**S7 L1**

**AMATO SARA**

**Hacking con Metasploit**

Obiettivo dell’Esercizio:

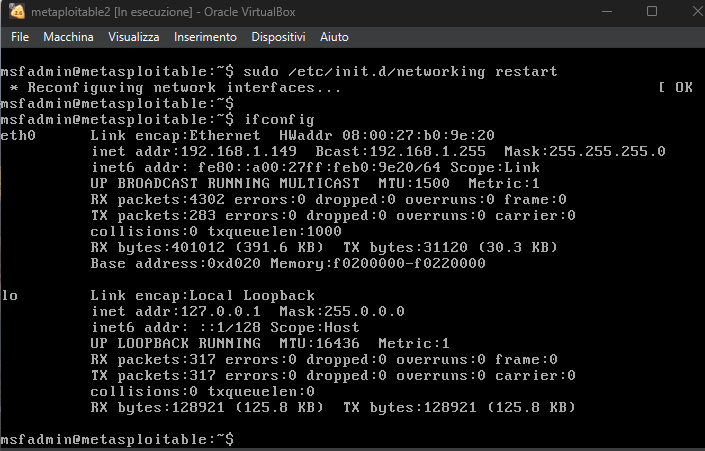
L’obiettivo di questo esercizio è stato quello di utilizzare Metasploit per testare la sicurezza di una macchina virtuale con vulnerabilità nota (Metasploitable 2). L’attacco è stato condotto sul servizio "vsftpd" attraverso un exploit specifico, dimostrando i concetti fondamentali dell’hacking etico, incluso l’uso di exploit e payload per ottenere accesso non autorizzato.

Configurazione dell'Indirizzo IP

Prima di iniziare con l'attacco, è stato assegnato alla macchina Metasploitable l’indirizzo IP 192.168.1.149/24. Questo passaggio permette di impostare un ambiente di rete controllato, in cui l'attaccante (nel nostro caso, la macchina Kali Linux) e la vittima (Metasploitable) sono all’interno della stessa subnet.

- La configurazione è stata realizzata nel file /etc/network/interfaces.

- Una volta salvate le modifiche, l’interfaccia è stata riavviata per applicare il nuovo IP.



Introduzione a Metasploit e all'Attacco su vsftpd

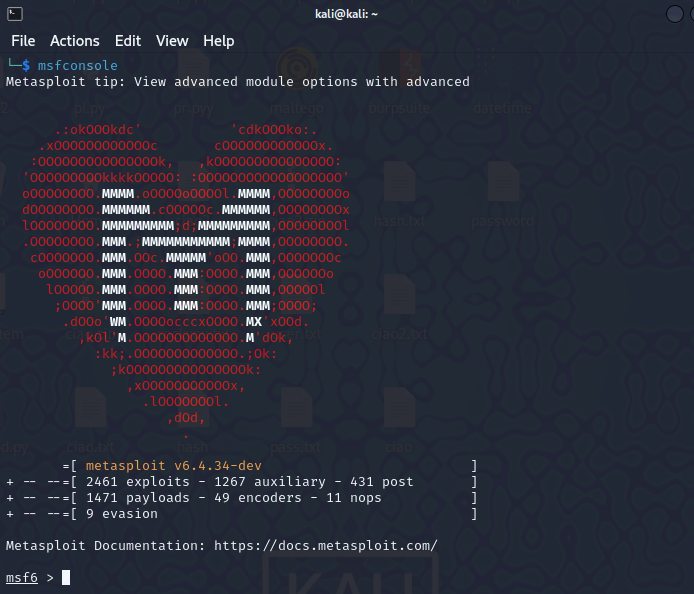
Metasploit è un framework di penetration testing che semplifica l’esecuzione di exploit su vulnerabilità note. Metasploit fornisce strumenti avanzati che permettono di:

- Scegliere un exploit: un codice specifico che sfrutta una vulnerabilità.

- Definire un payload: il codice eseguito una volta che si ottiene l’accesso.

- Gestire sessioni di accesso: una volta ottenuta l’accesso, l’attaccante può esplorare e manipolare il sistema compromesso.

In questo esercizio, è stato scelto un exploit per il servizio vsftpd, una versione vulnerabile del server FTP.



Ricerca dell’Exploit:

Utilizzando il comando `search vsftpd`, abbiamo cercato gli exploit disponibili per la versione vulnerabile del servizio. Il framework restituisce un elenco di moduli exploit per le vulnerabilità note.

Caricamento dell’Exploit:

Dopo aver identificato l’exploit giusto, è stato caricato con il comando `use exploit/unix/ftp/vsftpd\_234\_backdoor`. Questo exploit sfrutta una backdoor inserita nel servizio vsftpd versione 2.3.4, che consente accesso root senza autenticazione.

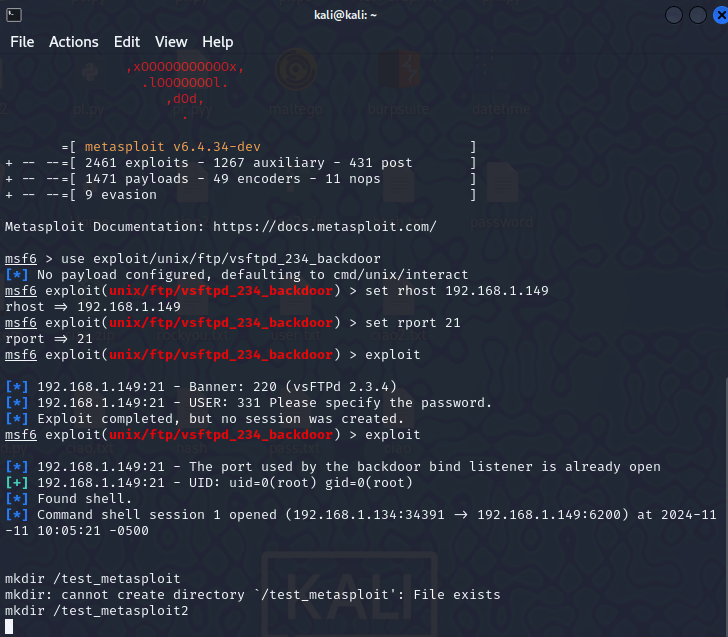
Configurazione dei Parametri:

- RHOST: l’indirizzo IP della macchina Metasploitable (192.168.1.149).

- RPORT: la porta su cui è attivo il servizio FTP (21 per impostazione predefinita).

Esecuzione dell’Exploit:

L’attacco è stato lanciato con il comando exploit. Una volta eseguito, Metasploit ha sfruttato la vulnerabilità per ottenere accesso root sulla macchina Metasploitable.



Creazione della Cartella

Una volta ottenuto accesso root, è stato possibile eseguire comandi di sistema. Il primo comando utilizzato è stato mkdir /test\_metasploit2, per creare una cartella denominata test\_metasploit2 nella directory root della macchina compromessa. Questo passaggio serve come conferma dell'accesso ottenuto e della capacità di interagire con il sistema.

Considerazioni finali

L’esercizio dimostra come, in un contesto controllato, un attaccante possa sfruttare vulnerabilità note per ottenere accesso non autorizzato. Metasploit, pur essendo uno strumento potente, deve essere usato in conformità con le leggi e le linee guida etiche di penetration testing.