S7L1

Esercizio: Hacking con Metasploit

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.

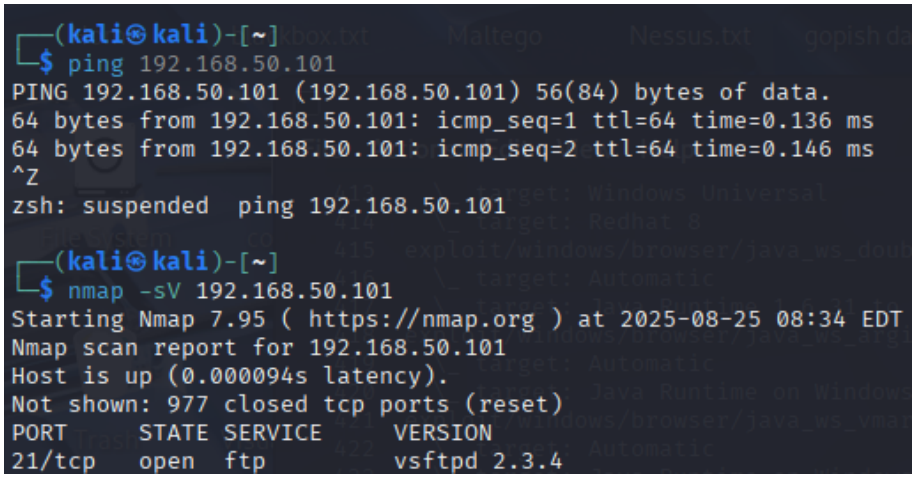
Dettagli dell'Attività
Configurazione dell'Indirizzo IP L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable. Configurate l'indirizzo come segue:

192.168.1.149/24

1. Svolgimento dell'Attacco 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, navigate fino alla directory di root (/) e create una cartella chiamata test_metasploit utilizzando il comando mkdir.
   mkdir /test_metasploit

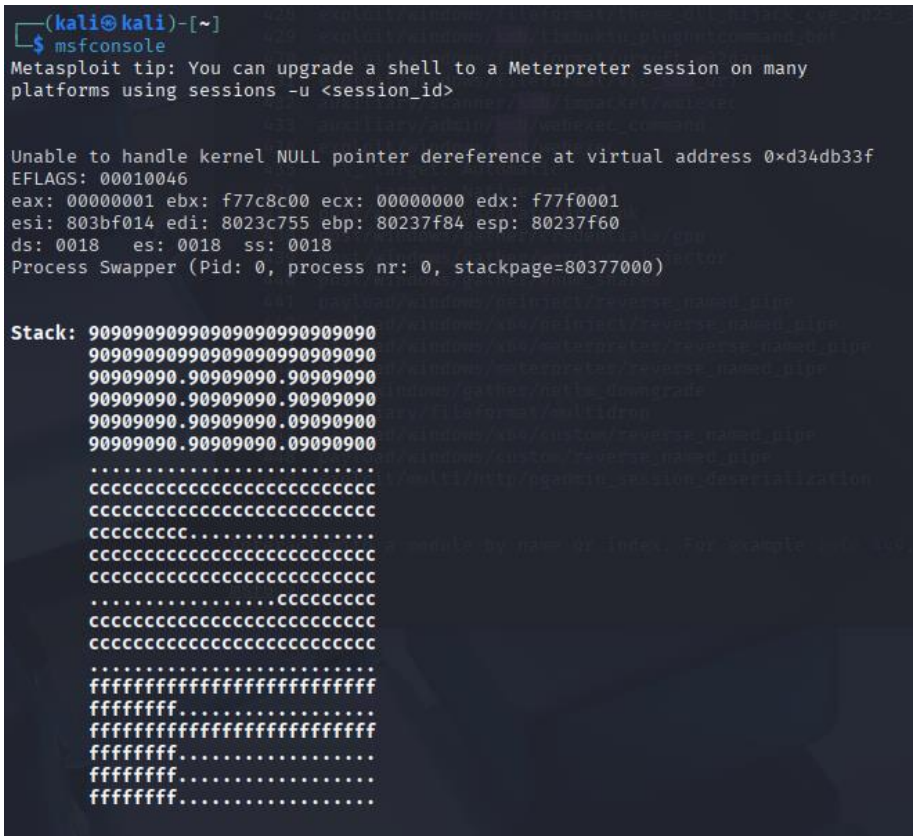
Per il corretto svolgimento dell'esercizio mi sono assicurato della comunicazione con la macchina vittima tramite un ping seguito dall'indirizzo IP corrispondente. Il ping mostra che la comunicazione funziona quindi ho avviato una scansione tramite nmap con il comando -sV seguito dall'IP della macchina vittima, nel nostro caso la metasploit.

