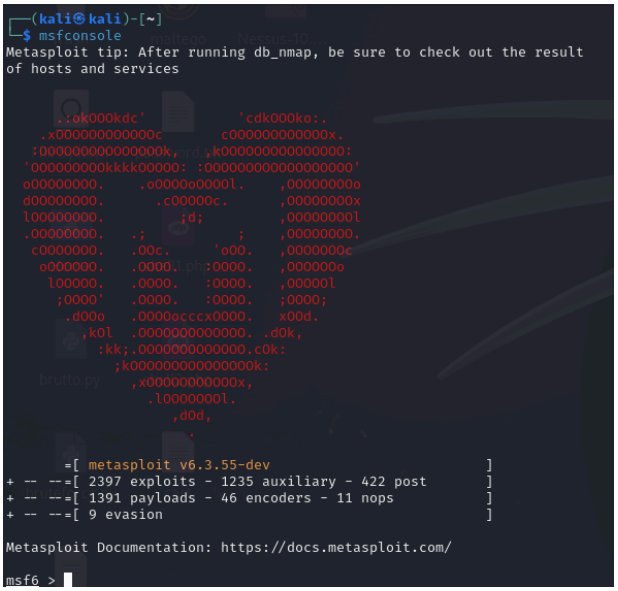
S7.L1 Metasploit Hacking

Traccia:

Nella lezione pratica di oggi, impareremo come eseguire una sessione di hacking utilizzando Metasploit sulla macchina Metasploitable.
Compito:
Basandoci sull'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, utilizzando il servizio "vsftpd" (lo stesso trattato nella lezione teorica).
L'unica differenza sarà l'indirizzo della vostra macchina Metasploitable. Configuratela con il seguente indirizzo: 192.168.1.149/24.
Una volta ottenuta la sessione sulla macchina Metasploitable, create una cartella nella directory di root (/) con il comando mkdir e chiamatela "test_metaspploit".

Inizio configurando la mia macchina di metaspoitable con il seguente ip: 192.168.1.149/24

Fase 1: Avvio di MSFConsole.



Comando utilizzato: msfconsole

- Descrizione: L'apertura di Metasploit Framework Console (MSFConsole) è il primo passo. MSFConsole è l'interfaccia principale di Metasploit, che permette di eseguire exploit e gestire vari moduli di attacco. Quando viene avviato, mostra un banner ASCII e alcune informazioni utili come il numero di exploit, payload, encoder e moduli di evasione disponibili.

Spiegazione:

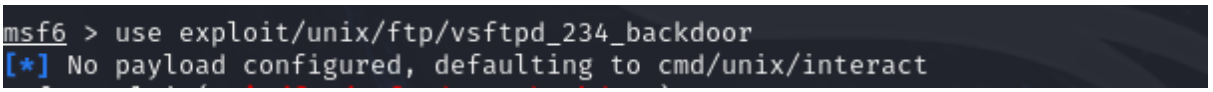
1. Aprire il terminale: Per prima cosa, apro il terminale sulla mia macchina Kali Linux.
2. Eseguire il comando msfconsole: Digito msfconsole nel terminale e premo Invio. Questo comando avvierà la console di Metasploit.

3. Attendere l'avvio della console: Dopo aver eseguito il comando, la console di Metasploit si avvierà. Potrebbe richiedere alcuni secondi per completare il caricamento.
4. Verifica dell'avvio: Una volta completato l'avvio, si vedrà un banner ASCII e un prompt che indica che la console è pronta per ricevere comandi (msf6 >).

Questa fase è essenziale perché ti prepara per caricare e configurare gli exploit e i payload necessari per compromettere la macchina target.

Fase 2: Selezione dell'Exploit

Utilizzo l'exploit unix/ftp/vsftpd_234_backdoor, anteponendo al path il comando «use»



1. Comando utilizzato: use exploit/unix/ftp/vsftpd_234_backdoor
    - Descrizione: Questo comando seleziona l'exploit specifico per il servizio vsftpd versione 2.3.4, noto per contenere una backdoor. Utilizzando questo exploit, è possibile sfruttare la vulnerabilità nel servizio FTP per ottenere accesso non autorizzato alla macchina target.

