ESERCIZIO S7/L2

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

In questo esercizio, l'obiettivo è utilizzare Metasploit, una delle più potenti piattaforme di penetration testing, per sfruttare una vulnerabilità nel servizio Telnet presente sulla macchina virtuale Metasploitable.

Telnet è un protocollo di rete non sicuro per il login remoto che è vulnerabile a diverse minacce, come l'intercettazione delle credenziali in chiaro.

Una volta creato l'ambiente di lavoro avviando la macchina di Metasploitable e messa in comunicazione con la macchina attaccante Kali, ho avviato Metasploit su Kali con il comando << msfconsole >>.

Poi ho cercato il modulo ausiliare con il comando << serach telnet_version >>. I moduli ausiliari in Metasploit sono progettati per svolgere funzioni di supporto durante il test della sicurezza, eseguono funzioni di supporto come la scansione della rete, la raccolta di informazioni e altre attività non direttamente offensive. Utilizzati principalmente per attività di ricognizione e raccolta dati, che possono essere fondamentali per pianificare attacchi più mirati e precisi.

La differenza chiave rispetto ai moduli normali è che i moduli ausiliari sono progettati per supportare i test di sicurezza attraverso la raccolta di informazioni e la scansione, piuttosto che eseguire attacchi diretti.

```
search telnet_versiomsf6 > search telnet_version

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version  .                normal  No     Lantronix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version            .                normal  No     Telnet Service Banner Detection


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version

msf6 > use auxiliary/scanner/telnet/lantronix_telnet_version
```

Dalla ricerca otteniamo due opzioni, in questo caso ho scelto la numero 0 auxiliary/scanner/telnet/lantronix_telnet_version e lo selezioniamo con il comando << use >>.

Impostiamo indirizzo IP target, con << set RHOSTS 192.168.1.149 >> e lanciamo con exploit.
Meterpreter mette a disposizione degli script da utilizzare per recuperare determinati dati sul bersaglio con il comando << run >>.