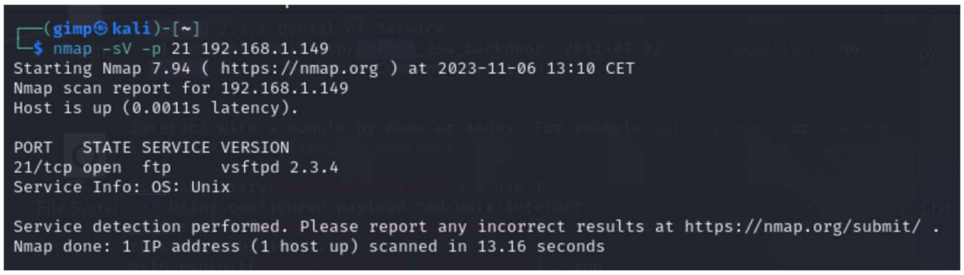
Esercizio S7-L1

L'esercizio prevedeva di usare l'exploit vsftpd su metaspoitable.

Un exploit è un codice malevola che sfrutta una vulnerabilità già presente nel sistema, a differenza di un malware che invece ha bisogno di comando esterno.

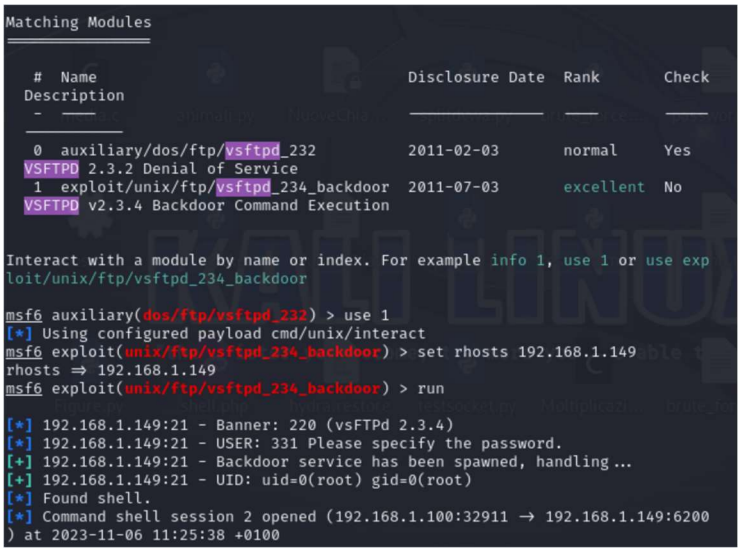
Vsftp sfrutta una vulnerabilità nel protocollo ftp, adibito al trasferimento dei dati.

Per prima cosa sono andato ad usare nmap per una scansione per vedere il servizio attivo sulla porta 21 (ftp) e che versione fosse.



Dopodiche ho lanciato msfconsole su kali e seguito tutto il procedimento spiegato.

Utilizzando search vsftpd ho trovato la versione corretta da usare (backdoor), ho impostato l'rhosts su 192.168.1.149 come descritto dall'esercizio e avviato l'exploit.



Dopo aver confermato la corretta esecuzione, mi sono spostato sulla directory root di meta e creato una nuova directory di nome test_metasploit.

Da meta ho cercato la suddetta directory per confermare che la creazione fosse andata a buon fine.