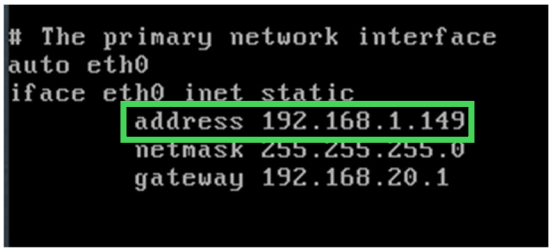
Come primo passaggio, viene richiesto di impostare l'indirizzo IP della macchina metasploitable a 192.168.1.149, così ho modificato il file di sistema per le impostazioni network:

E ho impostato l'indirizzo IP richiesto dalla consegna:

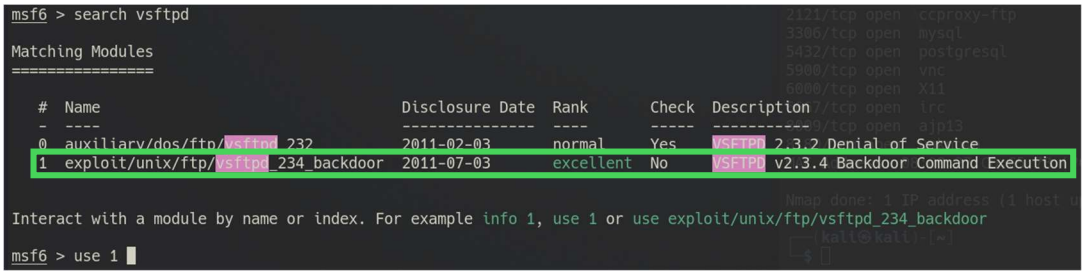


Per confermare i settaggi, ho dovuto riavviare la macchina e successivamente fatto un check per verificare che l'indirizzo fosse stato cambiato:

Successivamente sono andato a modificare l'indirizzo IP di Kali per averlo sotto la stessa rete della macchina metasploitable:

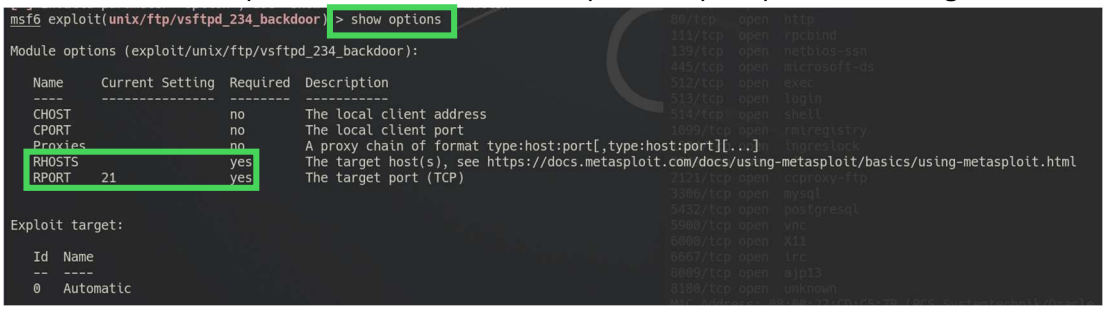
Come prossimo passo volevo verificare che la porta 21, riservata al servizio ftp fosse libera, così ho effettuato una scansione nmap verso la macchina metasploitable:

Successivamente sono andato ad avviare il framework di Metasploit su Kali e cercato l'exploit da utilizzare usando come parola chiave, il nome del servizio di cui sfruttare la vulnerabilità:

