Obiettivo

Utilizzare Metasploit per sfruttare la vulnerabilità relativa al servizio Telnet presente sulla macchina Metasploitable.

Passaggi eseguiti

1. **Configurazione IP**
    - Kali Linux: 192.168.1.25/24 (rete interna)
    - Metasploitable: 192.168.1.40/24 (rete interna)
2. **Verifica connessione**
    - Ping riuscito da Kali a Metasploitable.
3. **Scansione con Metasploit**
    - Avviato `msfconsole`
    - Usato modulo `auxiliary/scanner/telnet/telnet_version` per verificare la presenza del servizio Telnet sulla porta 23 di Metasploitable.
    - Il modulo ha correttamente mostrato il banner di login Telnet.
4. **Login Telnet**
    - Utilizzato il modulo `auxiliary/scanner/telnet/telnet_login` con username e password di default `msfadmin/msfadmin`.
    - Login effettuato con successo.
    - Apertura di una sessione shell interattiva sulla macchina Metasploitable.
5. **Verifica shell**
    - Comando `whoami` restituisce `msfadmin`, confermando l'accesso come utente remoto.