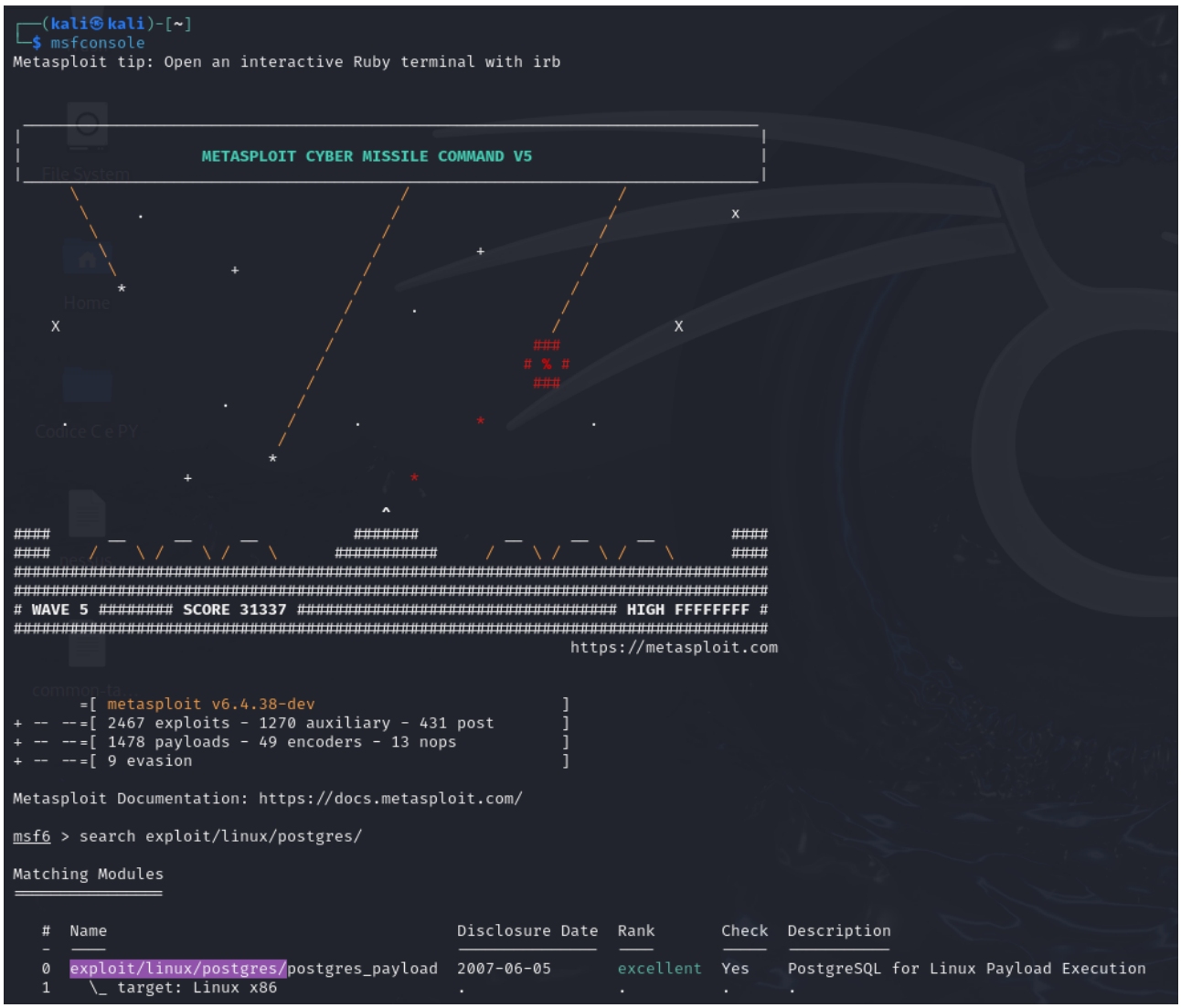
