ESERCIZIO TEST METASPLOIT

Vi chiediamo di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd». Configurare l’indirizzo della vostra macchina Metasploitable come di seguito: 192.168.1.149/24. Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test\_metasploit. 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)

VSFPDT:

(Very Secure File Transfer Protocol Daemon)

È un servizio FTP (File Transfer Protocol) open source utilizzato per consentire il trasferimento di file tra un client e un server tramite il protocollo FTP.

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 program

Description automatically generated

Porta 21: aperta, servizio: ftp, versione: vsftpd 2.3.4

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

Con msfconsole avviamo il servizio e con il comando search seguito da vsftpd 2.3.4

E troveremo l’exploit per bucare quel servizio (importante da selezionare la versione corretta)

A screenshot of a computer

Description automatically generated

Una volta scelto l’exploit (con il comando use seguito dal path ) 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 screenshot of a computer

Description automatically generated

Dopo questa fase possiamo passare a settare il payload con il comando show. Ora ci uscirà una lista di payload da scegliere e con il comando set lo utilizzeremo

A screenshot of a computer

Description automatically generated

Settato anche il payload non ci resterà che lanciare l’exploit digitando il comando exploit.

A computer screen shot of a computer screen

Description automatically generated

Lanciato l’exploit otterremo come output command shell session con il cambio di ip,

dicendoci che ci troviamo nella macchina vittima.

Per assicurarci di essere dentro basta digitare il comando ifconfig, il risultato sarà l’ip della

macchina vittima.

Ora dovremmo acquisire i privilegi di root per poi creare una cartella.

Con il comando ls e cd ci siamo spostati nelle varie directory fino a trovare quella di root

Con il comando mkdir abbiamo creato la cartella richiesta dall’esercitazione test\_metasploit

A screen shot of a computer

Description automatically generated

Per concludere siamo andati su metasploitable per verificare che ciò sia avvenuto con successo e il risultato è stato positivo

A screenshot of a computer

Description automatically generated