# Relazione sulla Sessione di Hacking con Metasploit sulla Macchina Metasploitable

## Obiettivo

L'obiettivo di questa esercitazione pratica è effettuare una sessione di hacking sulla macchina Metasploitable sfruttando una vulnerabilità nel servizio vsftpd. Dopo aver ottenuto l'accesso, dobbiamo creare una cartella chiamata `test_metasploit` nella directory di root.

## Configurazione dell'Ambiente

Per iniziare, abbiamo configurato la macchina Metasploitable con l'indirizzo IP 192.168.1.149/24 e ci siamo assicurati che fosse accessibile dalla rete. La macchina attaccante ha utilizzato Metasploit Framework per eseguire l'exploit.

## Passaggi

Per prima cosa, abbiamo verificato che il servizio vsftpd fosse attivo sulla macchina Metasploitable utilizzando il comando `nmap`. Questo ci ha permesso di confermare che la porta 21, utilizzata dal servizio FTP, fosse aperta e pronta per essere sfruttata.

Successivamente, abbiamo avviato Metasploit Framework sulla macchina attaccante utilizzando il comando `msfconsole`. Una volta dentro Metasploit, abbiamo cercato un exploit specifico per vsftpd con il comando `search vsftpd`. Questo ci ha restituito una lista di exploit disponibili per il servizio vsftpd.

Abbiamo selezionato l'exploit `exploit/unix/ftp/vsftpd_234_backdoor` e lo abbiamo configurato per utilizzare l'indirizzo IP della macchina target con il comando `set RHOSTS 192.168.1.149`. Con l'exploit configurato correttamente, lo abbiamo eseguito con il comando `run`.

Durante l'esecuzione dell'exploit, abbiamo riscontrato un problema: la porta 6200 risultava già in uso poiché avevo provato a modificare l’interfaccia network tramite la backdoor ma, entrando nel file di configurazione, non potevo in alcun modo salvarlo e quindi la sessione è rimasta aperta

. Per risolvere questo problema, abbiamo individuato il processo che utilizzava la porta con il comando `sudo netstat -tulnp | grep :21` e lo abbiamo terminato utilizzando `sudo kill -9 <PID>`. Questo ci ha permesso di liberare la porta e riprovare l'exploit.

Con la porta 6200 ora libera, abbiamo rieseguito l'exploit e ottenuto con successo una shell sulla macchina Metasploitable. A questo punto, ci siamo spostati nella directory di root e abbiamo creato la cartella `test_metasploit` con il comando `mkdir /root/test_metasploit`.


**Conclusione**

Questa esercitazione ci ha permesso di utilizzare Metasploit per sfruttare una vulnerabilità nel servizio vsftpd della macchina Metasploitable e ottenere una shell. Abbiamo inoltre creato una cartella nella directory di root come richiesto. Questo esercizio ha fornito una preziosa esperienza pratica nell'uso di strumenti di penetration testing e nella risoluzione di problemi relativi ai servizi di rete.