ESERCIZIO DI OGGI S7/L3

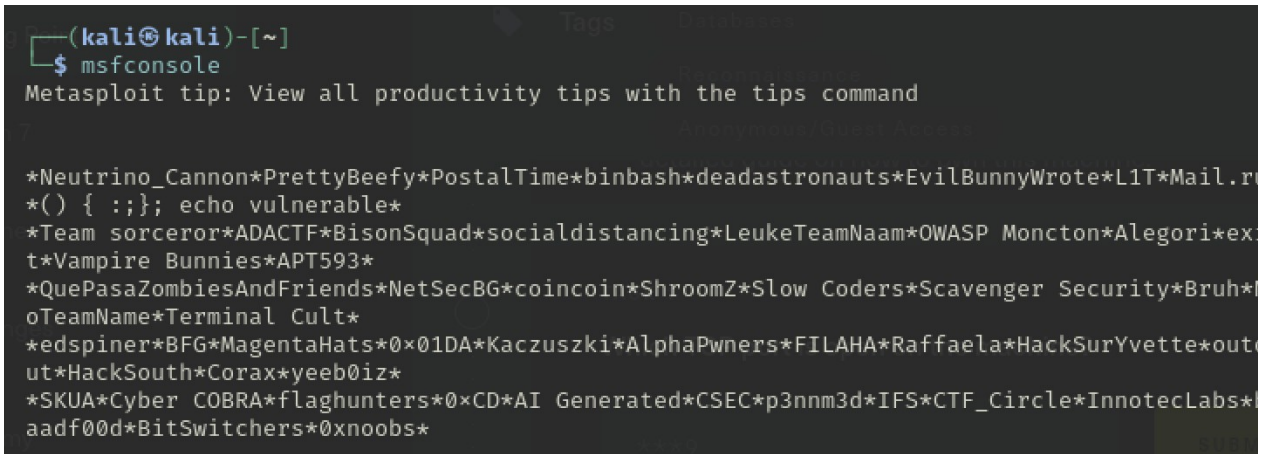
Usa il modulo exploit/ linux /postgres /postgres_payload PostgreSQL di Metasploitable 2.

Esegui l'exploit per ottenere una sessione Meterpreter sul sistema target. Esercizio Esercizio per sfruttare una vulnerabilità nel servizio

La prima cosa da fare è assicurarsi che le due macchine, Metasploit e Kali, comunichino tra di loro. Per verificare ciò, eseguiamo il seguente comando su entrambi i terminali:

ping

Verificata la corretta connessione, entriamo nella libreria di Metasploit come si evince nella schermata successiva

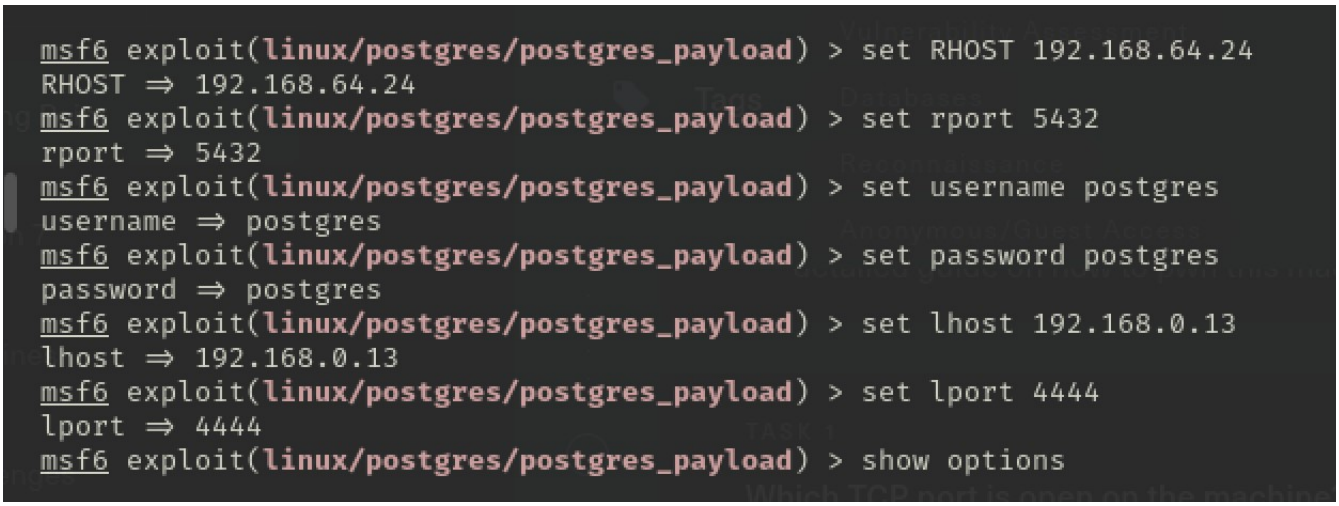


Entrati nella libreria,

eseguiamo il comando sottostante per utilizzare la libreria PostgreSQL

Di seguito trovate i vari dettagli di configurazione. Quelli mostrati nell'immagine sono i miei personali;

Ps. Se si intende eseguire la stessa configurazione, è necessario modificare RHOSTS, LHOST e LPORT



Conclusa la configurazione, per effettuare un test si esegue il comando exploit, come mostrato nell'immagine sottostante