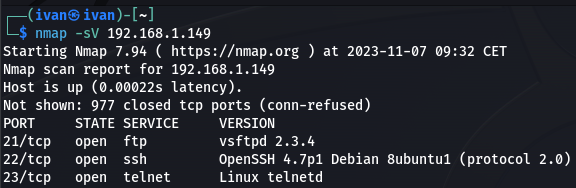
**EXPLOIT TELNET CON METASPLOIT**

**TRACCIA**  
1) Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet\_version sulla macchina Metasploitable.  
2) Mettere tutto su un report, spiegare cosa si intende per exploit, cos’è il protocollo attaccato, i vari step.

**LEGENDA**

**Exploit**: Un exploit è un attacco che sfrutta le vulnerabilità già presenti in un software. L'attacco è composto da 3 fasi:  
1) **Exploit** consiste nell’atto vero e proprio di bucare un dispositivo.  
2) **Payload** è il codice contenuto nell’exploit utile a creare una connessione (Shell) con la macchina vittima.  
3) **Shell** (**Bind o Reverse**) è la connessione vera e propria; può essere di due tipi: Bind e Reverse.  
Bind parte dall’attaccante, Reverse dalla vittima.  
L’obiettivo è quello di acquisire il controllo di un dispositivo e rubare i dati memorizzati su una rete.  
Si differenzia tra modulo normale e modulo ausiliario:  
1a) I moduli normali in Metasploit sono progettati per eseguire attacchi diretti su vulnerabilità specifiche.   
1b) I moduli normali vengono utilizzati principalmente per eseguire attacchi diretti e sfruttare le vulnerabilità con l'obiettivo di ottenere l'accesso al sistema di destinazione.  
1c) Utilizzano un payload.  
2a) I moduli ausiliari in Metasploit sono progettati per svolgere funzioni di supporto durante il test della sicurezza, come la scansione della rete, la raccolta di informazioni e altro ancora. Non eseguono necessariamente attacchi diretti, ma forniscono informazioni e supporto aggiuntivi che possono essere utili per ottenere un quadro completo della sicurezza della rete o del sistema.  
2b) Quasi mai utilizzano un payload.  
 **TELNET**: Un protocollo di rete utilizzato per stabilire una connessione remota con un dispositivo o un server su una rete. Questa connessione permette ad un utente di controllare e interagire con il dispositivo remoto da un computer locale.  
Con NMAP abbiamo scansionato tutte le porte aperte su Metasploitable, incluse anche le versioni del loro servizio.  
Troviamo la porta 23 Telnet, quella che utilizzeremo per l’exploit.



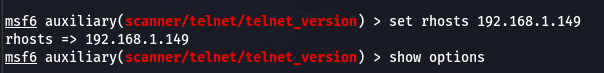
Avviamo Metasploit (software per la gestione di exploit) tramite il comando “msfconsole” e tramite il comando “search” andiamo a trovare l’exploit utile a bucare quel servizio.

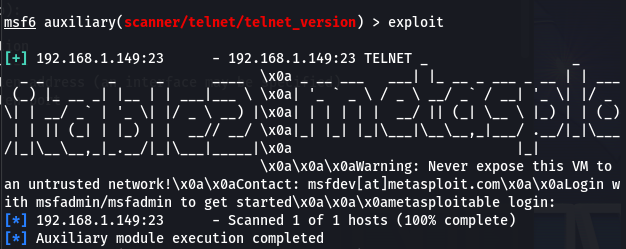
Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente

Successivamente, tramite il comando “use”, impostiamo l’exploit ausiliario.  
Questo non avrà bisogno di un payload.  
Tramite il comando “show options” notiamo tutti i parametri che ci servono per poter avviare l’attacco. In questo caso, l’unico parametro mancante è l’ip della macchina vittima. Lo andiamo ad impostare col comando “set rhosts” e facciamo un secondo check per verificare che sia tutto corretto.





Ora è tutto pronto, eseguiamo l’attacco tramite il comando “exploit”.  
Una volta completato, l’exploit ci fornirà le credenziali per poterci connettere alla macchina vittima



Infine andiamo ad eseguire il comando “telnet” su un nuovo terminale ed accediamo con le credenziali fornite dall’exploit. Siamo dentro e possiamo controllare Metasploitable tramite Telnet.

