Esercizio: Hacking con Metasploit Esercizio Traccia Nella lezione pratica di oggi, ci concentreremo su come condurre una sessione di hacking utilizzando Metasploit su una macchina virtuale Metasploitable.

Traccia dell'Esercizio Seguendo l'esercizio trattato nella lezione di oggi, vi sarà richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica.

Dettagli dell'Attività Configurazione dell'Indirizzo IP L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable. Configurate l'indirizzo come segue: 192.168.1.149/24 1. 2. Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.

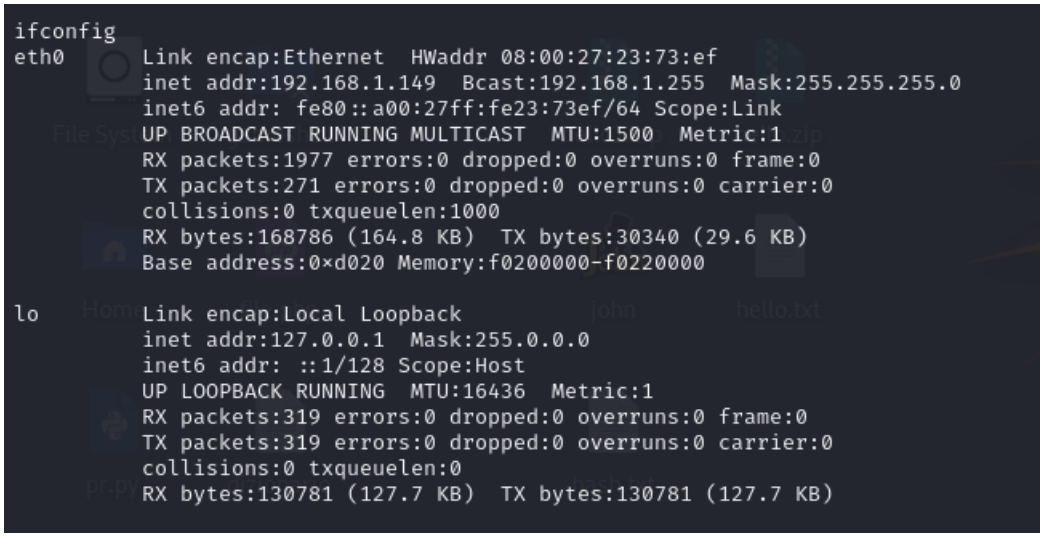
Creazione di una Cartella Una volta ottenuta l'accesso alla macchina Metasploitable, navigate fino alla directory di root (/) e create una cartella chiamata test_metasploit utilizzando il comando mkdir.

Esecuzione:

L'obiettivo principale è l'esplorazione di una vulnerabilità nel servizio FTP (vsftpd 2.3.4) utilizzando **Metasploit**, un framework per test di penetrazione. Dopo aver ottenuto accesso alla macchina target, si procede alla creazione di una cartella specifica come indicato nel compito.

L'esercizio ha come obiettivo:

1. Sfruttare una vulnerabilità nota di vsftpd 2.3.4 su Metasploitable.
2. Stabilire una sessione di shell sulla macchina target tramite Metasploit.
3. Creare una cartella denominata test_metasploit nella directory /root

