**Question 1:**

1. ● Create payload for windows.
2. ● Transfer the payload to the victim's machine.
3. ● Exploit the victim's machine.

**Ans**

Payload, in simple terms, are simple scripts that the hackers utilize to interact with a hacked system. Using payloads, they can transfer data to a victim system.

Metasploit payloads can be of three types −

* **Singles** − Singles are very small and designed to create some kind of communication, then move to the next stage. For example, just creating a user.
* **Staged** − It is a payload that an attacker can use to upload a bigger file onto a victim system.
* **Stages** − Stages are payload components that are downloaded by Stagers modules. The various payload stages provide advanced features with no size limits such as Meterpreter and VNC Injection.

**Exploiting**

After vulnerability scanning and vulnerability validation, we have to run and test some scripts (called **exploits**) in order to gain access to a machine and do what we are planning to do.

We have several methods to use exploits. The first and foremost method is to use Armitage GUI which will connect with Metasploit to perform automated exploit testing called HAIL MARY

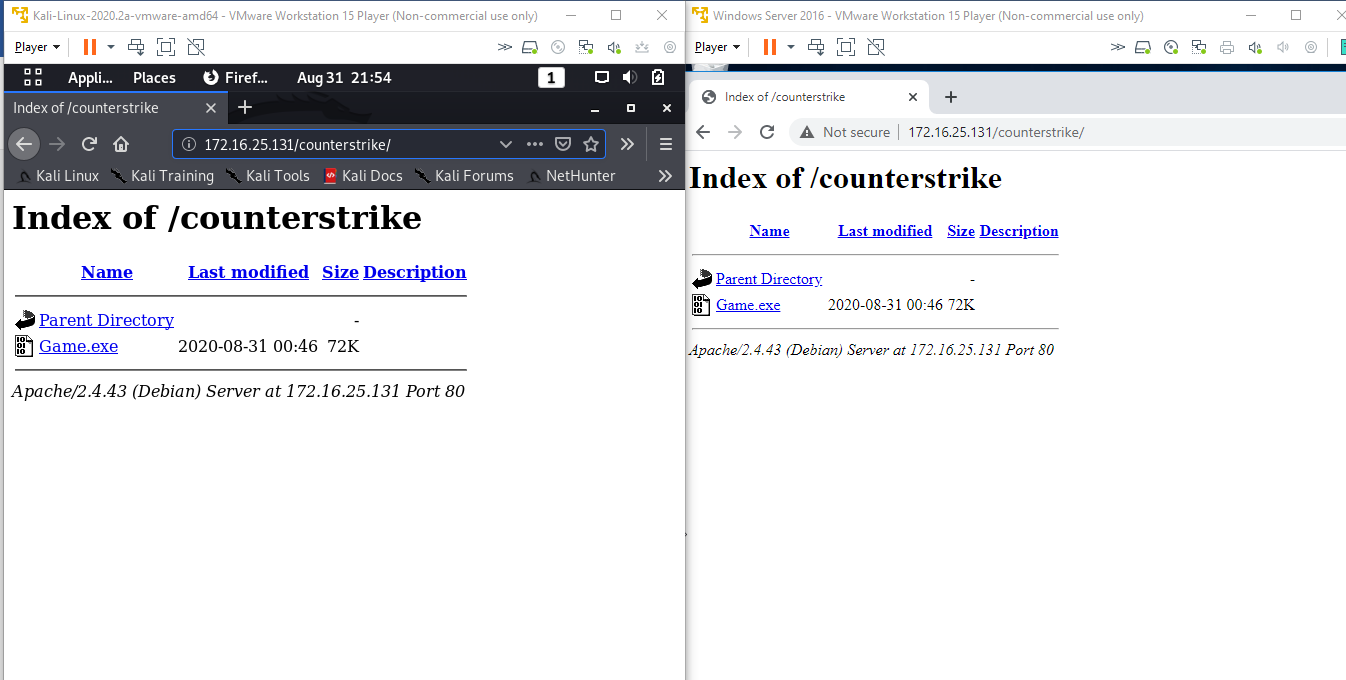
Exploit using Command Prompt

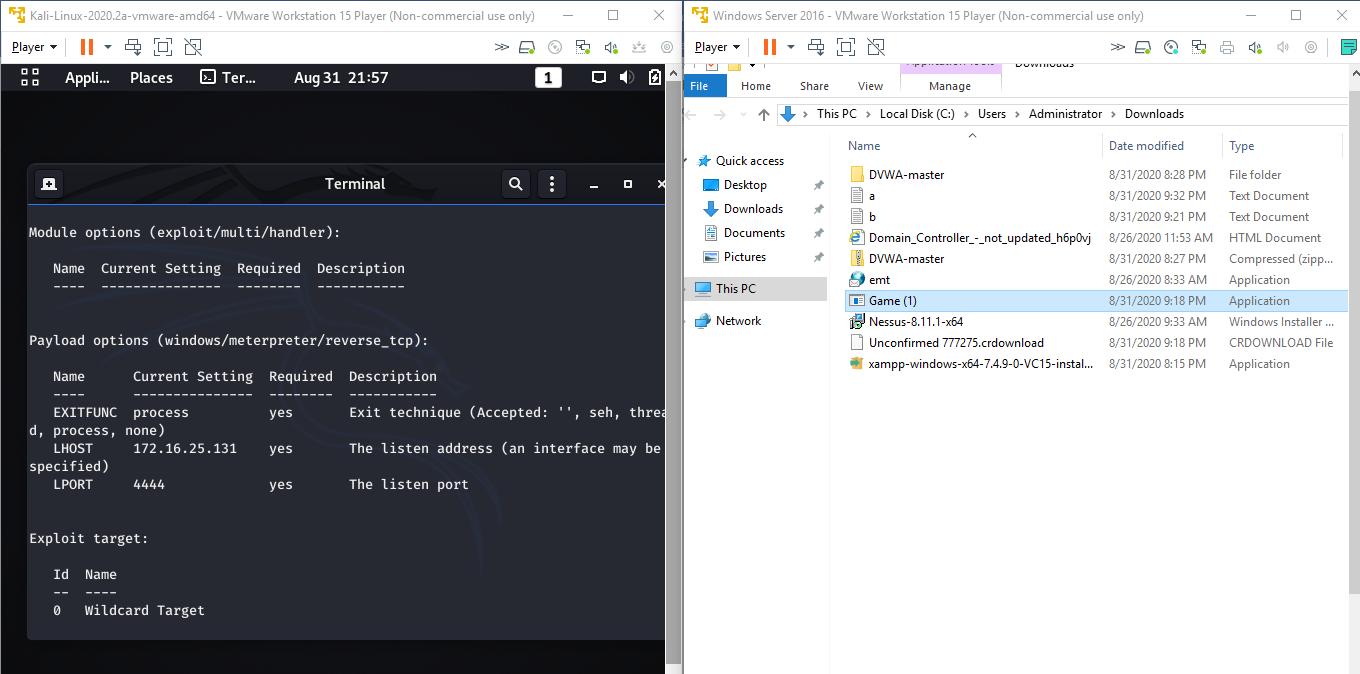
The second way (and probably a little professional way) to use an Exploit is by the Command Prompt.

From the Vulnerability Scanner, we found that the Linux machine that we have for test is vulnerable to FTP service. Now we will use an **exploit** that can work for us

