Esercizio: S7-L1 Hacking con Metasploit

Esercizio Traccia : condurre una sessione di hacking utilizzando Metasploit su una macchina virtuale Metasploitable, e completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.

Dettagli dell'Attività: Configurazione dell'Indirizzo IP come segue: 192.168.1.149/24

Svolgimento dell'Attacco:

1) Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.

2) Creazione di una Cartella Una volta ottenuta l'accesso alla macchina Metasploitable.

SVOLGIMENTO

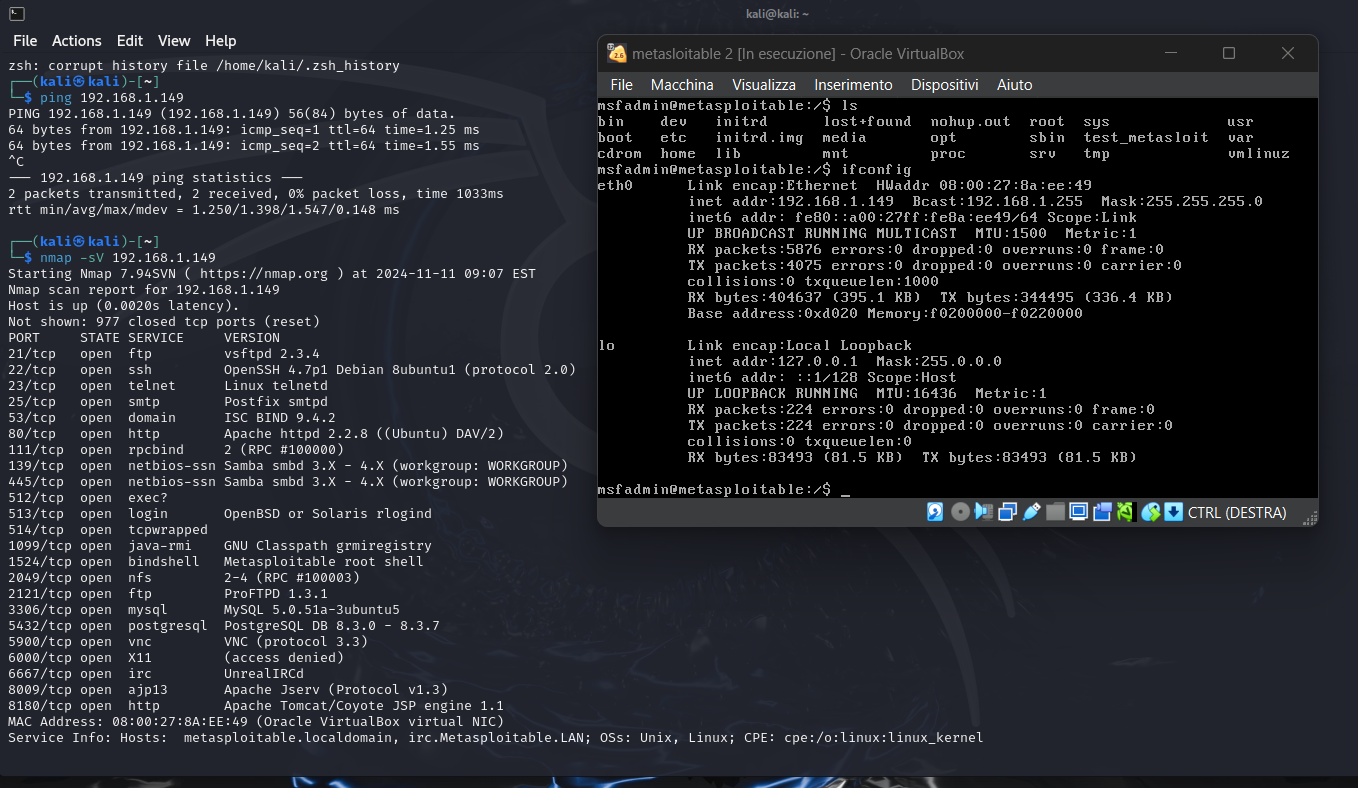
Per prima cosa cambiamo l’ip della macchina metasloitable.

Una volta avviata la macchina tramite il comando:

Sudo nano /etc/network/interface

Da qui cancelleremo “dhcp” e manualmente inseriremo la rete del nuovo ip.

Una volta volta che ci siamo accertati che comunicano kali con meta, tramite il comando: nmap -sV + ip della macchina target vedremo i servizi in esecuzione su una macchina e otterremmo informazioni dettagliate sulle versioni dei software collegati alle porte aperte.



