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

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

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

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

TRAINING FOR ORGS (HTTPS://WWW.OFFENSIVE-SECURITY.COM/OFFSEC-FOR-ORGS/)

ENROLL (/REGISTRATION)

WHY OFFSEC? (HTTPS://WWW.OFFENSIVE-SECURITY.COM/WHY-OFFSEC/)

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

USING THE DATABASE IN METASPLOIT

TABLE OF CONTENTS

CONTENTS

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.offensive-security.com/pwk-oscp/)

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

Cracking the Perimeter (CTP) (https://www.offensive-security.com/ctp-osce/)

Advanced Windows Exploitation (AWE) (https://www.offensive-security.com/awe-osee/)

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

CERTIFICATIONS

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

OSCP Certified Professional (https://www.offensive-security.com/pwk-oscp/)

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

OSWP Wireless Professional (https://www.offensive-security.com/wifu-oswp/)

OSEE Exploitation Expert (https://www.offensive-security.com/awe-osee/)

SECURITY SERVICES

OffSec for Orgs (https://www.offensive-security.com/offsec-for-orgs/)

Proving Grounds (Hosted Labs) (https://www.offensive-security.com/labs/)

Penetration Testing Services (https://www.offensive-security.com/penetration-testing/)

Advanced Attack Simulation (https://www.offensive-security.com/penetration-testing/#other-services)

Application Security Assessment (https://www.offensive-security.com/penetration-testing/#asa)

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

Try Harder Ethos (/why-offsec/#try-harder)

Leadership Team (https://www.offensive-security.com/leadership-team/)

Blog (https://www.offensive-security.com/blog/)

OPEN SOURCE TOOLS (HTTPS://WWW.OFFENSIVE-SECURITY.COM/COMMUNITY-PROJECTS/)

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

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

Exploit Database (https://www.exploit-

DOWNLOADS

Kali Linux Virtual Machines (https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/)

Kali Linux ARM Images (https://www.offensive-security.com/kali-linux-arm-images/)

Kali Linux NetHunter Images (https://www.offensive-