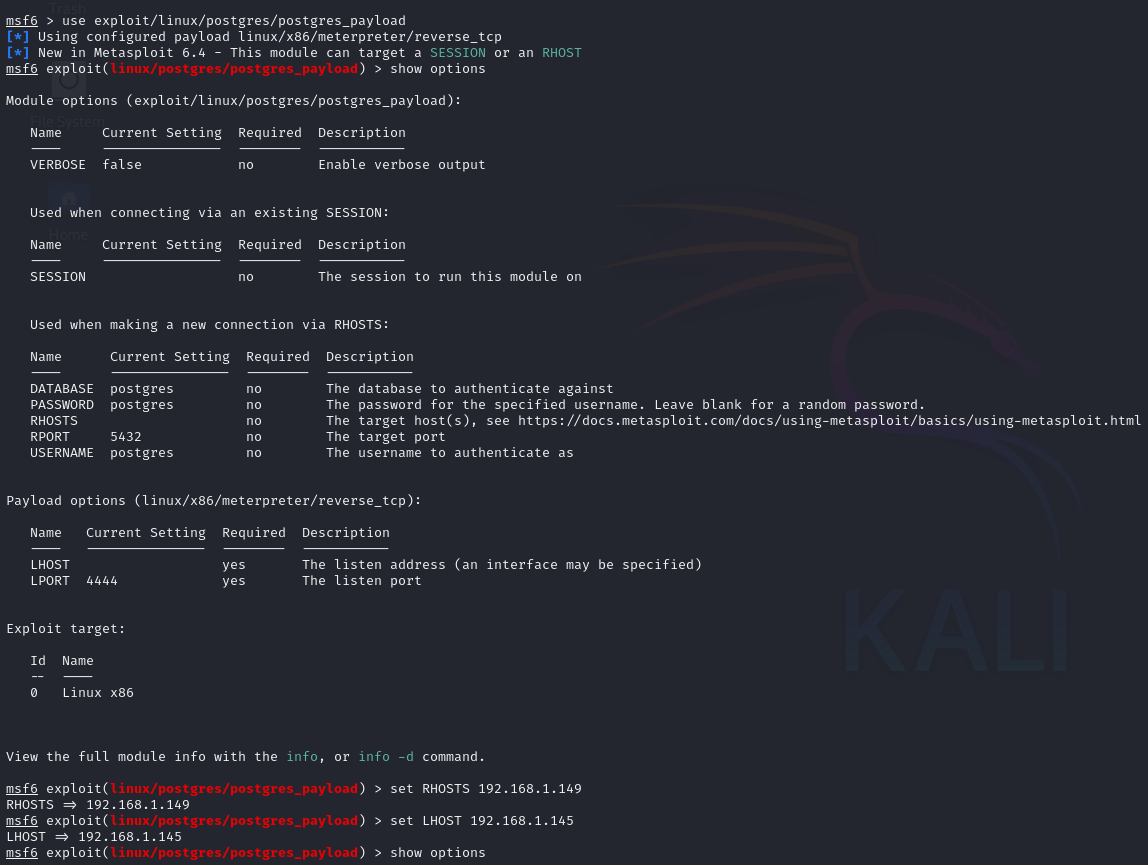
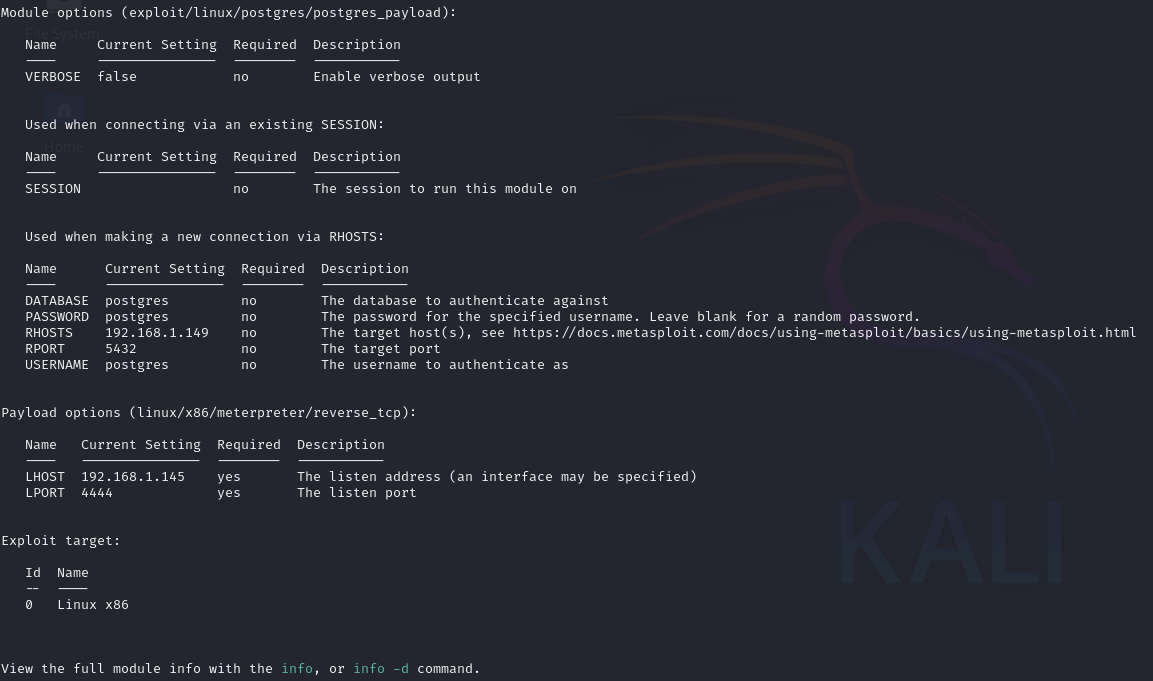
**PRATICA 13 NOVEMBRE 2024**