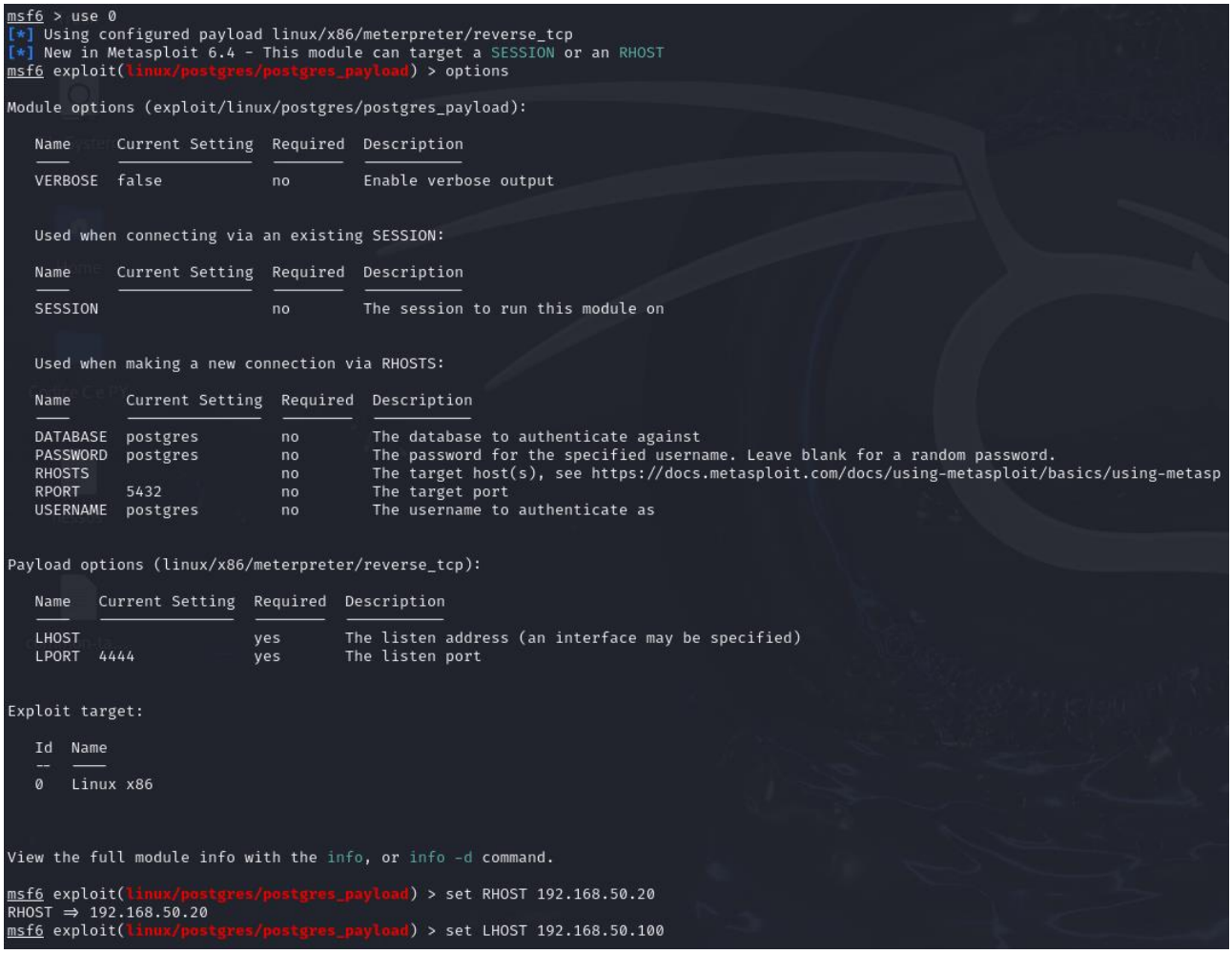
Escalation di privilegi