Spiegazione:

1. Selezionare l'exploit: Digito use exploit/unix/ftp/vsftpd_234_backdoor nella console di Metasploit e premo Invio. Questo comando caricherà l'exploit specifico nella sessione di Metasploit.
2. Caricamento dell'exploit: Dopo aver eseguito il comando, si vedrà un messaggio che conferma il caricamento dell'exploit, specificando che nessun payload è stato configurato e che verrà utilizzato il payload di default cmd/unix/interact.
3. Verifica: La console di Metasploit dovrebbe mostrare il prompt cambiato in msf6 exploit(unix/ftp/vsftpd_234_backdoor) >, indicando che l'exploit è stato correttamente selezionato e pronto per essere configurato.

Questo passaggio è cruciale per preparare l'attacco, poiché seleziona lo specifico modulo di exploit che verrà utilizzato per compromettere la macchina target.

Fase 3: Configurazione dell'RHOSTS

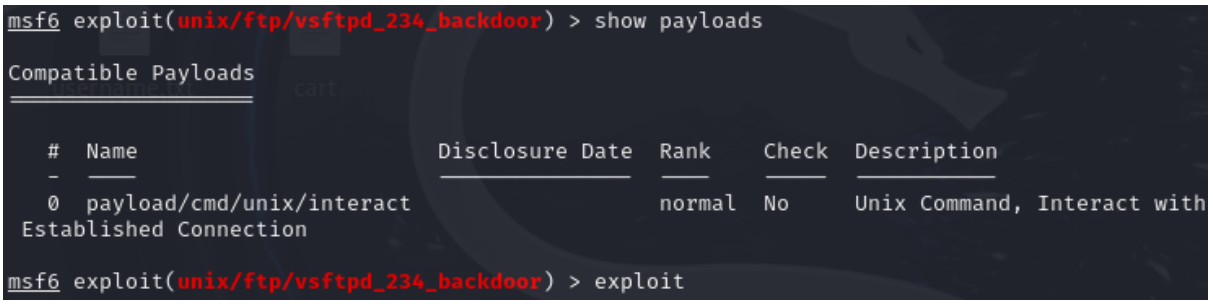
1. Comando utilizzato: set RHOSTS 192.168.1.149
    - Descrizione: In questo passo, viene configurato l'indirizzo IP della macchina target, ovvero la macchina Metasploitable. Il comando set RHOSTS assegna l'indirizzo IP della macchina vulnerabile su cui si desidera eseguire l'exploit.

Spiegazione:

1. Impostare l'indirizzo IP del target: Digito set RHOSTS 192.168.1.149 nella console di Metasploit e premi Invio. Questo comando indica a Metasploit di utilizzare l'indirizzo IP specificato come target dell'exploit.
2. Verifica della configurazione: Dopo aver eseguito il comando, si vedrà una conferma che il valore di RHOSTS è stato impostato su 192.168.1.149. La console mostrerà un messaggio di conferma RHOSTS => 192.168.1.149.
3. Assicurarsi che l'indirizzo sia corretto: È importante verificare che l'indirizzo IP configurato corrisponda a quello della macchina Metasploitable su cui si vuole eseguire l'exploit.

Configurare correttamente l'RHOSTS è essenziale perché definisce il target dell'attacco, assicurando che l'exploit venga inviato alla macchina corretta.

Fase 4: Selezione del Payload



Comando utilizzato: show payloads

a. Descrizione: Questo comando elenca tutti i payload compatibili con l'exploit attualmente selezionato. Nel caso dell'exploit vsftpd 2.3.4 backdoor, viene visualizzato il payload cmd/unix/interact, che permette di ottenere una connessione interattiva sulla macchina target.

