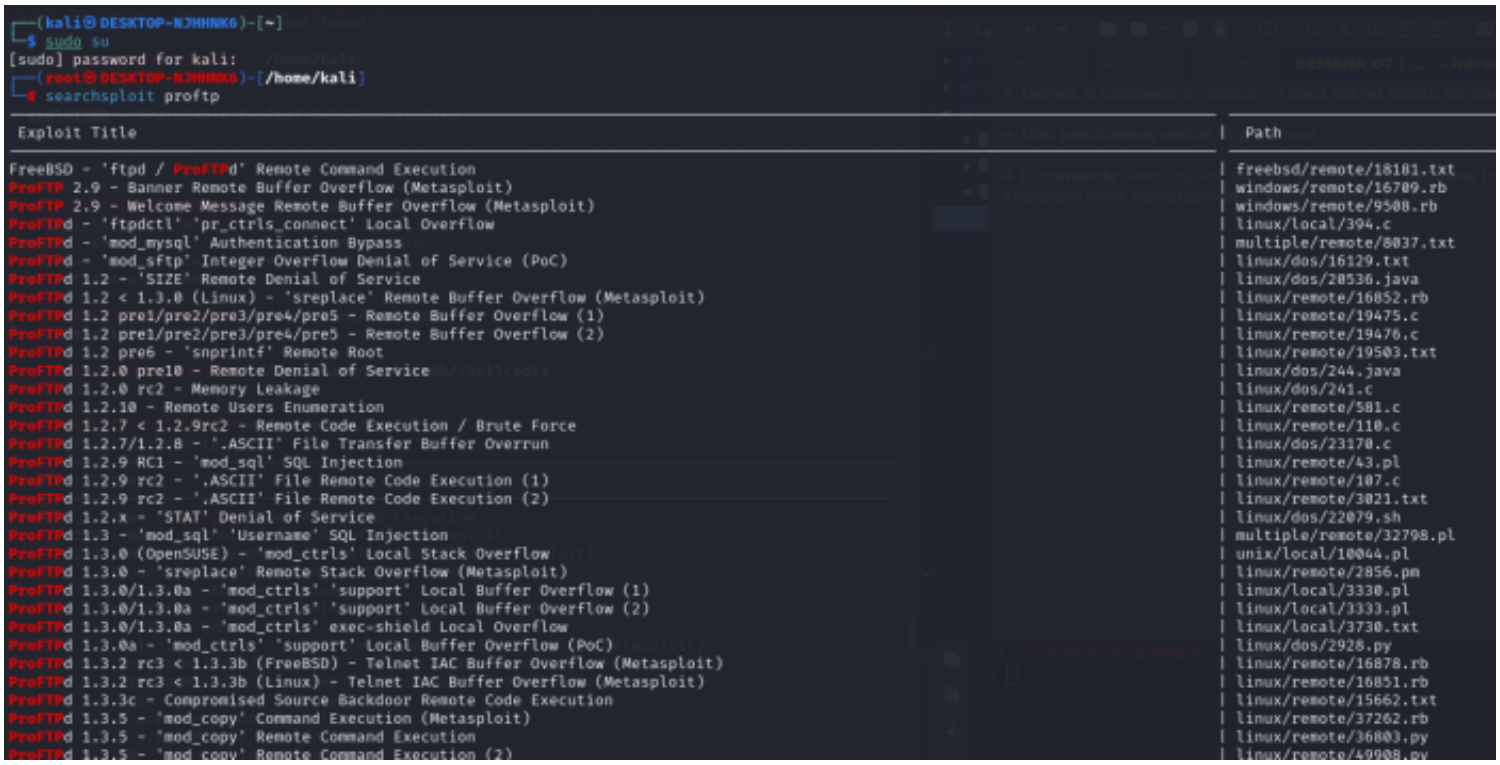
Metasploit Framework - Introdução

+ Demos o comando exploitdb -h para entrar direto no diretório /usr/share/exploitdb

+ Não precisamos entrar lá para isso

+ O comando searchsploit proftpd permite que vejamos todos os exploits que exploram essa vulnerabilidade armazenados no kali



+ Para gerenciar as bases de dados do metasploit,

`msfdb`

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# msfdb

Manage the metasploit framework database

You can use an specific port number for the
PostgreSQL connection setting the PGPORT variable
in the current shell.

Example: PGPORT=5433 msfdb init

  msfdb init     # start and initialize the database
  msfdb reinit   # delete and reinitialize the database
  msfdb delete   # delete database and stop using it
  msfdb start    # start the database
  msfdb stop     # stop the database
  msfdb status   # check service status
  msfdb run      # start the database and run msfconsole
```

+ Quando analisamos seu status, podemos ver se há ou não uma base de dados rodando

```
msfdb status
```

→ No caso acima, não tínhamos nenhuma

+ Antes de subir uma base de dados, é bom atualizarmos nosso sistema

```
apt update; apt install metasploit-framework
```

+ Para iniciar uma base de dados, executamos

```
systemctl start postgresql
```

+ Ao verificarmos novamente o status do msfbd:

```
msfdb status
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# msfdb status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/usr/lib/systemd/system/postgresql.service; disabled; preset: disabled)
     Active: active (exited) since Fri 2024-02-02 22:24:33 -03; 3s ago
    Process: 67896 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 67896 (code=exited, status=0/SUCCESS)
        CPU: 2ms

Feb 02 22:24:33 DESKTOP-NJHHNK6 systemd[1]: Starting postgresql.service - PostgreSQL RDBMS...
Feb 02 22:24:33 DESKTOP-NJHHNK6 systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.

