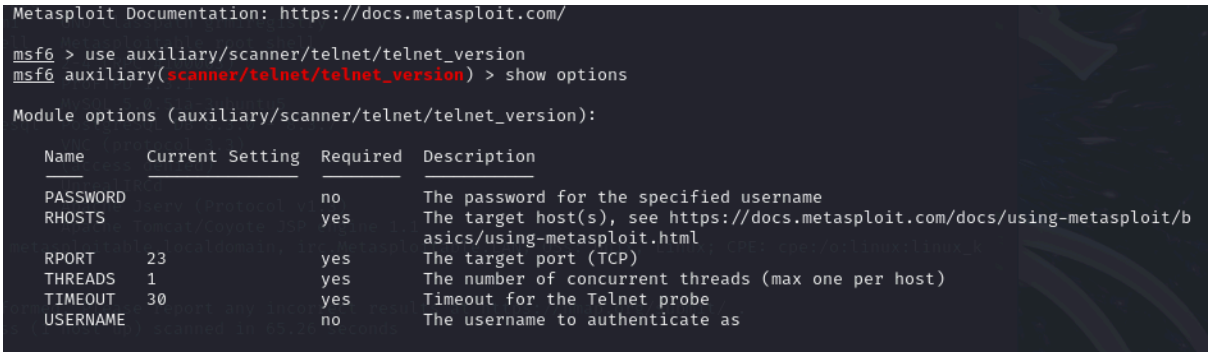
EXPLOIT SU PROTOCOLLO TELNET

Traccia: Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Svolgimento:
L'esercizio di oggi è analogo a quello eseguito ieri, si chiede l'utilizzo di Metasploit per andare ad attaccare Metasploitable2 tramite protocollo Telnet, ovvero un protocollo non criptato che consente di utilizzare un dispositivo da remoto.
Protocollo Telnet su Metasploit
Per prima cosa, si va a verificare che il dispositivo attaccante Kali Linux comunichi correttamente con quello Metasploitable, dopo aver verificato ciò andrò ad eseguire il comando nmap:

nmap -sV 192.168.1.247

Tramite questo comando potremo andare a verificare quali porte sono aperte sul dispositivo in questione per andare ad individuare se la porta 23 è aperta e quindi è possibile effettuare l'attacco con successo.
Andremo ad attivare Metasploit sulla macchina Kali Linux per andare ad attivare l'exploit interessato.



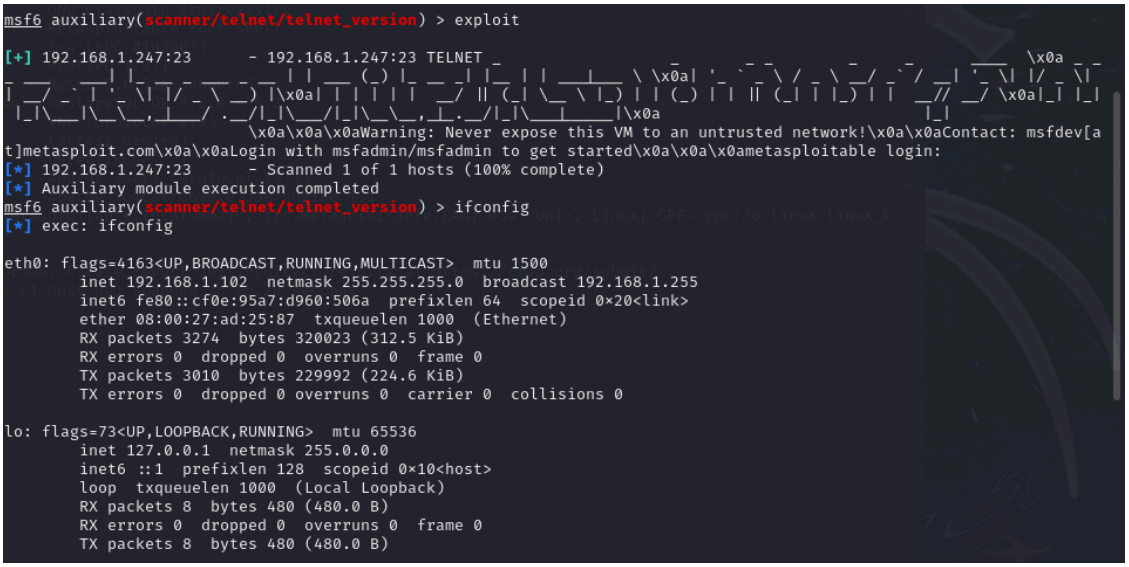
Questo sarà il modulo ausiliare che andremo ad utilizzare per utilizzare il protocollo Telnet su Metasploitable.
I moduli ausiliari hanno la funzione di effettuare attacchi non diretti alla macchina bersaglio, ed hanno l'utilità di raccogliere informazioni per effettuare attacchi mirati e più precisi.