Spiegazione:

1. Visualizzare i payload compatibili: Digito show payloads nella console di Metasploit e premo Invio. Questo comando elenca tutti i payload che possono essere utilizzati con l'exploit corrente.
2. Verificare i dettagli del payload: Nella lista visualizzata, si vedrà il payload compatibile cmd/unix/interact, che ha come descrizione "Unix Command, Interact with Established Connection". Questo payload è configurato di default per questo exploit.
3. Utilizzo del payload di default: Nel contesto dell'exploit vsftpd 2.3.4, non è necessario configurare ulteriormente il payload poiché cmd/unix/interact è predefinito e sufficiente per ottenere l'accesso.

Questa fase è cruciale perché seleziona il tipo di accesso che si otterrà una volta che l'exploit è stato eseguito con successo. Il payload cmd/unix/interact è particolarmente utile perché fornisce una shell interattiva sulla macchina target.

Fase 5: Esecuzione dell’attacco

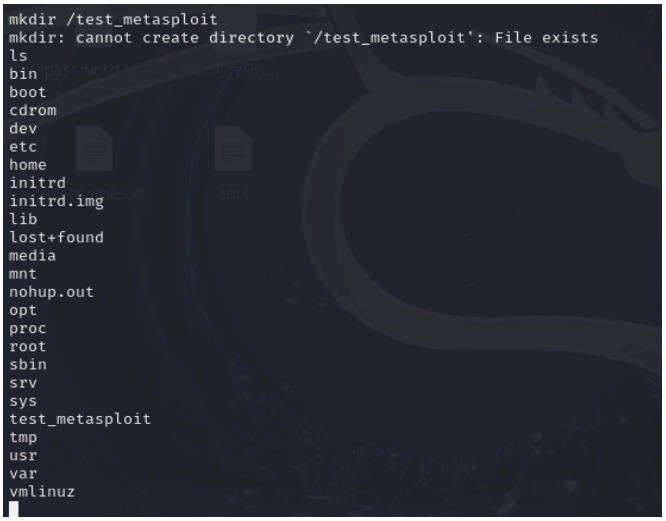
1. Comando utilizzato: exploit
    - Descrizione: Questo comando lancia l'exploit configurato contro il target. Se l'exploit ha successo, apre una shell di comando sulla macchina target.

Spiegazione passo per passo:

1. Eseguire l'exploit: Digita exploit nella console di Metasploit e premi Invio. Questo comando invia l'exploit verso il target specificato nelle configurazioni precedenti.
2. Analisi dei risultati:
    - Banner: La console visualizza il banner del servizio vsftpd 2.3.4, confermando che il servizio target è vulnerabile.
    - USER: Il sistema richiede di specificare la password dell'utente.
    - Backdoor: Il servizio di backdoor viene attivato e gestito.
    - UID: Il comando mostra che è stata trovata una shell con privilegi di root (uid=0(root) gid=0(root)).
3. Shell di comando aperta: La console conferma che una shell di comando è stata aperta con successo. La connessione viene stabilita tra la macchina dell'attaccante (192.168.1.150) e la macchina target (192.168.1.149).

Eseguire con successo l'exploit significa ottenere l'accesso alla macchina target, consentendo di eseguire comandi con privilegi di root. Questo passo è cruciale perché permette di compromettere completamente il sistema target.

Fase Finale: Creazione della Directory "test_metasploit"



Creazione della Directory:

- Ho creato una directory denominata test_metasploit con il comando mkdir

mkdir /test_metasploit

Verifica della Creazione della Directory

Verifica dalla Shell di MSFconsole:

- Ho verificato che la directory fosse stata creata correttamente utilizzando il comando ls con grep:
- ls -l / | grep test_metasploit
- Questo comando elenca i dettagli della directory test_metasploit, mostrando che esiste e visualizzando i suoi permessi.

Verifica dalla Root di Metasploitable:

- Ho controllato la root di Metasploitable per vedere se la directory test_metasploit era presente:
- ls /

Nell'output, ho confermato la presenza della directory test_metasploit.

Conclusione:

Ho eseguito correttamente tutti i passaggi per creare e verificare la directory test_metasploit. La directory è stata creata nella root del sistema target, come confermato dai comandi di verifica.