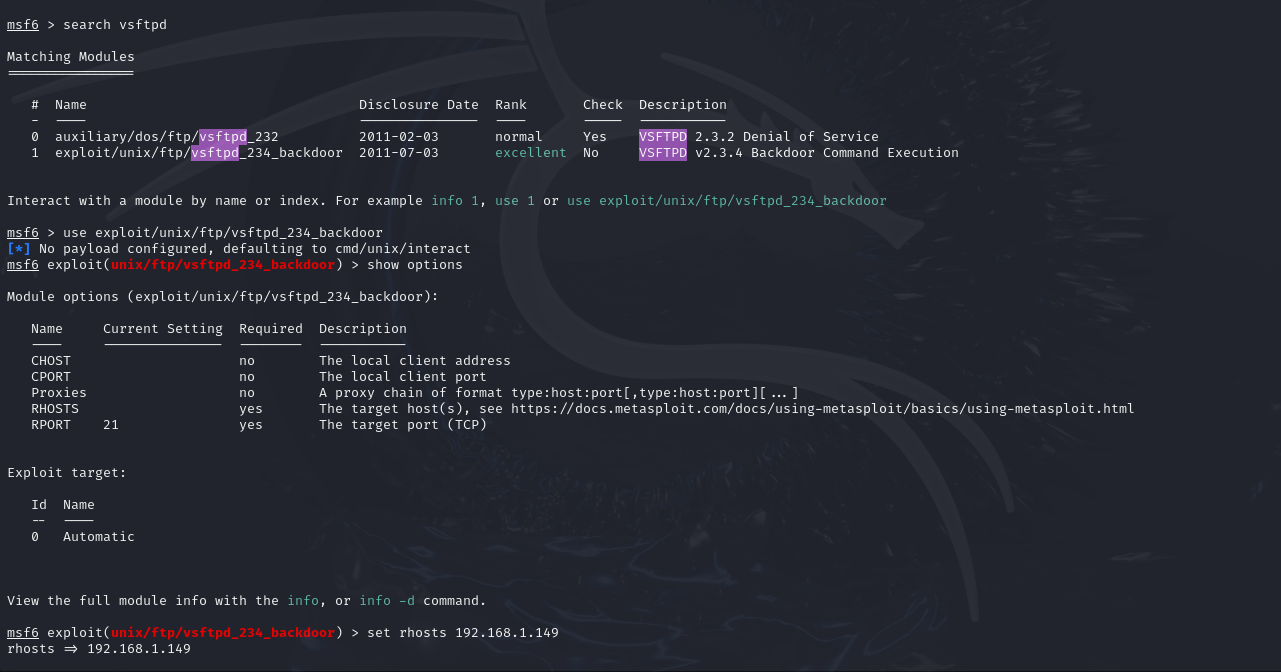
Con il comando :

Search vsftpd

Ci mostrerà un elenco di moduli disponibili che corrispondono alla parola chiave "vsftpd".

Ed useremo il path che ci serve mandando il comando :

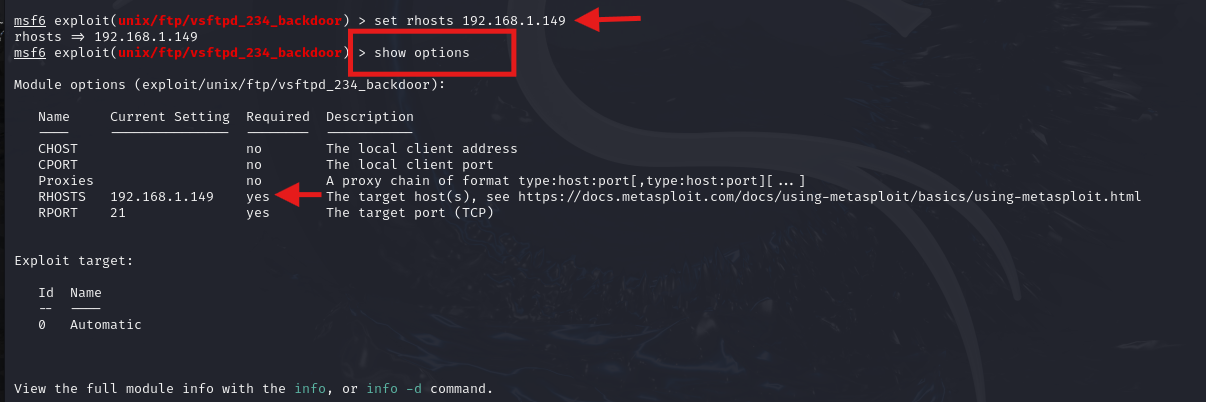
use + path



Inserendo il comando

Set rhosts + ip di meta

Andremo ad inserire l’ip per l’exploit e con il comando “show options “ vedremo che è stata inserita.



