

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

```
(kali@DESKTOP-R3HHNK6)-[~]
$ sudo su
[sudo] password for kali:
(kali@DESKTOP-R3HHNK6)-[~/home/kali]
$ searchsploit proftpd
```

Exploit Title	Path
FreeBSD - 'ftpd / ProFTPD' Remote Command Execution	freebsd/remote/18181.txt
ProFTPD 2.9 - Banner Remote Buffer Overflow (Metasploit)	windows/remote/16789.rb
ProFTPD 2.9 - Welcome Message Remote Buffer Overflow (Metasploit)	windows/remote/9508.rb
ProFTPD - 'ftpdctl' 'pr_ctrls_connect' Local Overflow	linux/local/394.c
ProFTPD - 'mod_mysql' Authentication Bypass	multiple/remote/8037.txt
ProFTPD - 'mod_sftp' Integer Overflow Denial of Service (PoC)	linux/dos/16129.txt
ProFTPD 1.2 - 'SIZE' Remote Denial of Service	linux/dos/28536.java
ProFTPD 1.2 < 1.3.0 (Linux) - 'sreplace' Remote Buffer Overflow (Metasploit)	linux/remote/16852.rb
ProFTPD 1.2 pre1/pre2/pre3/pre4/pre5 - Remote Buffer Overflow (1)	linux/remote/19475.c
ProFTPD 1.2 pre1/pre2/pre3/pre4/pre5 - Remote Buffer Overflow (2)	linux/remote/19476.c
ProFTPD 1.2 pre6 - 'snprintf' Remote Root	linux/remote/19503.txt
ProFTPD 1.2.0 pre10 - Remote Denial of Service	linux/dos/244.java
ProFTPD 1.2.0 rc2 - Memory Leakage	linux/dos/241.c
ProFTPD 1.2.10 - Remote Users Enumeration	linux/remote/581.c
ProFTPD 1.2.7 < 1.2.9rc2 - Remote Code Execution / Brute Force	linux/remote/110.c
ProFTPD 1.2.7/1.2.8 - '.ASCII' File Transfer Buffer Overrun	linux/dos/23170.c
ProFTPD 1.2.9 RC1 - 'mod_sql' SQL Injection	linux/remote/43.pl
ProFTPD 1.2.9 rc2 - '.ASCII' File Remote Code Execution (1)	linux/remote/107.c
ProFTPD 1.2.9 rc2 - '.ASCII' File Remote Code Execution (2)	linux/remote/3021.txt
ProFTPD 1.2.x - 'STAT' Denial of Service	linux/dos/22079.sh
ProFTPD 1.3 - 'mod_sql' 'Username' SQL Injection	multiple/remote/32798.pl
ProFTPD 1.3.0 (OpenSUSE) - 'mod_ctrls' Local Stack Overflow	unix/local/10044.pl
ProFTPD 1.3.0 - 'sreplace' Remote Stack Overflow (Metasploit)	linux/remote/2856.pm
ProFTPD 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (1)	linux/local/3330.pl
ProFTPD 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (2)	linux/local/3333.pl
ProFTPD 1.3.0/1.3.0a - 'mod_ctrls' exec-shield Local Overflow	linux/local/3730.txt
ProFTPD 1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (PoC)	linux/dos/2928.py
ProFTPD 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit)	linux/remote/16878.rb
ProFTPD 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)	linux/remote/16851.rb
ProFTPD 1.3.3c - Compromised Source Backdoor Remote Code Execution	linux/remote/15662.txt
ProFTPD 1.3.5 - 'mod_copy' Command Execution (Metasploit)	linux/remote/37262.rb
ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution	linux/remote/36803.py
ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution (2)	linux/remote/49908.py

- + 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
```

```
(root@DESKTOP-NJHHNK6)-[/home/kali]
# msfdb status
o postgresql.service - PostgreSQL RDBMS
  Loaded: loaded (/usr/lib/systemd/system/postgresql.service; disabled; preset: disabled)
  Active: inactive (dead)
[i] No network service running
[i] No configuration file found
```

→ 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 iniciá-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
```

```
[#####] $a, [#####]
[#####] $S ?a, [#####]
[#####] ?a, [#####]
[#####] a$% [#####]
[#####] aS$ [#####]
[#####] %P" [#####]
[#####] "a, "$ [#####]
[#####] [#####]
[#####] [#####]
```

```
=[ 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 > 
```

FINALIZAR ESTA AULA