi abbiamo ibserito il comando exploit per avviare l'attaco e abbiamo ottenuto gli informazione di login(username e password) , che possiamo vedere indicato con la banda bianca qua sotto.

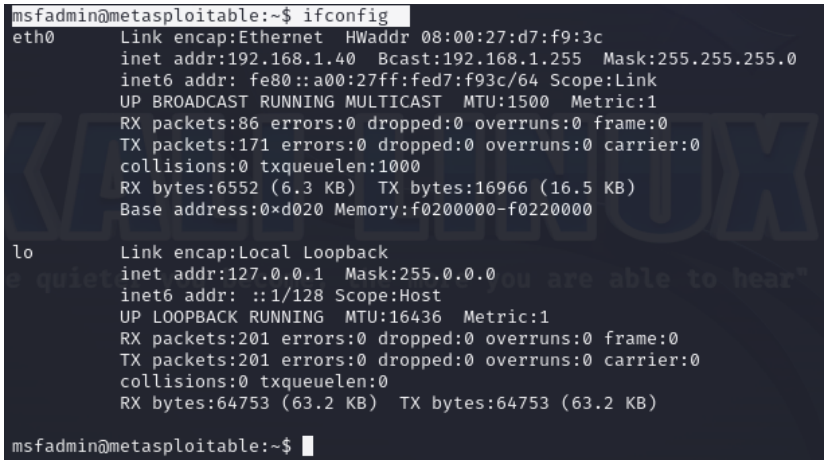


Poi inserendo il comando telnet seguito dall'indirizzo IP di Metsploitable ci esce la schermata principale della macchina metasploitable dove inserire le credenziale e dopo aver inserito le credenziale otteniamo la schermata che segue:



PROGETTO S7-L2

Inserendo il comando ifconfig otteniamo gli informazioni di rete della macchina Metasploitable come segue:



E a questo punto possiamo dire che l'attacco è andato a buon fine.