Pratica S7/L2

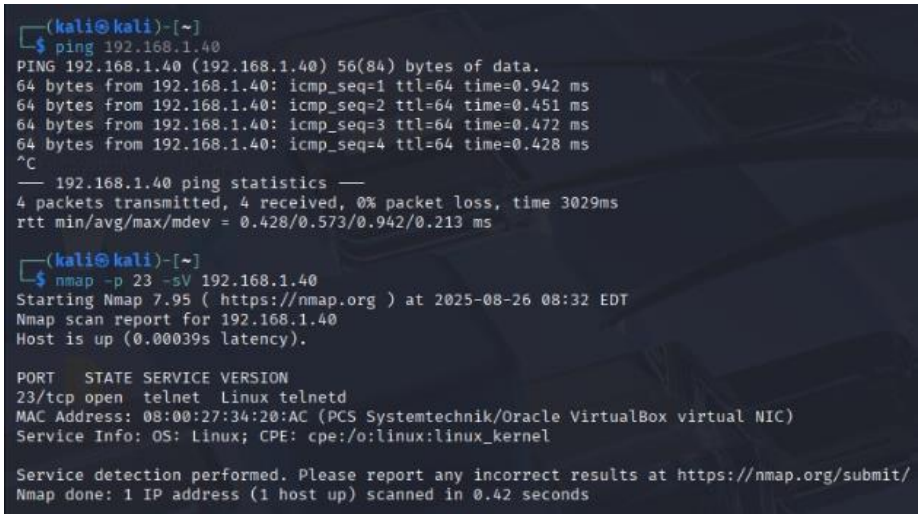
Introduzione: l'obiettivo di questo esercizio era eseguire un penetration testing svolto a testare la sicurezza del servizio Telnet su una macchina virtuale Metasploitable2 e di mostrare la capacità di un attaccante di raccogliere informazioni critiche e ottenere un accesso non autorizzato sfruttando le configurazioni deboli.

Configurazione del laboratorio:

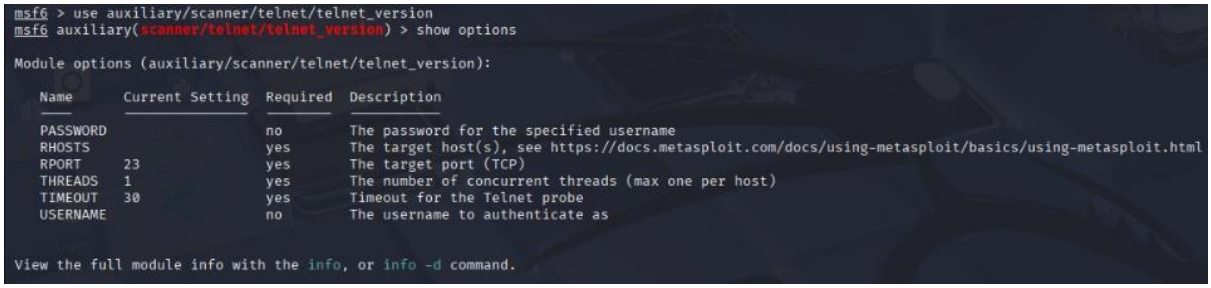
- Kali Linux IP: 192.168.1.150 (macchina attaccante)
- Metasploitable2 IP: 192.168.1.149 (macchina bersaglio)

Fase di attacco

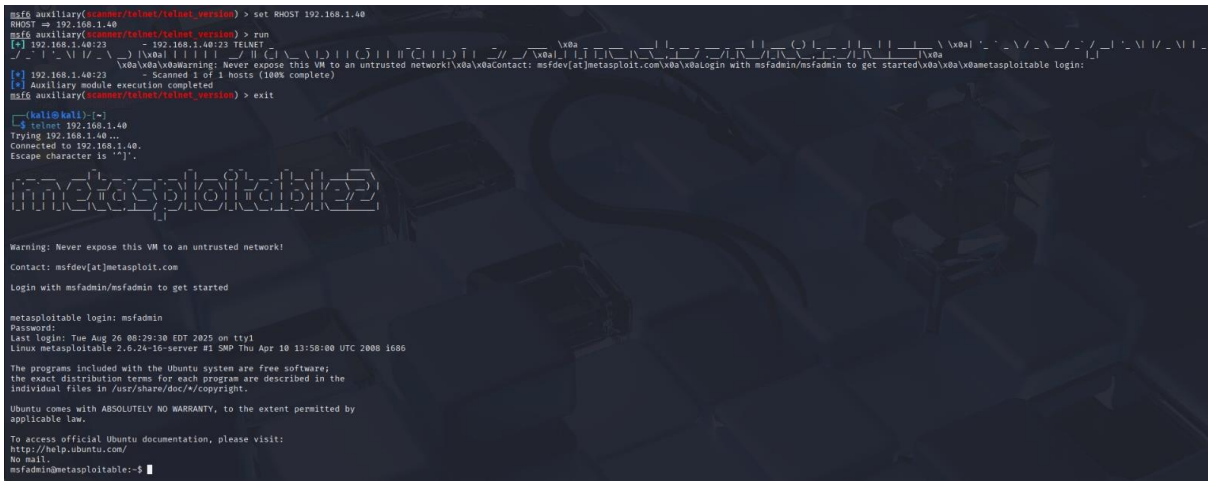
Il primo passo è stato verificare la connettività tra le due macchine e eseguire una scansione nmap sulla porta 23.



La fase di attacco è iniziata avviando la console di Metasploit per utilizzare il modulo "auxiliary/scanner/telnet/telnet_version", ovvero un modulo progettato per scansionare e raccogliere informazioni dai servizi Telnet.



Dopo aver configurato l'indirizzo IP del bersaglio con il comando "set RHOST", il modulo è stato eseguito. La scansione ha avuto successo, rilevando le credenziali predefinite del servizio Telnet che erano state lasciate senza modifiche sulla macchina Metasploitable2.



Conclusioni: l'esercizio ha dimostrato che un servizio Telnet configurato in modo debole rappresenta un grave rischio per la sicurezza. L'uso di credenziali predefinite e la mancanza di crittografia (Telnet invia i dati in chiaro) rendono il servizio un obiettivo facile per gli attaccanti.

Raccomandazioni:

- **Disattivare i servizi non necessari**: Se il servizio Telnet non fosse essenziale, dovrebbe essere disattivato per ridurre la superficie d'attacco.
- **Utilizzare protocolli sicuri**: Sostituire Telnet con alternative crittografate come SSH (Secure Shell), che cifra i dati di autenticazione e la sessione.
- **Gestione delle credenziali**: Modificare sempre le credenziali predefinite su qualsiasi servizio installato e utilizzare password complesse.
- **Principio del privilegio minimo**: Assicurarsi che i servizi di rete siano eseguiti con il minor numero di privilegi possibile.