Il prossimo passo sarà quello di settare le impostazioni tramite il comando:

set RHOSTS 192.168.1.247

Avvio attacco

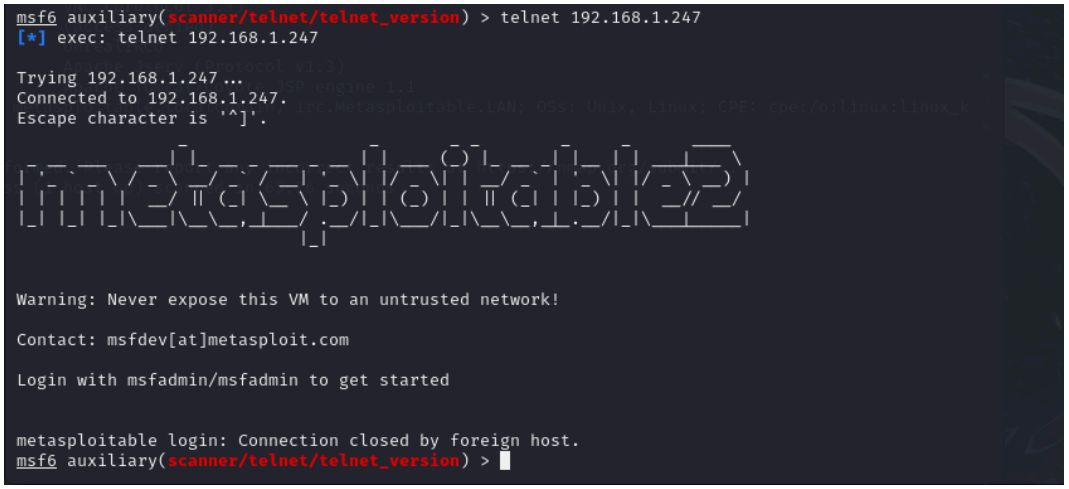
Dopo aver settato l'attacco sulla macchina interessata, andremo ad avviarlo per scoprire le credenziali di accesso della macchina bersaglio.



Da notare come con ifconfig risulteremo ancora all'interno della macchina Kali, ma conosceremo le credenziali per accedere alla macchina Metasploitable.

Per avviare il protocollo telnet invieremo il comando:

telnet 192.168.1.247



Adesso Metasploit ci ha consentito di entrare nell'interfaccia grafica di Metasplooitable2 e potremo eseguire le operazioni come se fossimo su quel dispositivo.

Conclusioni

L'attacco eseguito con Metasploit contro il protocollo Telnet ha il fine di accedere senza autorizzazioni all'interno della macchina bersaglio e ne consente il controllo da remoto, il protocollo Telnet è considerato una vulnerabilità piuttosto grave in quanto, non essendo criptato, trasmette i dati in chiaro, compresi username e password.

Progetto a cura di
Sonia Laterza