Login Metasploitable

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.

msfconsole e auxiliary telnet_version

User/Password e Login

Relazione

Il compito di oggi prevedeva di effettuare un attacco alla macchina Metasploitable sfruttando la vulnerabilità del servizio Telnet sulla porta 23.

1. Ho avviato Metasploit con il comando: msfconsole.
2. Successivamente, ho utilizzato il modulo use auxiliary/scanner/telnet/telnet_version per scansionare il servizio Telnet.
3. Ho impostato il target con il comando set RHOSTS 192.168.1.149.
4. Dopo aver trovato un nome utente e una password validi, ho aperto una connessione Telnet per verificare le credenziali con il comando: telnet 192.168.1.149 23 (inserendo l'IP e la porta).
5. Inserendo il nome utente e la password recuperati, sono riuscito ad accedere al sistema.

Questo mi ha permesso di confermare l'efficacia dell'attacco e dimostrare la vulnerabilità di Telnet a un attacco di brute-force, consentendo un accesso non autorizzato alla macchina Metasploitable.

Daniel_Gabriel_Costeanu