COMMAND    PID     USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
postgres 67862 postgres    6u  IPv6 320240      0t0  TCP localhost:5432 (LISTEN)
postgres 67862 postgres    7u  IPv4 320241      0t0  TCP localhost:5432 (LISTEN)

UID          PID    PPID  C STIME TTY      STAT   TIME CMD
postgres   67862       1  0 22:24 ?        Ss     0:00 /usr/lib/postgresql/16/bin/postgres -D

[i] No configuration file found
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# netstat -nlpt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      67862/postgres
tcp6       0      0 ::1:5432                :::*                    LISTEN      67862/postgres
```

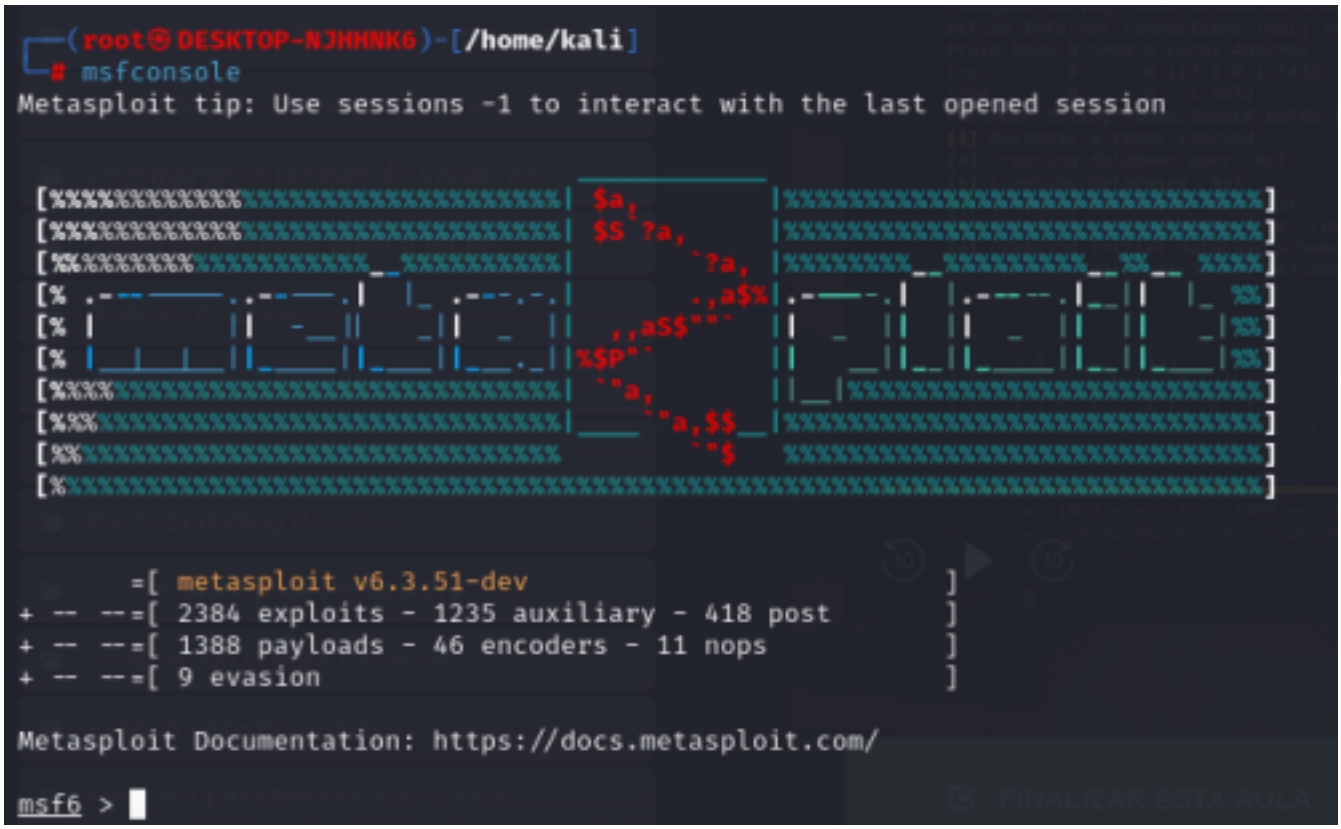
+ Nesse caso, apenas subimos o servidor da base dados. Para inciá-lo, fazemos

`msfdb init`

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
[+] Creating databases 'msf_test'
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

+ Para chamar o metasploit:

`msfconsole`


(root㉿DESKTOP-NJHHNK6)-[/home/kali]
msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session
=[metasploit v6.3.51-dev
+ -- --=[2384 exploits - 1235 auxiliary - 418 post
+ -- --=[1388 payloads - 46 encoders - 11 nops
+ -- --=[9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 >