

\_(https://www.offensive-security.com)

COURSES AND CERTIFICATIONS (/COURSES-AND-CERTIFICATIONS/)

LABS (HTTPS://WWW.OFFENSIVE-SECURITY.COM/LABS/)

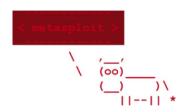
PENTEST
SERVICES
(HTTPS://WWW.OFFENSIVESECURITY.COM
/PENETRATION-TESTING/)

TRAINING FOR CENTRALION

FOR OFISTRATION)
(HTTPS://WWW.OFFENSIVESECURITY.COM/OFFSECFOR-ORGS/)

WHY
OFFSEC?
(HTTPS://WWW.OFFENSIVESECURITY.COM/WHYOFFSEC/)

KALI AND
INFOSEC TOOLS
(HTTPS://WWW.OFFENSIVESECURITY.COM
/COMMUNITY-PROJECTS/)



### TABLE OF CONTENTS

METASPLOIT UNLEASHED (HTTPS://WWW.OFFENSIVE-SECURITY.COM /METASPLOIT-UNLEASHED/)

DONATE – HELP FEED A CHILD (HTTPS://WWW.OFFENSIVE-SECURITY.COM /METASPLOIT-UNLEASHED /DONATE/)

INTRODUCTION ▼
(HTTPS://WWW.OFFENSIVESECURITY.COM
/METASPLOITUNLEASHED
/INTRODUCTION/)

METASPLOIT FUNDAMENTALS
(HTTPS://WWW.OFFENSIVE-SECURITY.COM
/METASPLOIT-UNLEASHED
/METASPLOIT-FUNDAMENTALS/)

MSFCLI (HTTPS://WWW.OFFENSIVE-SECURITY.COM /METASPLOIT-UNLEASHED /MSFCLI/)

MSFCONSOLE ▼ (HTTPS://WWW.OFFENSIVE-SECURITY.COM /METASPLOIT-UNLEASHED /MSFCONSOLE/)

MSFCONSOLE COMMANDS

# USING THE DATABASE IN METASPLOIT

#### **CONTENTS**

- 1 SETUP
- 2 WORKSPACES
- 3 IMPORTING & SCANNING
- 4 BACKING UP
- 5 HOSTS
- 6 SETTING UP MODULES
- 7 SERVICES
- 8 CSV EXPORT
- 9 CREDS
- 10 LOOT

## SETUP OUR METASPLOIT DATABASE

In Kali, you will need to start up the postgresql server before using the database.

root@kali:~# systemctl start postgresql

After starting postgresql you need to create and initialize the msf database with **msfdb init** 

root@kali:~# msfdb init
Creating database user 'msf'
Enter password for new role:
Enter it again:
Creating databases 'msf' and 'msf\_test'
Creating configuration file in /usr/share/metasp

#### COURSES

Penetration Testing with Kali Linux (PWK) (https://www.offensivesecurity.com/pwk-oscp/)

Advanced Web Attacks and **Exploitation (AWAE)** (https://www.offensivesecurity.com/awae-oswe/)

Cracking the Perimeter (CTP)

(https://www.offensivesecurity.com/ctp-osce/)

**Advanced Windows** Exploitation (AWE) (https://www.offensivesecurity.com/awe-osee/)

Offensive Security Wireless Attacks (WiFu) (https://www.offensivesecurity.com/wifu-oswp/)

#### CERTIFICATIONS

OSWE Web Expert (https://www.offensivesecurity.com/awae-oswe/)

**OSCP** Certified Professional (https://www.offensivesecurity.com/pwk-oscp/)

OSCE Certified Expert (https://www.offensivesecurity.com/ctp-osce/)

**OSWP Wireless** Professional (https://www.offensivesecurity.com/wifu-oswp/)

**OSEE Exploitation Expert** (https://www.offensivesecurity.com/awe-osee/)

#### SECURITY SERVICES

OffSec for Orgs (https://www.offensivesecurity.com/offsec-fororgs/)

Proving Grounds (Hosted Labs) (https://www.offensivesecurity.com/labs/)

**Penetration Testing** Services (https://www.offensivesecurity.com/penetrationtesting/)

Advanced Attack Simulation (https://www.offensivesecurity.com/penetrationtesting/#other-services)

**Application Security** Assessment (https://www.offensivesecurity.com/penetrationtesting/#asa)

#### ABOUT OFFSEC (HTTPS://WWW.OFFENSIVEFOOLS SECURITY.COM /WHY-OFFSEC/)

Try Harder Ethos (/whyoffsec/#try-harder)

Leadership Team (https://www.offensivesecurity.com/leadershipteam/)

Blog (https://www.offensivesecurity com/blog/)

### **OPEN SOURCE**

#### SECURITY.COM /COMMUNITY-PROJECTS/)

Kali Linux (https://www.kali.org/)

Kali NetHunter (https://www.kali.org/kalilinux-nethunter/)

**Exploit Database** (https://www.exploit-

#### DOWNLOADS

(HTTPS://WWW.OFFENSIVE Sali Linux Virtual Machines (https://www.offensivesecurity.com/kali-linux-vmvmware-virtualbox-imagedownload/)

> Kali Linux ARM Images (https://www.offensivesecurity.com/kali-linuxarm-images/)

Kali Linux NetHunter **Images**