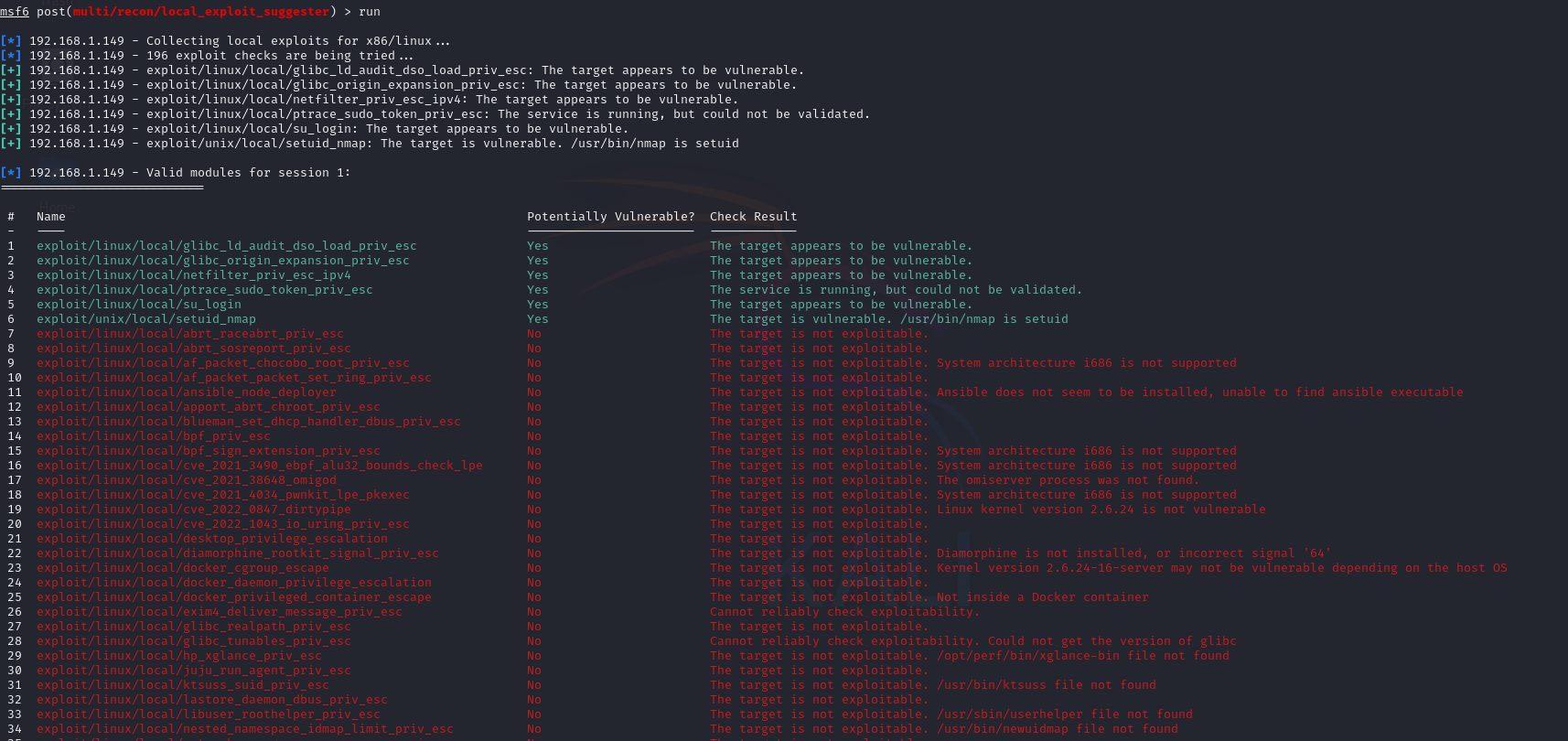
**Exploit con Meterpreter**L’obiettivo di oggi è utilizzare Metasploit su Kali Linux per bucare la macchina vittima (Metasploitable2) ed effettuare una scalata di privilegi per ottenere una maggiore stabilità.  
  