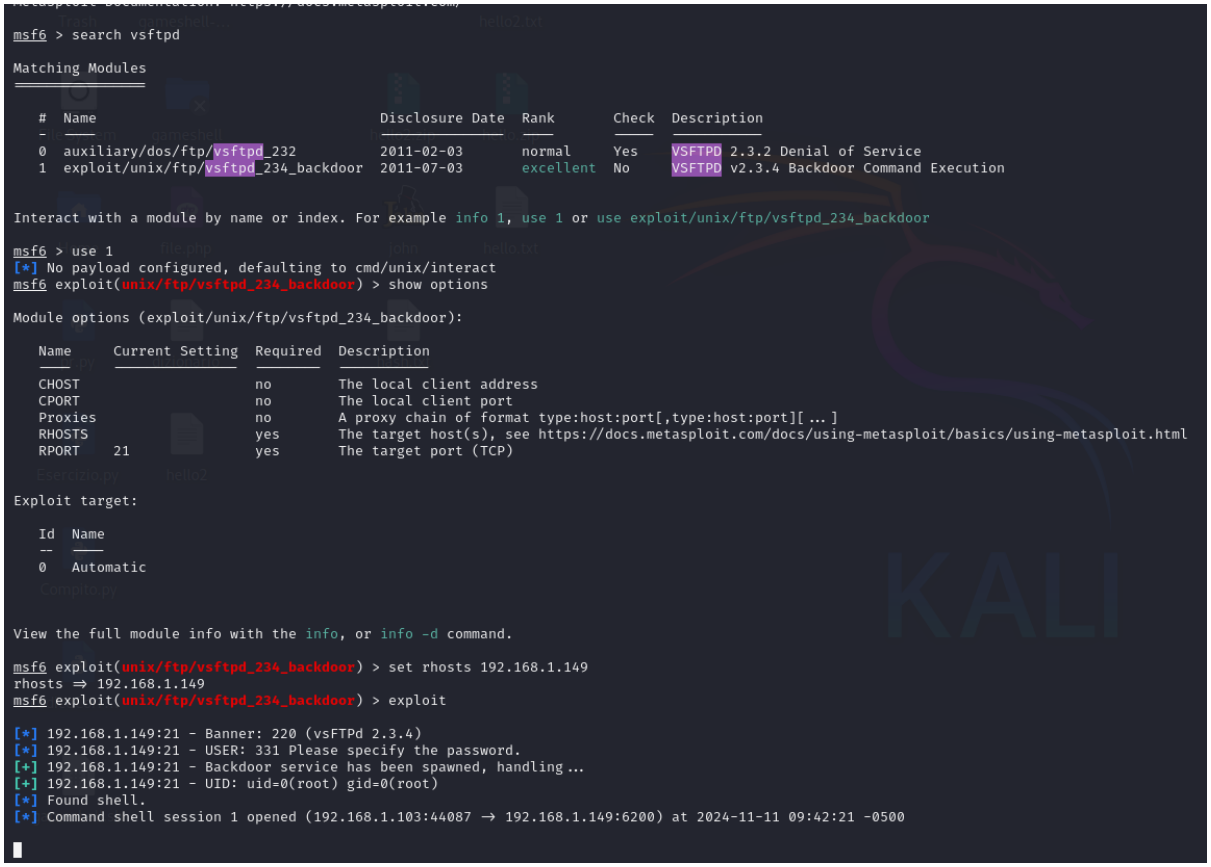


*Configurazione ip di metasploitable.

Nel terminale della macchina attaccante, abbiamo avviato Metasploit utilizzando il comando msfconsole. Successivamente, abbiamo ricercato l'exploit per la versione vulnerabile di vsftpd con il comando search vsftpd.

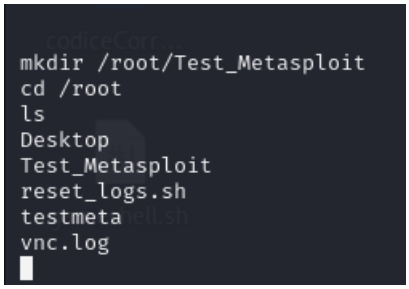
Abbiamo individuato l'exploit exploit/unix/ftp/vsftpd_234_backdoor, noto per sfruttare una backdoor presente nella versione 2.3.4 di vsftpd. Abbiamo quindi selezionato questo exploit e configurato l'indirizzo IP della macchina target con i seguenti comandi:

use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.1.149



Dopo aver completato la configurazione, abbiamo lanciato l'exploit per iniziare la sessione. Una volta ottenuto l’accesso alla macchina target, siamo entrati nella directory / e abbiamo tentato di creare la cartella richiesta.

Questo esercizio ci ha permesso di esplorare il processo di sfruttamento di una vulnerabilità nota in un servizio FTP attraverso Metasploit. La procedura ha sottolineato l’importanza di una configurazione accurata e della verifica dei risultati, specialmente in ambienti di test. La visualizzazione della cartella creata ha richiesto alcuni passaggi aggiuntivi, evidenziando anche i limiti di alcune shell ottenute tramite exploit.



L'attività ha dimostrato come strumenti come Metasploit possano essere utilizzati per test di sicurezza, evidenziando le vulnerabilità comuni e l’importanza delle patch di sicurezza.