**Relazione sull’Exploit di una Vulnerabilità FTP su Metasploitable tramite Kali Linux**

**1. Introduzione**

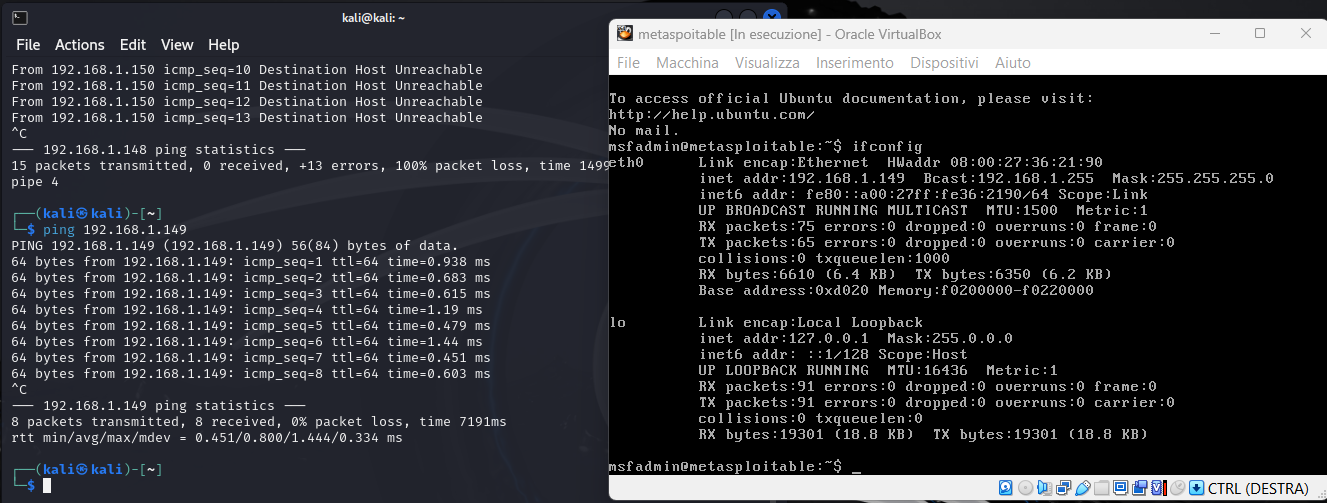
In questo esercizio, abbiamo utilizzato Kali Linux per eseguire un exploit contro una macchina virtuale vulnerabile, Metasploitable, sfruttando una debolezza nota nel servizio FTP (porta 21). L’obiettivo era ottenere l’accesso a Metasploitable e confermare il controllo sulla macchina target attraverso la creazione di una directory.

**2. Configurazione degli Indirizzi IP**

Per permettere la comunicazione tra Kali Linux e Metasploitable, abbiamo configurato manualmente gli indirizzi IP su entrambe le macchine, impostandoli sulla stessa subnet per consentire una connessione diretta. Le configurazioni erano le seguenti:

• **Kali Linux**: 192.168.1.150

• **Metasploitable**: 192.168.1.149



Questi indirizzi IP sono stati scelti per mantenere le macchine virtuali sulla stessa rete locale e garantire la possibilità di comunicazione diretta.

**3. Avvio di Metasploit e Ricerca dell’Exploit**

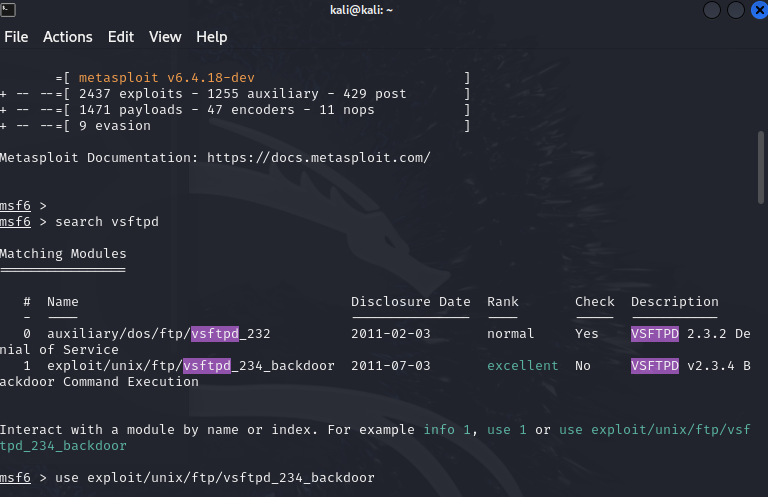
Con le macchine configurate e collegate, abbiamo avviato Metasploit su Kali Linux utilizzando il comando:

msfconsole

**b. Ricerca dell’exploit per VSFTPD**

Abbiamo cercato l’exploit specifico per il servizio **VSFTPD 2.3.4** utilizzando il comando:

search vsftpd



La ricerca ha restituito un exploit per **VSFTPD** con una backdoor che può essere sfruttata per ottenere accesso non autorizzato.