Come prima cosa avviamo Metasploit e ad avviamo il processo utilizzando il payload suggerito:  


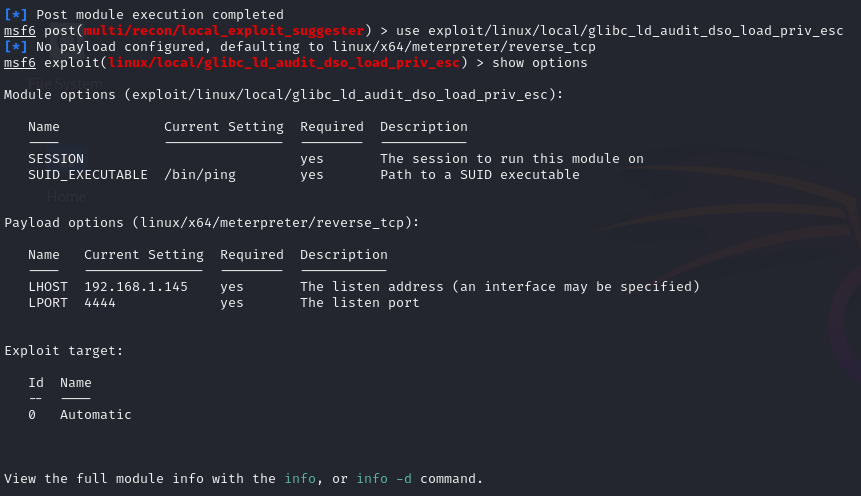
Una volta utilizzato il payload, andremo ad utilizzare il comando show options per vedere quali sono i parametri da settare. In questo caso dovremo settare RHOSTS (192.168.1.149 di Metasploitable2) e LHOST (192.168.1.145 di Linux)

