Esercizio S7L2

Traccia:

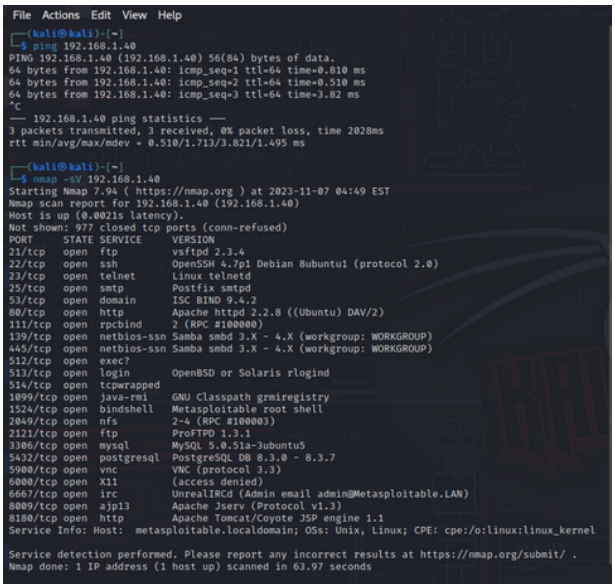
Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito: Configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40.
Mettere tutto su un report, spiegare cosa si intende per exploit, cos'è il protocollo attaccato, i vari step.

1) Per Exploit s'intende un codice malevolo che va a sfruttare le vulnerabilità del codice o del software.
Per Malware s'intende un codice malevolo che crea problemi al dispositivo o al software.

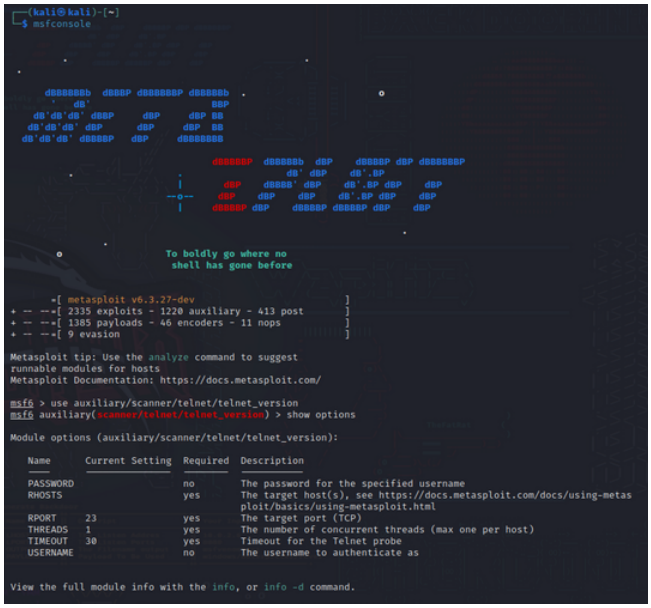
La differenza tra i due è che l'exploit non ha bisogno dell'interazione dell'uomo dato che la vulnerabilità è già presente nel codice o nel software invece il malware ha bisogno dell'interazione dell'uomo per poter iniziare ad infettare.

2) Il protocollo attaccato è il Telnet è quel protocollo che ci permette di connetterci e di communicare con un altro dispositivo da remoto.



3) si va a vedere se le due macchine communicano,si fa una scansione con nmap per vedere la versione del protocollo che effettueremo l'attacco

Si avvia Metasploit



Si cerca il servizio da fare l'exploit, controlliamo le opzioni necessarie per vedere se abbiamo inserito tutti i parametri necessari.

In questo caso l'unico parametro richiesto che mancava era l'RHOSTS.

quindi si va a settare per l'RHOSTS l'indirizzo IP della vittima cioè Windows XP.

si rifà il controllo dei parametri necessari

Poi è possibile effettuare l'exploit

Da qui si può vedere l'username e la password per accedere a Telnet

si fa un controllo se l'exploit è andato a buon fine inserendo l'username e la password trovati con l'exploit

come si può vedere mi ha permesso di accedere alla schermata della vittima in questo caso Metasploitable