L’esercizio di oggi prevede l’escalation di privilegi per passare da un utente limitato a root utilizzando solo i mezzi forniti da msfconsole.

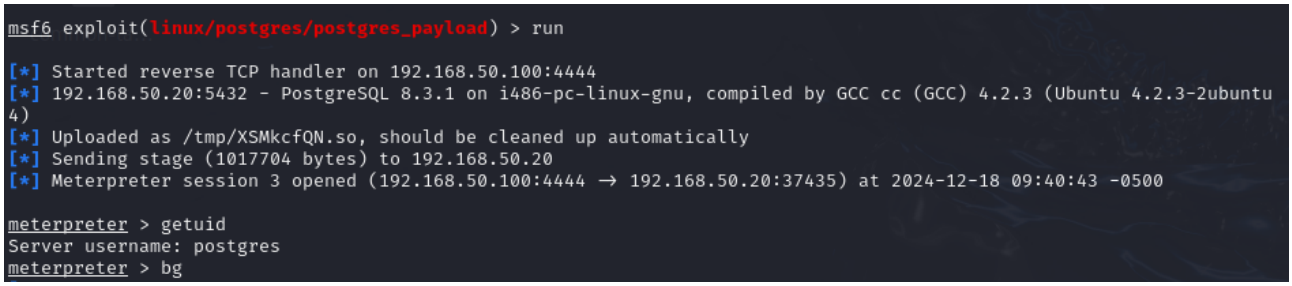
Ho aperto il terminale di kali e ho avviato ‘msfconsole’ e ho cercato l’exploit con il comando ‘search exploit/linux/postgres’.



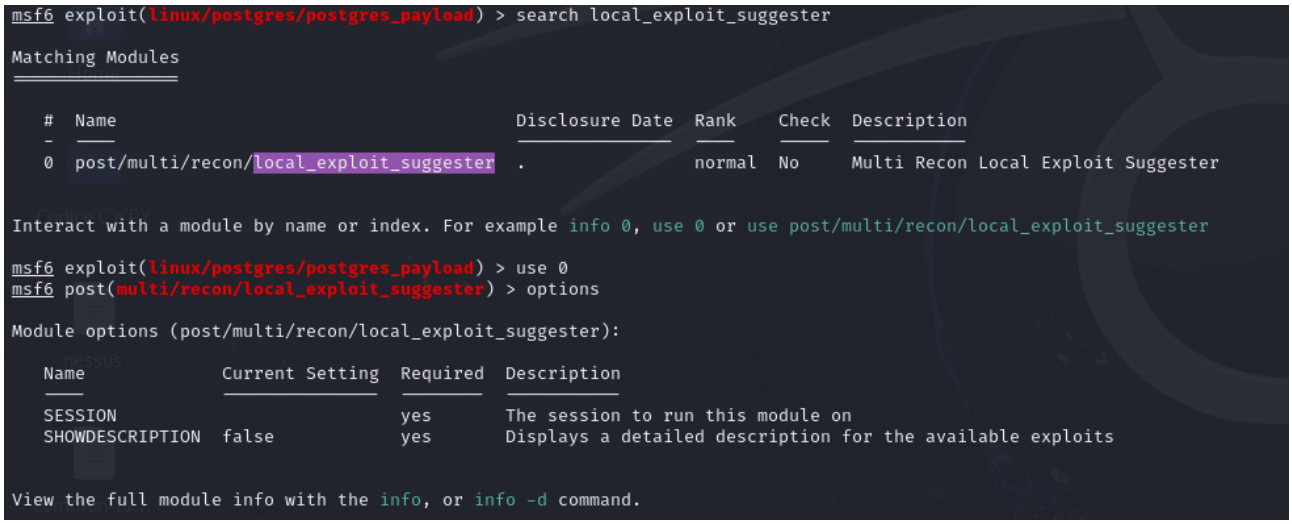
Ho usato il modulo ‘0’ con il comando ‘use 0’, con il comando ‘options’ ho controllato la configurazione e quindi con ‘set’ ho settato l’RHOST e LHOST.



Quindi ho fatto partire l’exploit con il comando ‘run’ ed ero dentro con meterpreter ma con username postgres e quindi ho mandato l’exploit in background con ‘bg’.