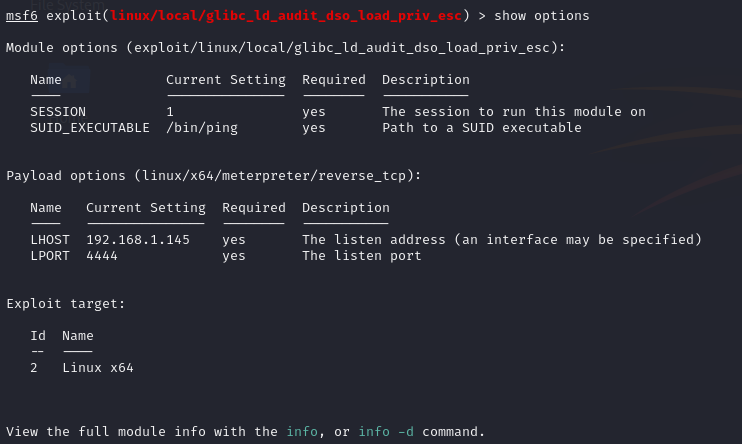
Il risultato sarà il seguente:  


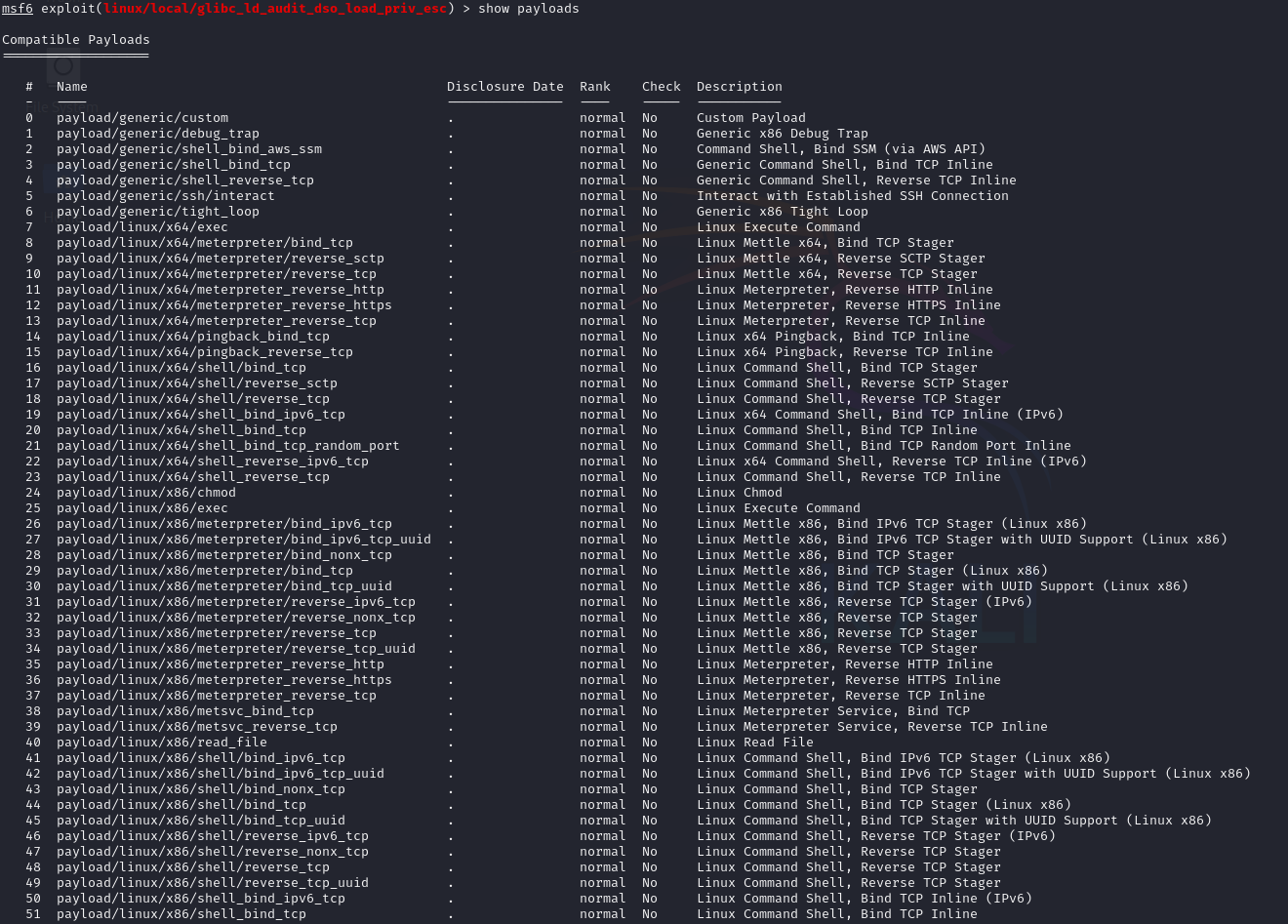
Fatto ciò, avvieremo la procedura tramite il comando run.  