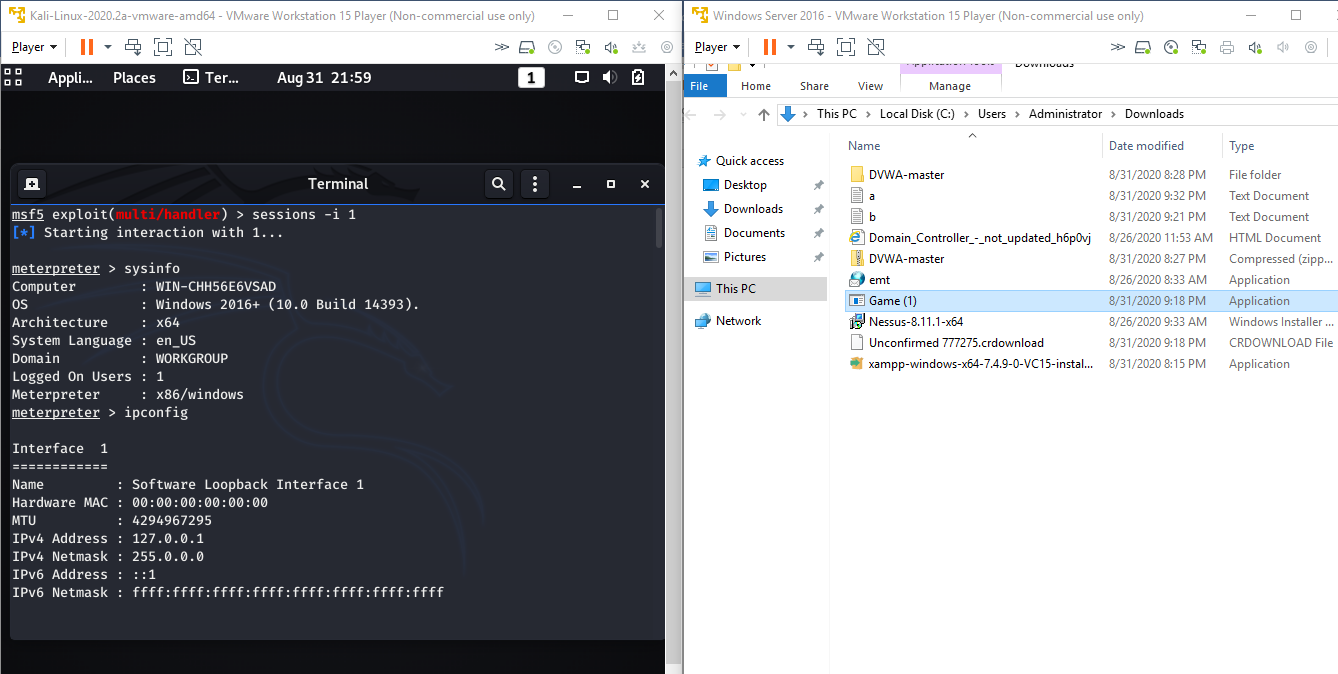
**Steps: -**

Create Game.exe in Kali and tried opening In Victim Machine

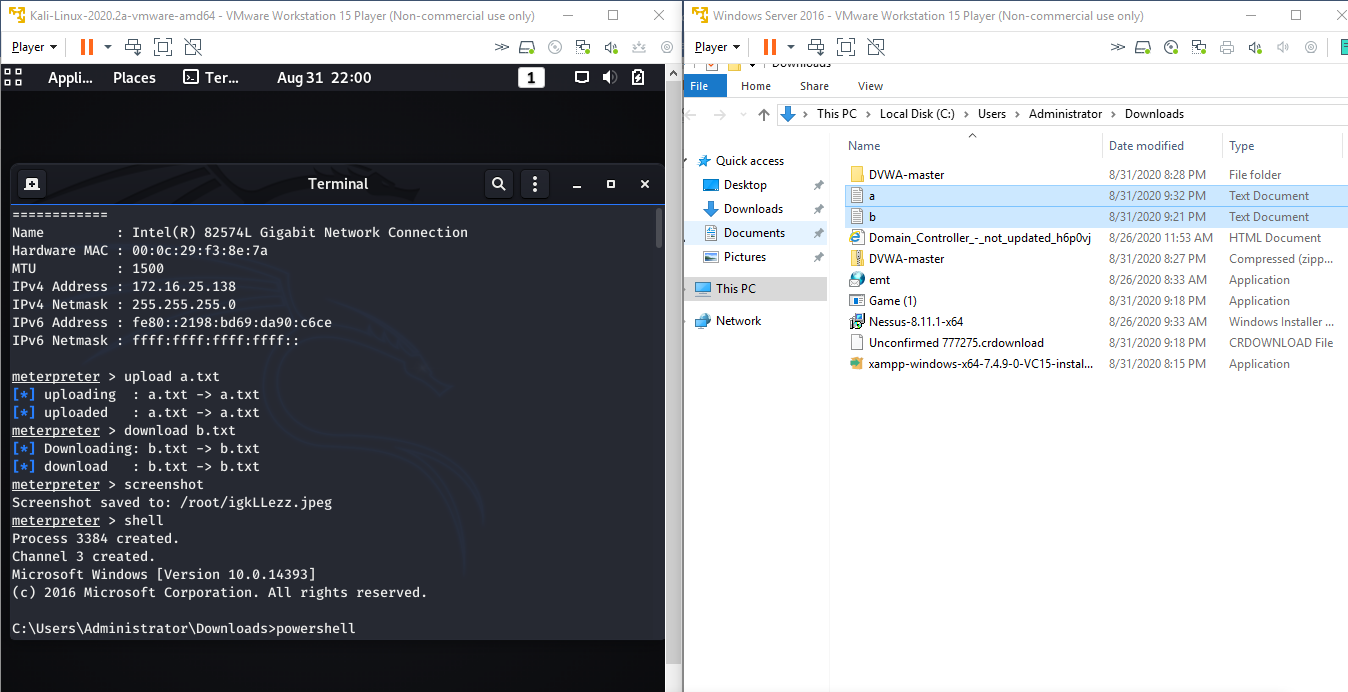




