ESERCIZIO TEST METASPLOIT

Traccia: Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet\_version sulla macchina Metasploitable. Requisito: Configurate l’ip della vostra Kali con 192.168.1.25 e l’ip della vostra Metasploitable con 192.168.1.40. Mettere tutto su un report, spiegare cosa si intende per exploit, cos’è il protocollo attaccato, i vari step.

Traccia: Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet\_version sulla macchina Metasploitable. Requisito: Configurate l’ip della vostra Kali con 192.168.1.25 e l’ip della vostra Metasploitable con 192.168.1.40. Mettere tutto su un report, spiegare cosa si intende per exploit, cos’è il protocollo attaccato, i vari step.

EXPLOIT :

Un exploit è un pezzo di codice o una tecnica che sfrutta una vulnerabilità presente in un software o in un sistema per ottenere un accesso non autorizzato o per eseguire codice malevolo su di esso.

Si divide in tre fasi:

exploit (l’atto di penetrare in un sistema informatico)

payload (codice contenuto nell’exploit per creare una shell con la macchina vittima)

shell (connessione vera e propria che collega le macchine, può essere bind o reverse)

i moduli degli exploit si dividono in moduli normali e ausiliari

moduli normali: sfruttano il payload, perché lo scopo principale è quello di ottenere il controllo della macchina

moduli ausiliari: non usano quasi mai il payload, lo scopo principale non è di ottenere il controllo della macchina, bensì le informazioni, supporto, scansione

TELNET:

l protocollo Telnet è un protocollo di rete che consente di stabilire una connessione remota tra due computer tramite una rete.

STEP DELL’ATTACCO:

per prima cosa abbiamo configurato la macchina virtuale metasploitable come richiesto dalla traccia,

ci siamo assicurati che le due macchine comunicassero tramite ping e abbiamo iniziato l’esercizio.

Successivamente tramite nmap abbiamo scansionato la macchina metasploitable con il comando nmap -sV

Trovandoci tutte le porte aperte, servizi e versioni del software. Il risultato ottenuto è il seguente

A computer screen shot of a computer

Description automatically generated

Ora che abbiamo queste informazioni possiamo avviare l’exploit usando metasploit

Con msfconsole avviamo il servizio e con il comando use seguito da auxiliary/scanner/telnet/telnet\_version (exploit fornito da consegna)

Una volta scelto l’exploit lo andiamo a configurare con il comando show option. Andranno configurati tutti i comandi con con request yes nel nostro vaso va configurato

RHOST (con l’ip di metasploitable) lo faremo con il comando set, questo è il risultato

A computer screen with white text and black text

Description automatically generated

Trattandosi di un modulo ausiliario non andiamo a settare nessun payload, in quanto l’exploit ci andrà a fornire le info che ci interessano per poter effettuare un accesso remoto sulla macchina vittima

Come vediamo nell’immagine

A screenshot of a computer screen

Description automatically generated

Ora ci basta aprire un altro terminale e lanciare il comando telnet seguito dall’ip di metasploitable

adesso utilizzeremo le credenziali fornite dall’exploit appena lanciato per poter accedere da remoto

Sulla macchina vittima

Il risultato è che adesso abbiamo il pieno controllo di metasploitable direttamente dal nostro kali