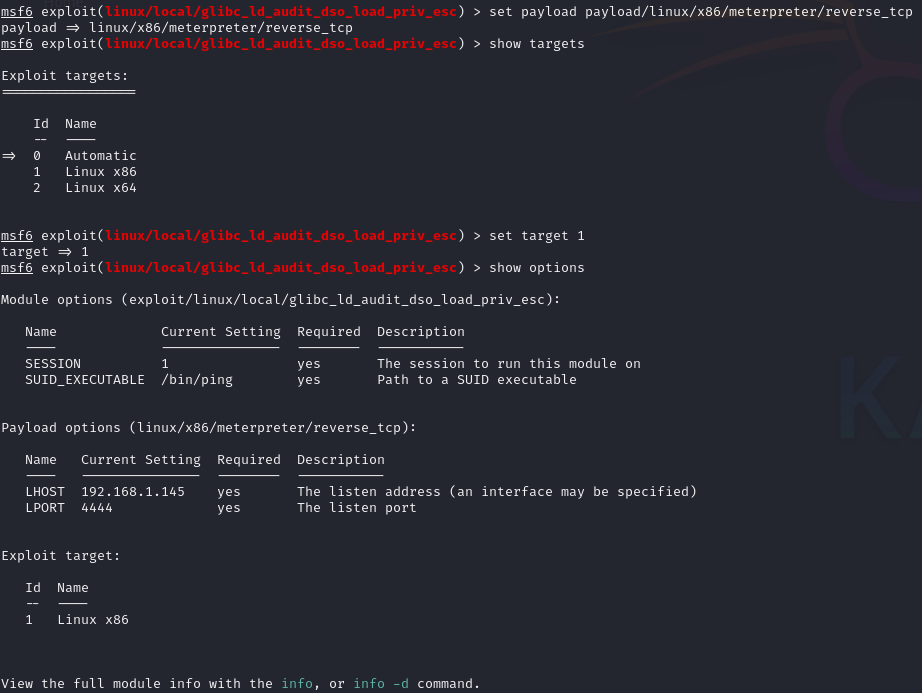

Siamo riusciti ad accedere alla macchina vittima, ma ancora non abbiamo i privilegi di root. Per farlo dovremo andare ad utilizzare un secondo payload.   
Per farlo, dunque, dovremo mettere l’attuale sessione in background e cercare il payload adatto per effettuare la scalata. In questo caso il payload suggester viene in nostro aiuto. Cerchiamolo tramite il comando search e facciamolo partire con il comando run.

Fatto questo, ci ritroveremo davanti una lunga lista di payload utili al nostro scopo. Quelli efficaci verranno evidenziati in verde.  


Fortunatamente il primo payload è quello giusto. Una volta eseguito, utilizzeremo il solito comando show options per vedere quali saranno i parametri da aggiustare:  


In questo caso l’unico parametro da settare sarà la sessione che abbiamo messo in background:  


Una volta impostata la sessione, notiamo che c’è un’incompatibilità con la versione del payload, dato che dovremo utilizzarne con versione x86. Per fare ciò andremo ad utilizzare il comando show payloads e sceglieremo il più adatto al nostro scopo:  


Selezionato il payload adatto lo andremo a selezionare, impostando i parametri corretto tramite l’utilizzo di show options:  


Eseguendo il programma, finalmente avremo effettuato la scalata di privilegi necessaria per arrivare al livello root. Per controllare basterà eseguire il comando getuid e noteremo finalmente che abbiamo raggiunto il nostro obiettivo:  
