

Relazione sull'Attività di Hacking sul Servizio "vsftpd" della Macchina Metasploitable

Introduzione

Nella lezione di oggi, l'esercizio trattato ha riguardato una sessione di hacking sul servizio "vsftpd" di una macchina Metasploitable. L'obiettivo era quello di ottenere accesso alla macchina e creare una cartella specifica all'interno della directory root.

Configurazione dell'Indirizzo IP

Prima di iniziare l'attività di hacking, è stato necessario configurare l'indirizzo IP della macchina Metasploitable. L'indirizzo IP assegnato è stato **192.168.1.149/24**. Questa configurazione è leggermente diversa rispetto a quella utilizzata in classe, ma è stata eseguita correttamente per garantire la comunicazione appropriata con la macchina target.

Svolgimento dell'Attacco

Per eseguire l'attacco, è stato utilizzato il framework **Metasploit**. Di seguito sono riportati i passaggi principali:

1. Avvio di Metasploit:

- Eseguito il comando per avviare Metasploit Framework.

2. Selezione dell'Exploit:

- Utilizzato il comando **use exploit/unix/ftp/vsftpd_234_backdoor** per selezionare l'exploit specifico per il servizio "vsftpd".

3. Configurazione del Target:

- Impostato l'indirizzo IP della macchina target con il comando **set RHOST 192.168.1.149**.

4. Esecuzione dell'Exploit:

- Eseguito l'exploit con il comando **exploit**.

Creazione della Cartella

Dopo aver ottenuto l'accesso alla macchina Metasploitable tramite l'exploit, è stato necessario navigare fino alla directory root (/) e creare una cartella chiamata **test_metasploit**.

1. Accesso alla Directory Root:

- Utilizzato il comando **cd /** per spostarsi nella directory root.

2. Creazione della Cartella:

- Utilizzato il comando **mkdir /test_metasploit** per creare la cartella.

Conclusione

L'esercizio è stato completato con successo. L'accesso alla macchina Metasploitable è stato ottenuto tramite l'exploit del servizio "vsftpd" e la cartella **/test_metasploit** è stata creata correttamente all'interno della directory root. Questa attività ha confermato la comprensione delle tecniche di hacking e l'utilizzo efficace del framework Metasploit.