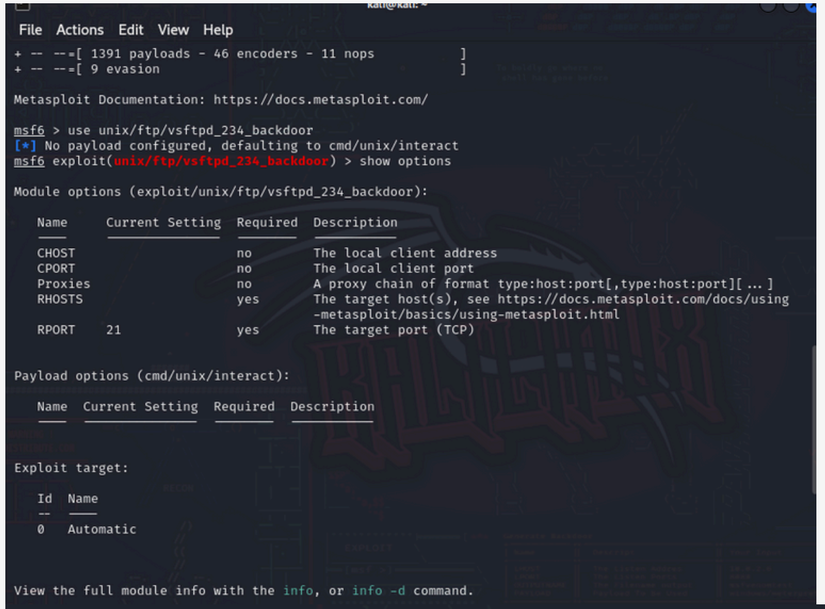
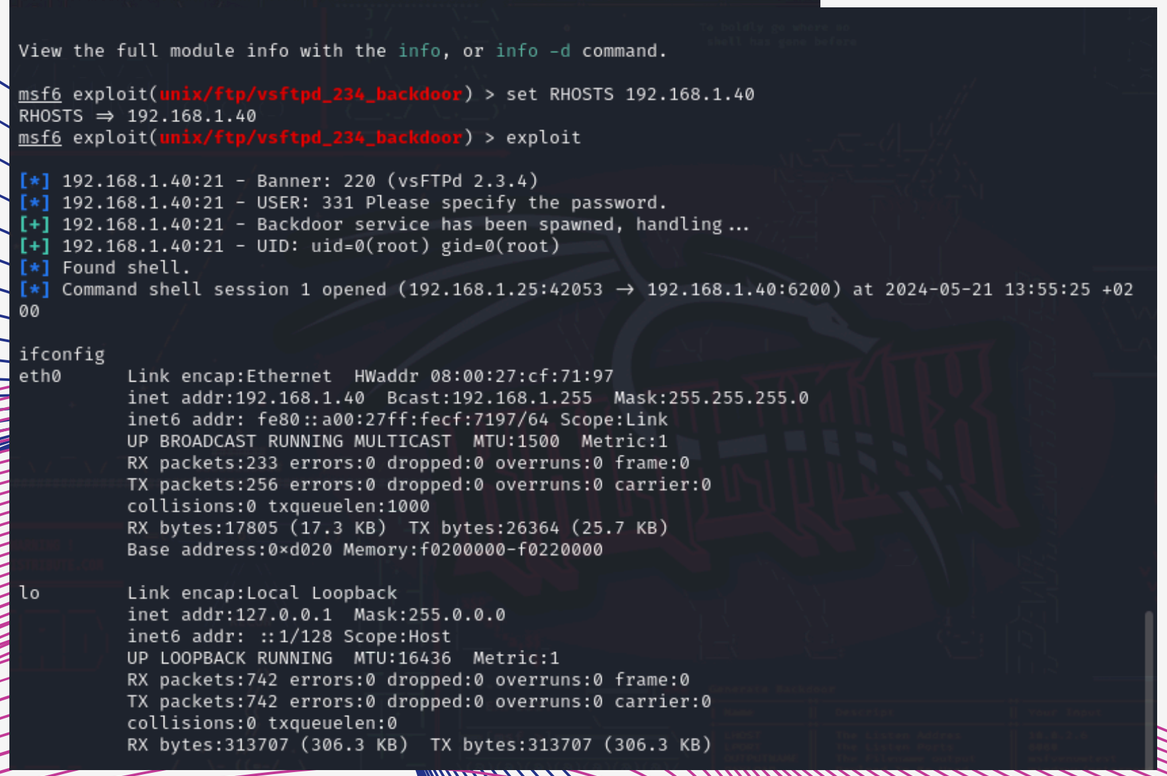
HACKING CON METASPLOIT





Obiettivo

L'obiettivo di questo esercizio è creare una backdoor su una macchina virtuale Metasploitable per garantire un accesso persistente utilizzando il framework Metasploit. Per raggiungere questo scopo, abbiamo utilizzato l'exploit unix/ftp/vsftpd_234_backdoor.

- Procedura
- Avvio di Metasploit Console Per iniziare, avviamo la console di Metasploit sulla nostra macchina Kali Linux con il comando: ‘msfconsole’
- Caricamento dell'Exploit Successivamente, carichiamo l'exploit specifico per la vulnerabilità del servizio FTP di VSFTPD versione 2.3.4. Questo exploit sfrutta una backdoor presente in questa versione del software FTP.

use unix/ftp/vsftpd_234_backdoor

- Configurazione del Target Configuriamo l'indirizzo IP della macchina Metasploitable come target dell'exploit. Utilizziamo il comando set per assegnare il valore corretto al parametro RHOSTS.

set RHOSTS 192.168.1.40

- Esecuzione dell'Exploit Una volta configurato il target, lanciamo l'exploit per ottenere l'accesso alla macchina Metasploitable

exploit

- Verifica dell'Accesso Dopo l'esecuzione dell'exploit, se l'attacco ha successo, otteniamo una shell sulla macchina Metasploitable. Per verificare l'accesso e confermare che siamo effettivamente entrati nel sistema target, eseguiamo il comando ifconfig all'interno della shell ottenuta.

ifconfig

- Analizzando l'output, possiamo vedere che l'indirizzo IP della macchina sulla quale siamo connessi è quello della macchina Metasploitable e non della nostra macchina Kali Linux. Questo conferma che abbiamo ottenuto l'accesso al sistema target.