

Setting up the work Enviornment

Setup and Work with MSF

- We will start off by initializing the MSF database service using the init command

```
sudo msfdb init
```

- Next we will enable the database service to run at boot time using **systemctl** which will save us a lot of time later.

```
sudo systemctl enable postgresql
```

- Now, lets Launch the Metasploit framework.

```
sudo msfconsole
```

- Check if database is connected or not.

```
db_status
```

- To display help.

```
help
```

- To avoid mixing the result, we can create particular workspaces, in that way we can store results in separate Databases.

```
# List all workspaces
```

```
workspace
```

```
# Create a new workspace
```

```
workspace -a pen200
```

- Perform nmap scan within metasploit and store the results.

```
db_nmap -A 192.168.50.202
```

- Once scanning is done, we can check the scanned hosts using the below command.

```
hosts
```

- Check for scanned services using the below command.

```
services
```

```
services -p 8000
```

- Categories of metasploit modules can be view using the below command.

```
show -h
```