-sV è un comando di nmap che serve ad identificare il servizio e la versione

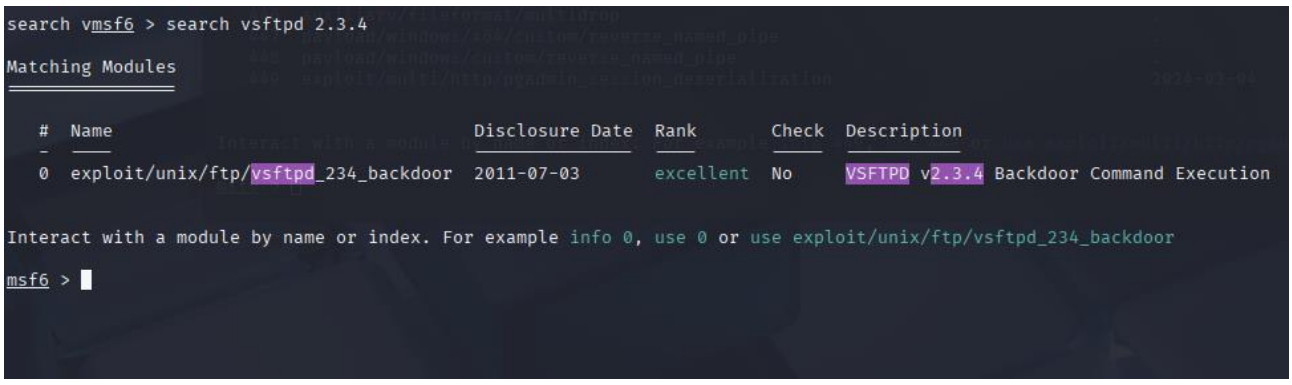


Tramite questa scansione otteniamo le informazioni sul servizio ftp, che è aperto e ha la versione vsftpd 2.3.4.

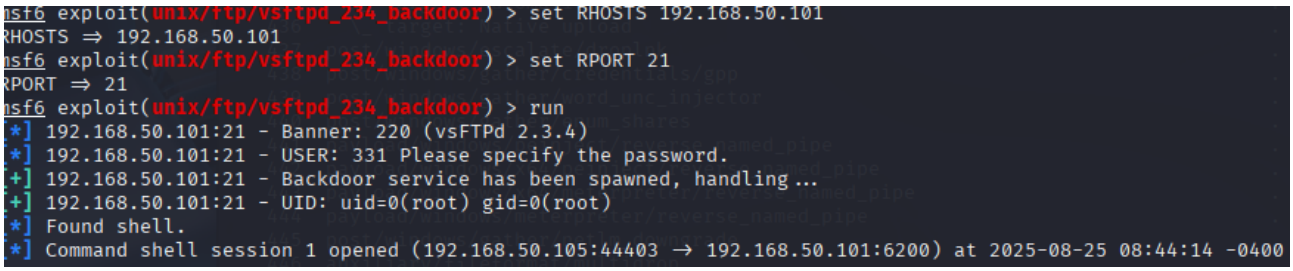
Ottenute queste informazioni riguardo la macchina vittima avvio msfconsole, un tool che permette di interagire con il framework Metasploit automatizzando e velocizzando attività come scansione vulnerabilità, creazione ed esecuzione di exploit e gestione di payload.



