

info

search

exploit

use

jobs

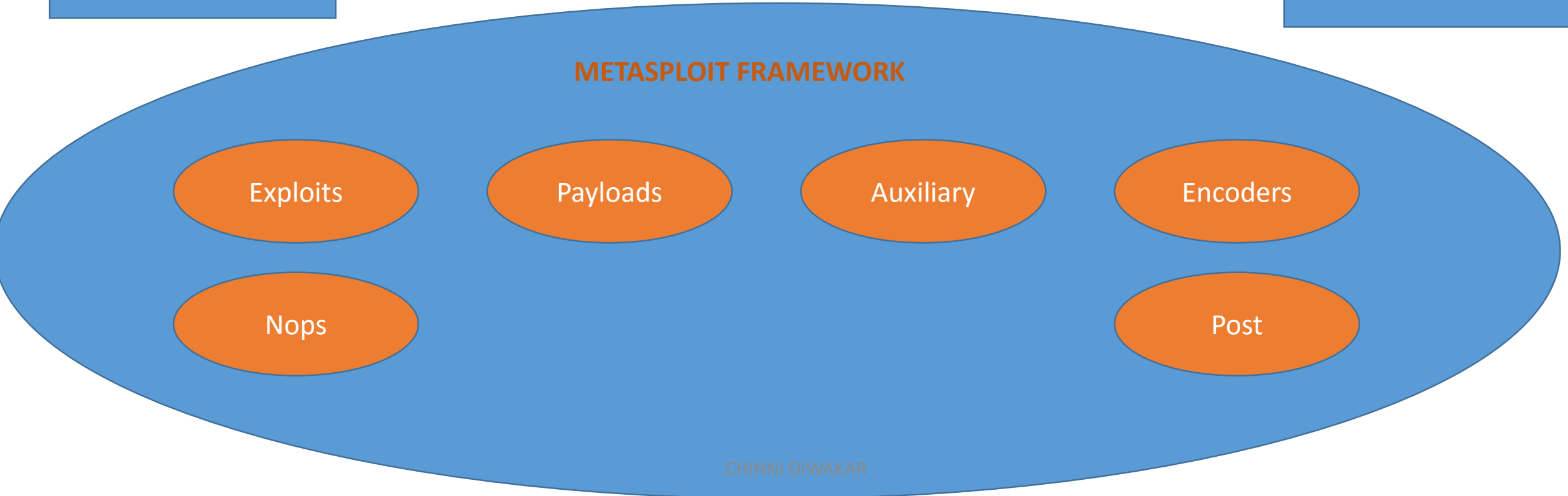
set

sessions

show

unset

kill



# Useful Options

RHOST => VICTIM IP

RPORT => VICTIM PORT

LHOST => ATTACKER IP

LPORT => ATTACKER PORT

SRVHOST => ATTACKER IP or 0.0.0.0

SRVPORT => ATTACKER PORT

URIPATH => /

“IP” refers either private or public ip

search Command Usage: We can use “search” command to search for modules matching with the keyword we give.

Syntax:

```
search <keyword>
```

```
search <exploit code>
```

Example:

```
search vlc
```

```
search chrome
```

```
search java
```

```
search windows
```

```
search ms08_167
```

info Command Usage: We can use “info” command to get information about any module.

Syntax:

```
info <modulename>
```

Example:

```
info post/smart_migrate
```

```
info payload/linux/x86/shell_reverse_tcp
```

```
info exploit/windows/smb/ms08_067_netapi
```

exploit Command Usage: We can use “exploit” command to run any configured exploit on the target

Syntax:

exploit <options>

exploit -j => to run as job for multi sessions

exploit -z => do not connect to session immediately(you have to take control manually)

Example:

exploit -j

exploit -z

use Command Usage: We can use “use” command to select any module which we want to use.

Syntax:

```
use <modulename>
```

Example:

```
use post/smart_migrate
```

```
use payload/linux/x86/shell_reverse_tcp
```

```
use auxiliary/scanner/windows/rdp/ms12_100_maxchannelids
```

set Command Usage: We can use “set” command to set custom options which are required for our selected module

Syntax:

```
set <OPTION> <OPTION PARAMETER>
```

Example:

```
set RHOST 192.168.0.1
```

```
set FILENAME file.exe
```

```
set SESSION 1
```

```
set URIPATH /
```

unset Command Usage: We can use “unset” command to remove custom options which are already set for the selected module

Syntax:

```
unset <OPTION>
```

Example:

```
unset RHOST
```

```
unset FILENAME
```

```
unset URIPATH
```



show Command Usage: We can use “show” command to see the options for any module, or we can list out the available objects in modules

Syntax:

show option

Example:

show exploits => will show available exploits in exploits module

show payloads => will show available payloads in payloads module

show auxiliary => will show available auxiliaries in auxiliary module

show post => will show available posts in post module

show nops => will show available nops in nops module

show encoders=> will show available encoders in encoders module

show options => will show available options for the selected modules

kill Command Usage: we can use “kill” command to terminate an existing session.

Syntax:

```
kill <session id>
```

Example:

```
kill 1
```

```
kill 51
```

```
kill 698
```

jobs Command Usage: we can use “jobs” command to list out available exploit jobs in our attacker machine.

Syntax:

jobs -l => lists out all jobs

jobs -i <job id> => will give info about that job

jobs -k <job id> => to kill given job

jobs -K => to kill all available jobs

Example:

jobs -l

jobs -i 1

jobs -k 1

jobs -K

sessions Command Usage: we can use “sessions” command to list out as well as take control the sessions we have in our Metasploit Framework Console.

Syntax:

sessions -l => To list out available sessions

sessions -i <session id> => To interact with selected session

Example:

sessions -l

sessions -i 2