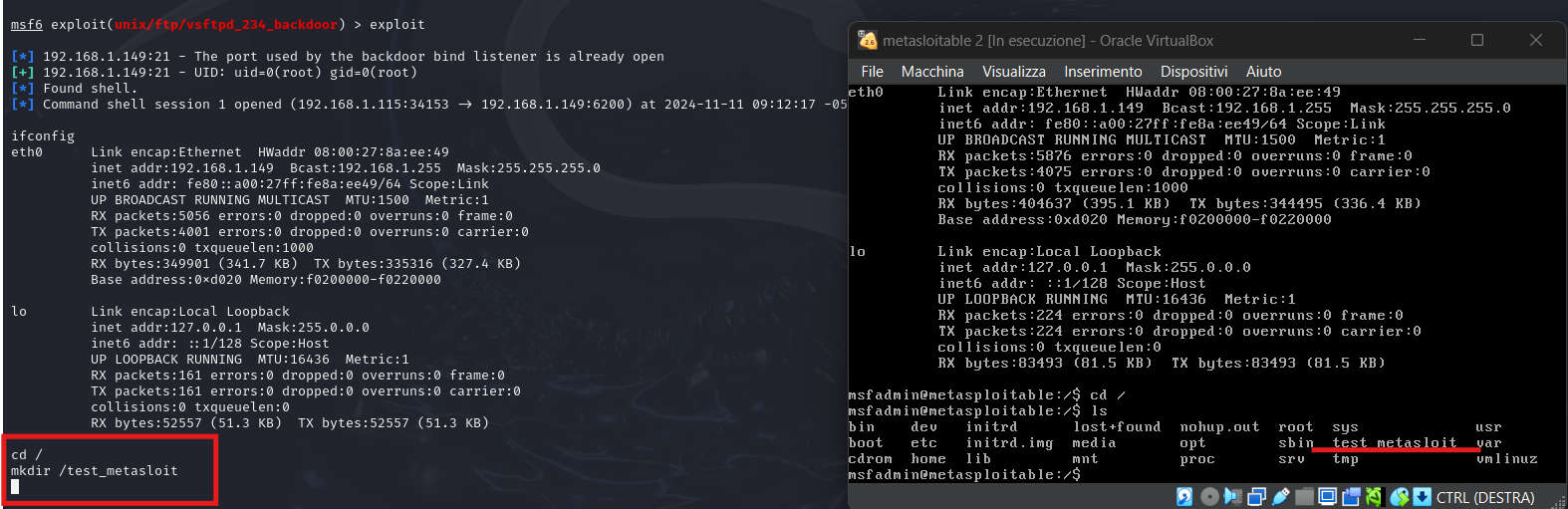
EXPLOIT

Un EXPLOIT è una tecnica o un programma che sfrutta una vulnerabilità di un sistema, applicazione o rete per ottenere un comportamento non previsto o dannoso. L'obiettivo principale di un exploit è ottenere accesso non autorizzato a un sistema, eseguire codice arbitrario o accedere a dati sensibili. Può essere utilizzato per escalation dei privilegi,bypassare misure di sicurezza o ottenere il controllo remoto del sistema. Gli exploit sono fondamentali sia per attacchi malevoli che per test di sicurezza legittimi come il pentesting.

Prima di tutto assicuriamoci che metasloitable non sia in stanby altrimenti l’exploit non darà risultati.

Poi mandando il comando “ exploit” manderemo l’attacco vero e propio.

La macchina target è quella che sta eseguendo il comando “ifconfig” e, di conseguenza, mostra la configurazione della rete di quella macchina. Quindi, se esegui un exploit, accedi a quella macchina, e poi esegui “ifconfig” vedremo l'IP della macchina target per la quale stiamo ora controllando i dettagli.



Inoltre procederemo con la creazione di una cartella una volta ottenuta l'accesso alla macchina Metasploitable, navigheremo fino alla directory di root (/) e creiamo una cartella chiamata “ test\_metasploit " utilizzando il comando:

mkdir test\_metasploit

Aprendo il terminale di metasploitable possiamo vedere come la cartella sia stata effettivamente creata.