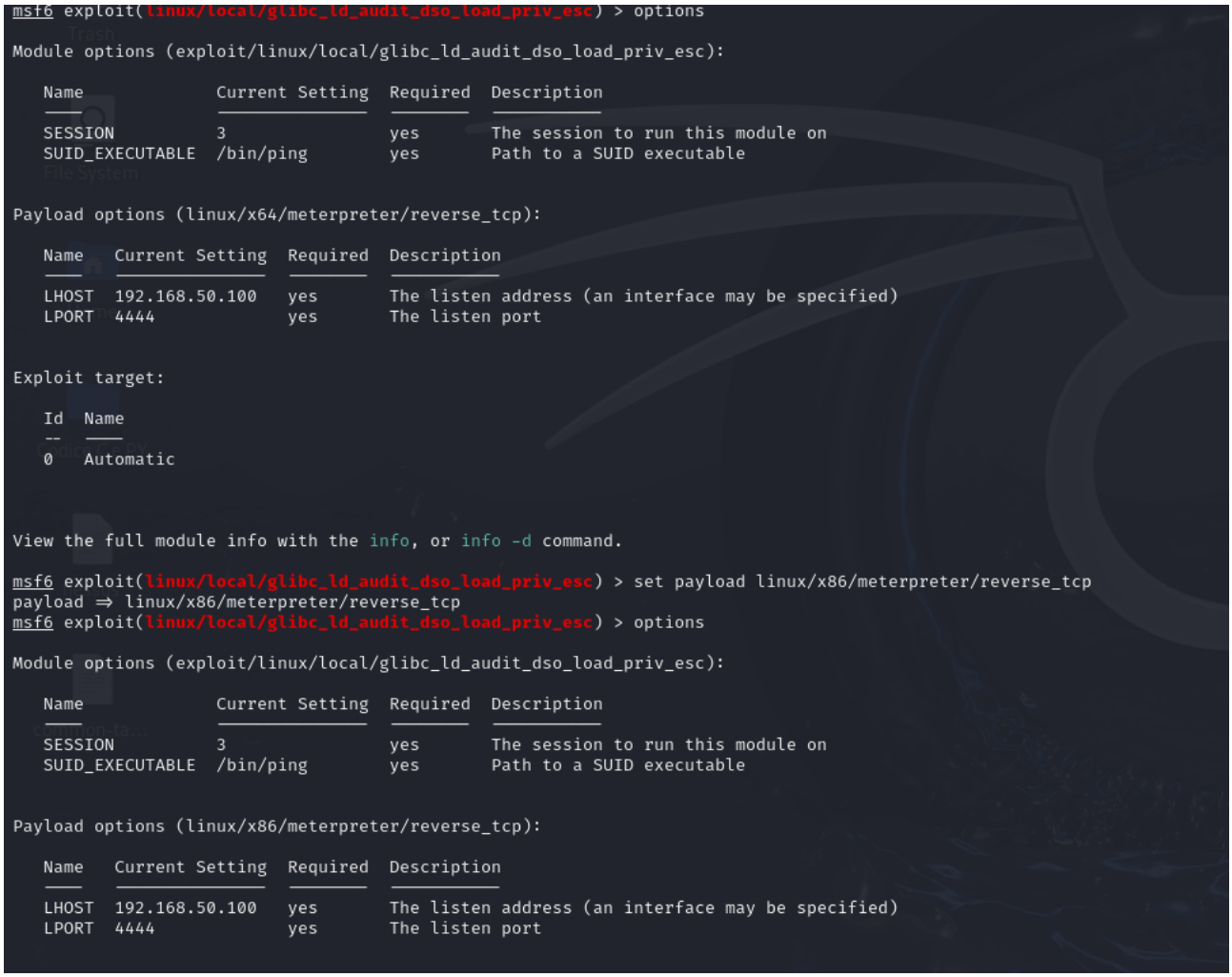


Ho cercato un post per trovare le vulnerabilità della macchina con ‘search local_exploit_suggester’ e ho scelto il post 0 e l’ho usato con ‘use 0’ e con il comando ‘options’ ho controllato la configurazione.



Ho settato la sessione con ‘set session 3’ e ho ricontrollato ‘options’ e vedendo che tutto era configurato esattamente ho lanciato l’exploit con ‘run’ e mi ha dato le vulnerabilità della macchina.

Ho preso il primo exploit e l'ho settato inserendo la sessione, poi grazie al suggerimento del prof, ho notato che il payload era di default a x64 e quindi con il comando 'set' ho modificato in x86. Ho ricontrollato 'options' ed era ben configurato.



Infine ho lanciato l'exploit con 'run' e una volta dentro con meterpreter con il comando 'getuid' ho controllato e sono diventato root.