Report – Accesso a Metasploitable 2 via Telnet e Upgrade a Meterpreter

1. Obiettivo dell’esercizio

L’obiettivo dell’esercizio è dimostrare come sia possibile ottenere accesso non autorizzato a una macchina vulnerabile **Metasploitable 2** sfruttando **credenziali di default** esposte sul servizio **Telnet**, e successivamente **gestire e migliorare la sessione ottenuta** tramite l’upgrade a **Meterpreter** utilizzando il framework **Metasploit**.

---

2. Ambiente di test

Componente	Descrizione
Attacker	Kali Linux
Target	Metasploitable 2
Framework	Metasploit
Servizio sfruttato	Telnet (porta 23/TCP)
Tipo di attacco	Credential-based access
Rete	LAN / Host-only

---

3. Fase 1 – Avvio di Metasploit

L’attività inizia con l’avvio della Metasploit Framework Console tramite il comando:

```
msfconsole
```

Metasploit fornisce una piattaforma modulare per l’esecuzione di exploit, scanner, payload e moduli di post-exploitation.

---

4. Fase 2 – Autenticazione tramite Telnet

4.1 Selezione del modulo

È stato utilizzato il modulo ausiliario:

`auxiliary/scanner/telnet/telnet_login`

Questo modulo consente di effettuare tentativi di autenticazione su servizi Telnet utilizzando credenziali note o fornite manualmente.

4.2 Configurazione del modulo

Sono stati impostati i seguenti parametri:

- **RHOSTS**: indirizzo IP della macchina Metasploitable 2
- **USERNAME**: `msfadmin`
- **PASSWORD**: `msfadmin`
- **STOP_ON_SUCCESS**: `true`

L'opzione `STOP_ON_SUCCESS` permette di interrompere la scansione non appena viene individuata una combinazione di credenziali valida.

4.3 Esecuzione

Il modulo è stato avviato tramite il comando:

`run`

Risultato

Il modulo ha identificato correttamente le credenziali valide e ha aperto una **command shell remota**, confermando la presenza di credenziali deboli e servizi non sicuri esposti sulla macchina target.

---

5. Fase 3 – Gestione delle Sessioni

5.1 Elenco delle sessioni attive

Le sessioni attive sono state verificate tramite:

```
sessions -l
```

Il comando restituisce informazioni quali ID della sessione, tipo di connessione e indirizzo IP remoto.

5.2 Interazione con la sessione

Per interagire con la sessione shell ottenuta:

```
sessions -i <ID_sessione>
```

È stato possibile eseguire comandi di sistema sulla macchina target, confermando il successo dell'accesso.

---

6. Fase 4 – Background della sessione

Al fine di procedere con l'upgrade della sessione, la shell attiva è stata messa in background utilizzando la combinazione:

```
Ctrl + Z
```

con conferma dell'operazione.

---

7. Fase 5 – Upgrade della Sessione a Meterpreter

7.1 Selezione del modulo

Per migliorare le capacità di post-exploitation è stato utilizzato il modulo:

```
post/multi/manage/shell_to_meterpreter
```

Questo modulo consente di convertire una shell standard in una sessione **Meterpreter**, più potente e flessibile.

7.2 Configurazione

È stato configurato il parametro:

- **SESSION**: ID della sessione shell precedentemente ottenuta

Le altre opzioni sono state lasciate ai valori di default.

7.3 Esecuzione

Il modulo è stato eseguito con successo, aprendo una nuova **Meterpreter session**.

---

8. Verifica dell'upgrade

La nuova sessione è stata verificata tramite:

```
sessions -l
sessions -i <ID_meterpreter>
```

Comandi come `sysinfo` e `getuid` hanno confermato l'accesso avanzato al sistema target.

---

9. Considerazioni di Sicurezza

L'esercizio evidenzia gravi problematiche di sicurezza:

- Utilizzo di **credenziali di default**
- Esposizione del servizio **Telnet**, protocollo non cifrato
- Assenza di controlli di accesso e hardening del sistema

In un contesto reale, tali vulnerabilità permetterebbero a un attaccante di ottenere rapidamente il controllo del sistema.

---

10. Conclusione

L’attività ha dimostrato come un attacco basato su credenziali deboli possa compromettere completamente un sistema vulnerabile. L’utilizzo di Metasploit ha permesso non solo l’accesso iniziale, ma anche la gestione e il potenziamento della sessione tramite Meterpreter, simulando realisticamente uno scenario di compromissione.