S7-L3

ESERCIZIO

Usando il modulo :

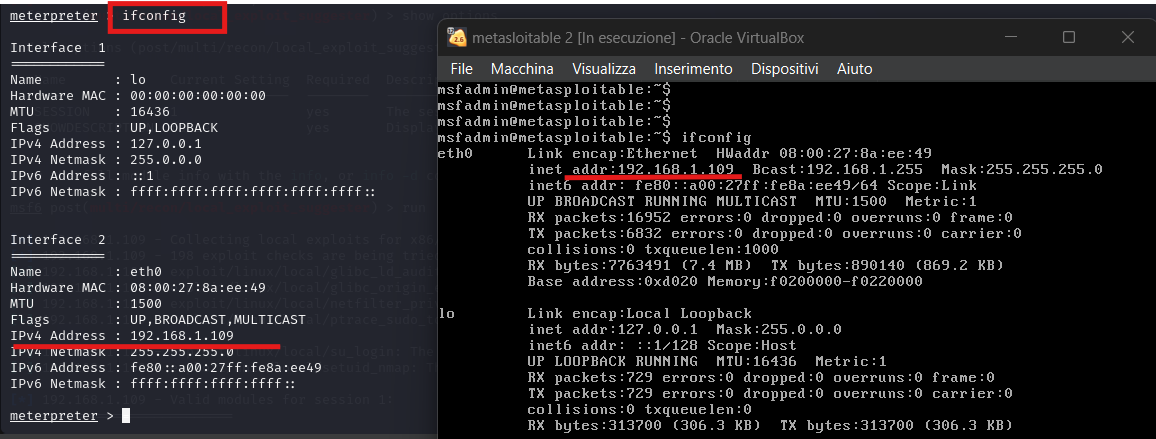
exploit/linux/postgres/postgres\_payload

per sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable 2. Eseguiamo l'exploit per ottenere una sessione Meterpreter sul sistema target.

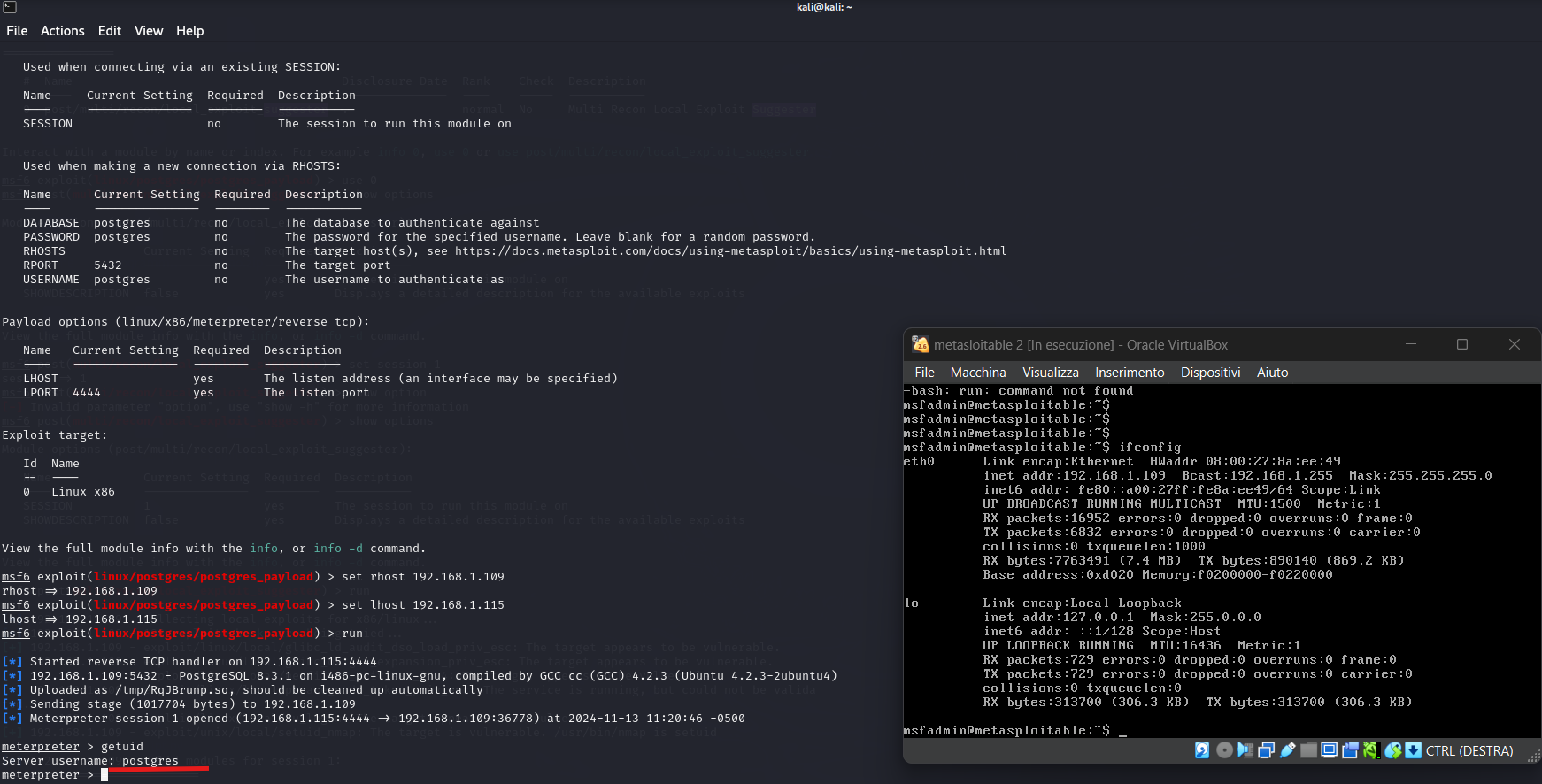
Una volta ottenuta la sessione Meterpreter, il nostro compito è di eseguire un'escalation di privilegi per passare da un utente limitato a root utilizzando solo i mezzi forniti da msfconsole.

SVOLGIMENTO

Per lo svolgimento una volta essersi accertati che le macchine pingano e mandando il comando “msfconsole” procediamo fino ad arrivare all’exloit e mandando il comando “ifconfig” vediamo che ci siamo impossessati della macchina target.



Mandando il comando : “ getuid” possiamo vedere l’identità dell’utente corrente, in questo caso ci darà come risultato “ postgrest” che vuol dire che siamo ancora ospiti.



Per arrivare a diventare root dovremmo eseguire una serie di passaggi.

Intanto dovremmo mettere una sessione Meterpreter in **background**.

Questo serve per tornare alla console principale di Metasploit (msfconsole) senza interrompere la connessione attiva con il sistema compromesso.

Successivamente dovremmo aprire un’altra **sessione** per fare il secondo exploit.

Scaricati i payload appropiati per diventare root possiamo vedere come siamo adesso diventati root.