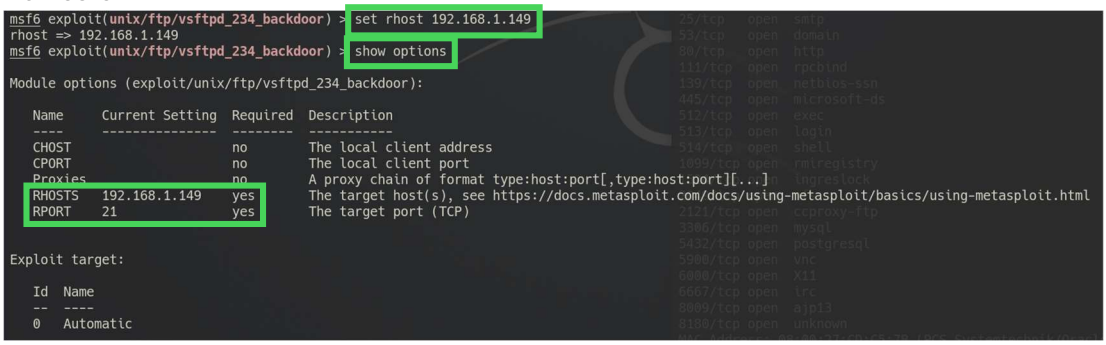


Per il nostro esercizio è necessario installare una backdoor, quindi userò il numero "1".

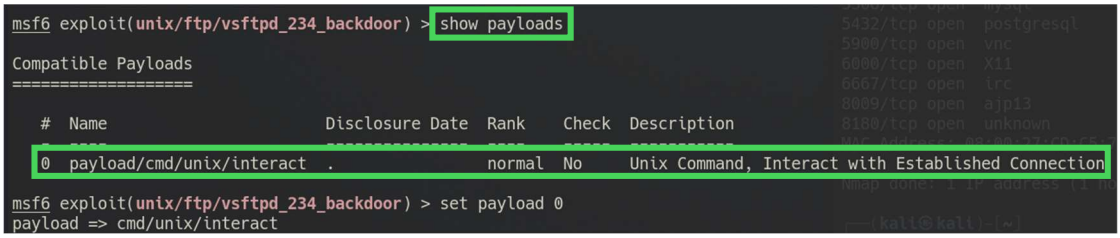
Ora vado a vedere quali informazioni richiede questo exploit per essere eseguito:



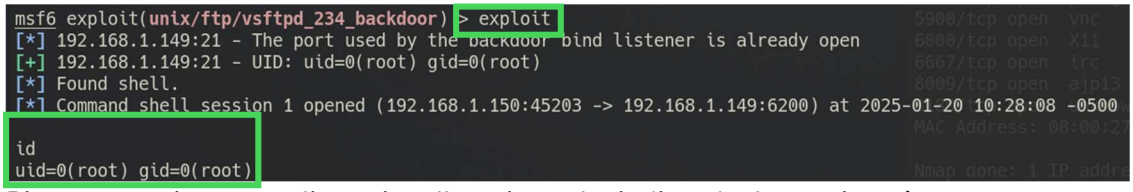
L'unica informazione mancante e richiesta è l'indirizzo IP del RemoteHOST, quindi do il comando "set rhost" seguito dall'indirizzo IP della macchina target che nel nostro caso è "192.168.1.149" come richiesto:



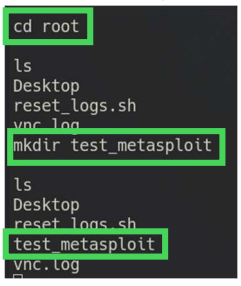
Do, infine, un comando di "show option" se ho impostato correttamente la configurazione.
Adesso devo specificare il payload, quindi scrivo "show payloads" per mostrare il payload piú pertinente exploit che abbiamo impostato:



Nel nostro caso esiste un solo payload quindi lo imposto usando il comando "set payload 0" dove 0 è il tag identificativo del payload elencato da metasploit.
Adesso non resta altro che avviare il processo di exploit dando il comando "exploit" o "run"



Rimane una riga vuota di seguito alla stringa che indica che la sessione è stata aperta, quella riga è proprio la shell inserita all'interno della macchina target; infatti, posso eseguire qualsiasi comando io voglia.
Sfrutto la backdoor per spostarmi nella directory "root" e inserire una directory chiamata "test_metasploit":



Per verificare l'avvenuta creazione, sono andato su metasploitable per verificare che la cartella non fosse presente prima dell'esecuzione del framework e successivamente la sua esecuzione ho elencato il contenuto della cartella root per mostrare l'effettiva presenza della cartella