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.

Requisito: Seguire gli step visti in lezione teorica.

Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40

Introduzione

In questo esercizio, oltre a identificare la versione di Telnet in esecuzione sulla macchina **Metasploitable** tramite Metasploit, abbiamo esteso l'attività cercando di ottenere l'accesso alla macchina sfruttando la vulnerabilità del servizio **Telnet**. Questo tipo di vulnerabilità può essere particolarmente pericoloso se il servizio è configurato in modo insicuro, come nel caso di Telnet che non richiede una password robusta o non ha meccanismi di protezione adeguati. L'obiettivo finale dell'esercizio è stato sia quello di determinare la versione di Telnet sulla macchina di destinazione, sia quello di recuperare la password per accedere al sistema.

Conclusioni

In questo esercizio abbiamo esplorato come sfruttare una vulnerabilità di Telnet su una macchina vulnerabile, utilizzando il framework **Metasploit** per raccogliere informazioni sulla versione del servizio Telnet e, successivamente, tentare di recuperare la password tramite un attacco di brute force.

Abbiamo visto che la macchina **Metasploitable** è configurata in modo insicuro, con credenziali di default come `msfadmin:msfadmin`, che possono essere facilmente recuperate. Questo tipo di vulnerabilità rappresenta un rischio significativo se Telnet è lasciato esposto su sistemi reali, poiché potrebbe permettere un attacco remoto da parte di un aggressore.

L'esercizio ci ha aiutato a comprendere l'importanza di configurare correttamente i servizi e di utilizzare meccanismi di protezione, come l'autenticazione forte e la disabilitazione di servizi non sicuri come Telnet, per migliorare la sicurezza dei sistemi.