**4. Configurazione dell’exploit e attacco**

**a. Selezione dell’exploit**

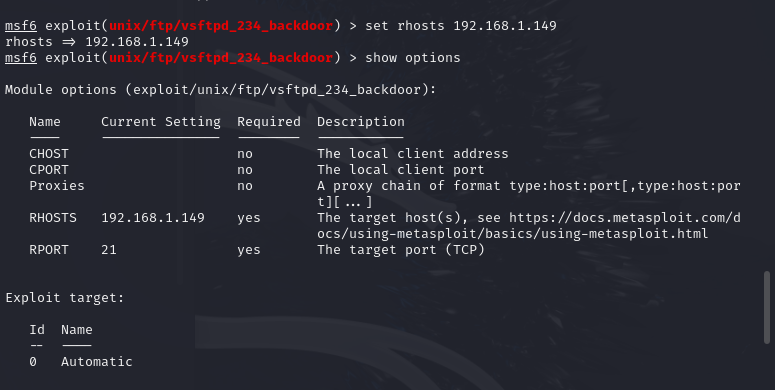
Dopo aver trovato l’exploit per VSFTPD 2.3.4, lo abbiamo selezionato con il comando:

use exploit/unix/ftp/vsftpd\_234\_backdoor

**b. Configurazione dell’host remoto**

Per indirizzare l’attacco verso Metasploitable, abbiamo configurato l’**RHOST** (remote host) impostando l’indirizzo IP di Metasploitable:

set RHOSTS 192.168.1.149

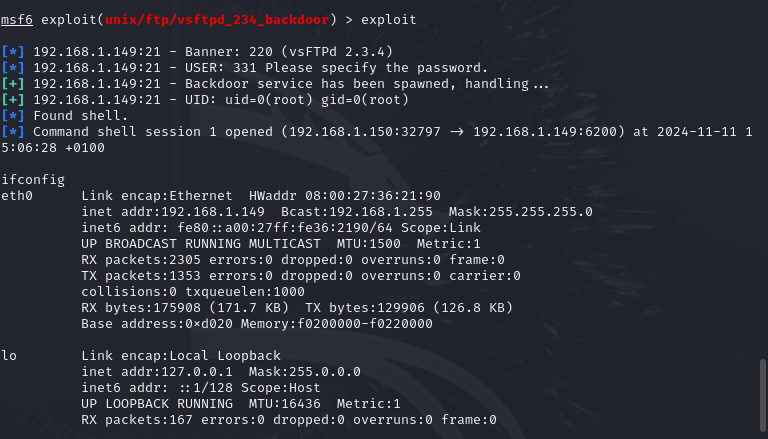


**c. Lancio dell’exploit**

Dopo aver configurato il target, abbiamo lanciato l’exploit con:

exploit

L’exploit ha aperto una backdoor sul servizio FTP, consentendo di stabilire una connessione con la macchina target. Abbiamo verificato che la connessione fosse stabilita correttamente utilizzando il comando ifconfig, che ha confermato la comunicazione tra le due macchine.



**5. Accesso a Metasploitable e creazione di una directory**

Dopo aver ottenuto l’accesso alla shell della macchina target (Metasploitable), abbiamo creato una nuova directory per confermare il controllo sul sistema compromesso. Il comando utilizzato è stato:

mkdir /test\_metasploit

La cartella test\_metasploit è stata quindi creata con successo all’interno del file system di Metasploitable, a prova dell’accesso e del controllo ottenuto.



**6. Conclusioni**

L’esercitazione ha dimostrato come, utilizzando un exploit noto di Metasploit, sia possibile ottenere accesso non autorizzato ad un sistema vulnerabile configurato con il servizio VSFTPD 2.3.4. Questo esempio evidenzia l’importanza della gestione delle vulnerabilità e della necessità di aggiornare costantemente i servizi per ridurre il rischio di attacchi simili.