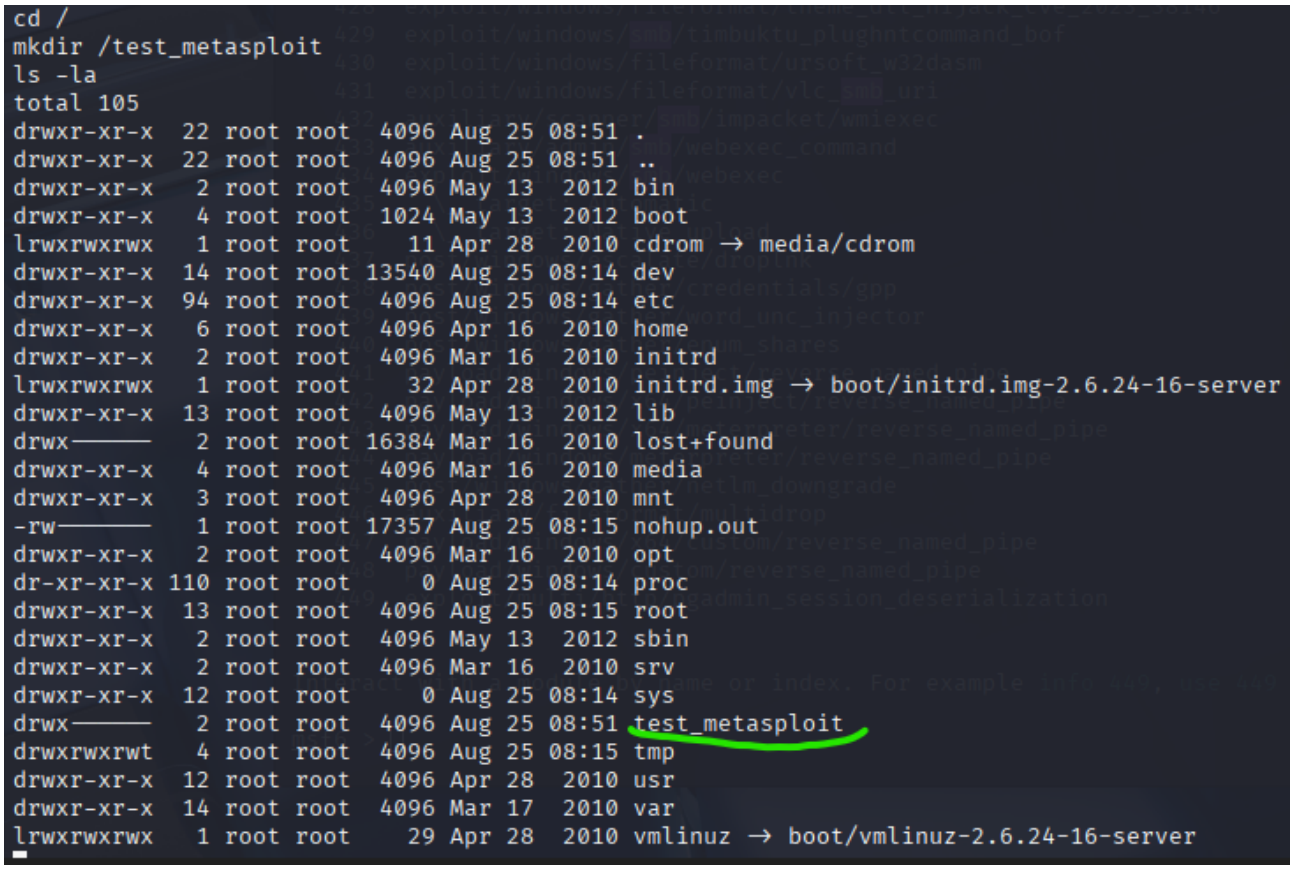
A questo punto facciamo una ricerca all'interno del tool utilizzando il comando **search** con parola chiave "**vsftpd**" per verificare se esiste un modulo che sfrutta esattamente quella versione e trovo **exploit/unix/ftp/vsftpd_234_backdoor.**



Scelgo di utilizzare l'exploit trovato utilizzando il comando **use** seguito dal nome del exploit **exploit/unix/ftp/vsftpd_234_backdoor**, preparo il modulo inserendo i parametri del nostro scenario, quindi IP della macchina vittima tramite set RHOSTS 192.168.50.101, set RPORT 21 che indica la porta e avvio con il comando **run**. Una volta lanciato l'expoit il tool ci avvisa che ha trovato la shell e che ha avviato la sessione.



Tramite il comando " **cd /** " Siamo entrati nella directory di root, non ci resta altro che creare la cartella richiesta dall'esercizio tramite il comando mkdir /test_metasploit e verificare la cartella compare nella directory, come mostrato nell'immagine qui sotto.



Tramite questo esercizio possiamo notare come, partendo dalla semplice verifica di connettività con la macchina Metasploitable2, sia stato possibile identificare un servizio FTP vulnerabile (vsftpd 2.3.4) grazie a una scansione con nmap. Utilizzando Metasploit ho quindi eseguito con successo l'exploit dedicato, ottenendo una shell remota sul sistema bersaglio. A conferma del controllo acquisito, ho creato una cartella all'interno del root del filesystem, mostrando così la possibilità di eseguire comandi arbitrari con privilegi elevati.
Questo percorso evidenzia l'importanza delle fasi di ricognizione, identificazione della versione del servizio e successivo sfruttamento, mostrando come una vulnerabilità non mitigata possa consentire in pochi passaggi l'accesso completo a un sistema.