Exploit Telnet con Metasploit

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 dell'esercizio

Passo 1: Avvio di Metasploit

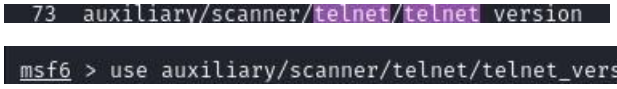
Il primo passo è avviare Metasploit. Questo può essere fatto tramite il comando msfconsole nel terminale. Una volta avviato, ci si trova all'interno dell'interfaccia di Metasploit, pronti per eseguire comandi.

Passo 2: Ricerca del Modulo Telnet

Utilizzando il comando **search telnet**, si cerca il modulo appropriato per la scansione Telnet.

Passo 3: Selezione del Modulo Telnet

Dopo aver identificato il modulo desiderato, si utilizza il comando **use auxiliary/scanner/telnet/telnet_version** per selezionare il modulo di scansione Telnet.



Passo 4: Configurazione delle Opzioni

Prima di eseguire la scansione, è necessario configurare le opzioni del modulo. Utilizzando il comando **show options**, si visualizzano le opzioni disponibili.

La principale opzione da configurare è **RHOSTS**, che specifica l'indirizzo IP del target. In questo caso, l'indirizzo IP che utilizzeremo è **192.168.40.101**.

Il comando **set RHOSTS 192.168.40.101** imposta questa opzione.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.40.101
RHOSTS ⇒ 192.168.40.101
```

Passo 5: Esecuzione della Scansione

Una volta configurato il modulo, si esegue la scansione con il comando **exploit** così da ottenere le credenziali di accesso di **metaspoitable**.

Passo 6: Esecuzione del comando telnet

Utilizzando il comando telnet seguito dall'IP del target, entreremo al suo interno e potremo inserire le credenziali di accesso ottenute in precedenza.