**Report di Penetration Testing su Metasploitable**

**Obiettivo dell'Esercizio**

Ho condotto un test di penetrazione sulla macchina Metasploitable, mirato specificamente al servizio ‘vsftpd 2.3.4’. L'esercizio è stato eseguito utilizzando la piattaforma Metasploit su un sistema operativo Kali Linux.

**Procedura Seguita**

**1.Scansione del Servizio e Identificazione della Vulnerabilità**

Come primo passo sono andato a eseguire il comando nmap -sP 192.168.1.149, il quale mi conferma se la macchina target è attiva e accessibile, successivamente ho eseguito il comando nmap -sV 192.168.1.149, il quale rileverà i servizi attivi sulle porte aperte, utile per determinare le possibili vulnerabilità.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

- Poi sono andato ad attivare metasploit da kali, con il comando msfconsole e a seguire ho utilizzato Metasploit per cercare exploit adatti per il servizio ‘vsftpd 2.3.4’.

Immagine che contiene testo, schermata, Software multimediale, Software per la grafica

Descrizione generata automaticamente

- Ho selezionato e configurato l'exploit noto come ‘exploit/unix/ftp/vsftpd\_234\_backdoor’.

- Dopo aver impostato gli opportuni parametri di rete, ho lanciato l'exploit che mi ha permesso di ottenere una shell con privilegi di root sulla macchina target.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**2. Creazione della Cartella**

- Come richiesto, ho creato una cartella chiamata ‘test\_metasploit’ nella directory root usando il comando ‘mkdir /test\_metasploit’.

- Per confermare la creazione, ho eseguito ‘ls /’ che ha mostrato chiaramente la presenza della nuova cartella nella directory root.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

**3. Comandi Aggiuntivi**

- Per una maggiore comprensione del sistema, ho eseguito il comando ‘cat /etc/passwd’, che mi ha permesso di visualizzare l'elenco degli utenti del sistema, identificando potenziali vettori di attacco aggiuntivi.

Immagine che contiene testo, schermata, menu, Carattere

Descrizione generata automaticamente

- Ho anche utilizzato il comando ‘netstat -tuln’ per esaminare le porte aperte sul sistema. Questo comando ha evidenziato quali servizi erano attivi e ascoltanti, fornendomi un quadro chiaro delle potenziali superfici di attacco.

Immagine che contiene testo, schermata, menu, design

Descrizione generata automaticamente

**Risultati**

L'exploit ha avuto successo, consentendomi di accedere come utente root. Questo dimostra una significativa vulnerabilità nel servizio ‘vsftpd 2.3.4’. Inoltre, la creazione della cartella ha avuto esito positivo e senza problemi. L'analisi degli utenti e delle porte ha rivelato ulteriori aree che necessitano di attenzioni per la sicurezza.