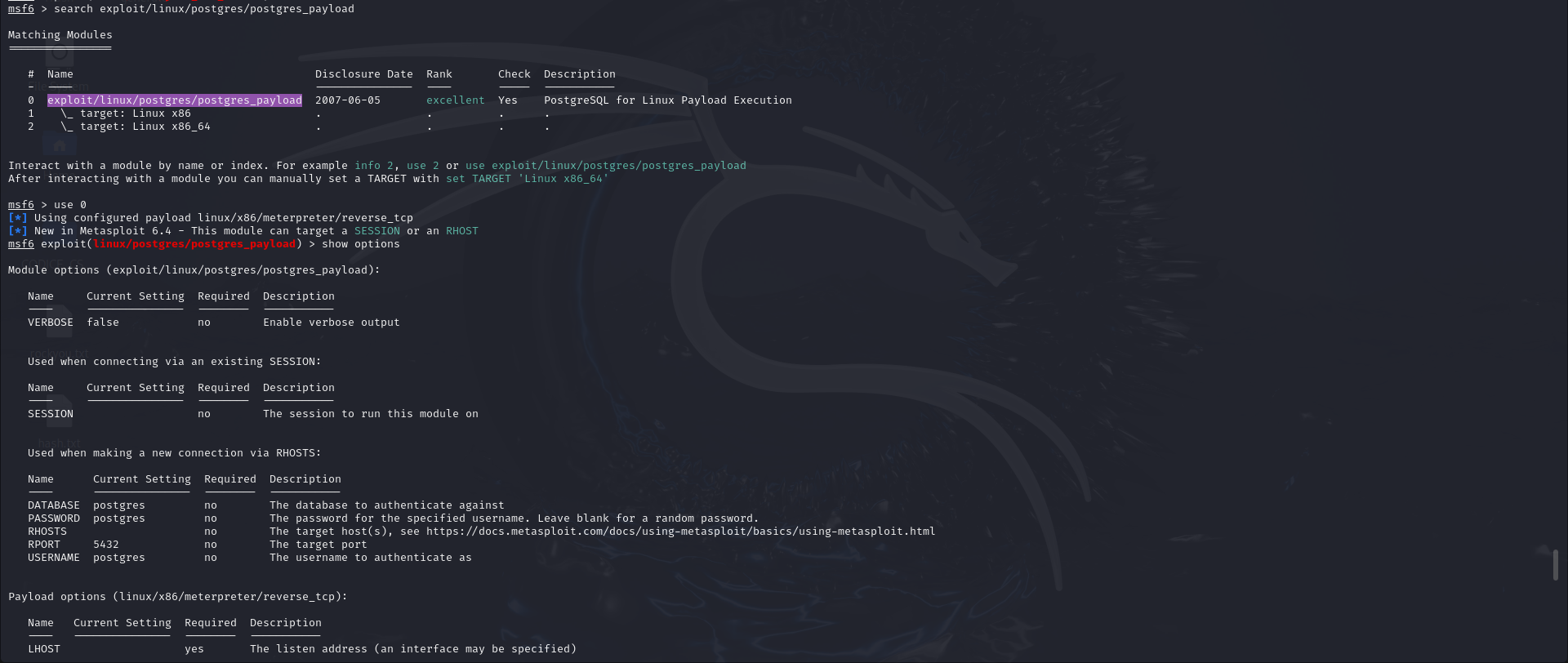
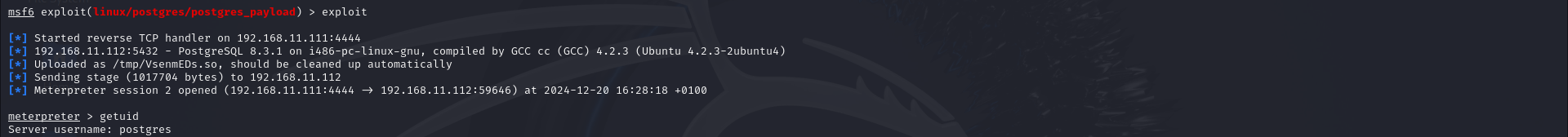
entro in metasploit e ricerco il payload indicato dall’esercizio. dopo di che, visualizzo le impostazioni presenti

setto l’rhost con l’ip della metasploitable e l’lhost con l’ip della kali



lancio l’attacco, poi con il comando getuid verifico l’utente attuale (postgres)

metto la sessione in background, ricerco vulnerabilità locali da poter sfruttare. una volta scelta e lanciata, sempre con il comando getuid possiamo vedere come da utente postgres sono passato ad essere root