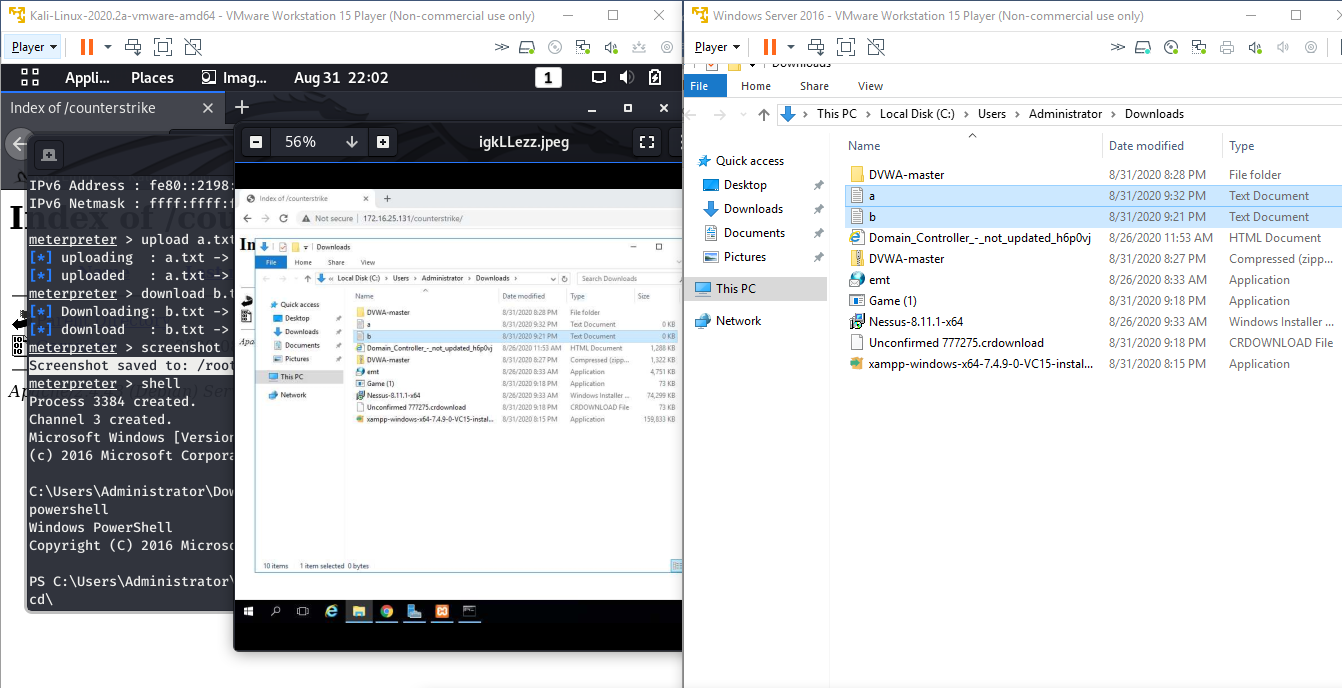
Exploitation Started of the Victim Machine (All details received from the Victim Machine)



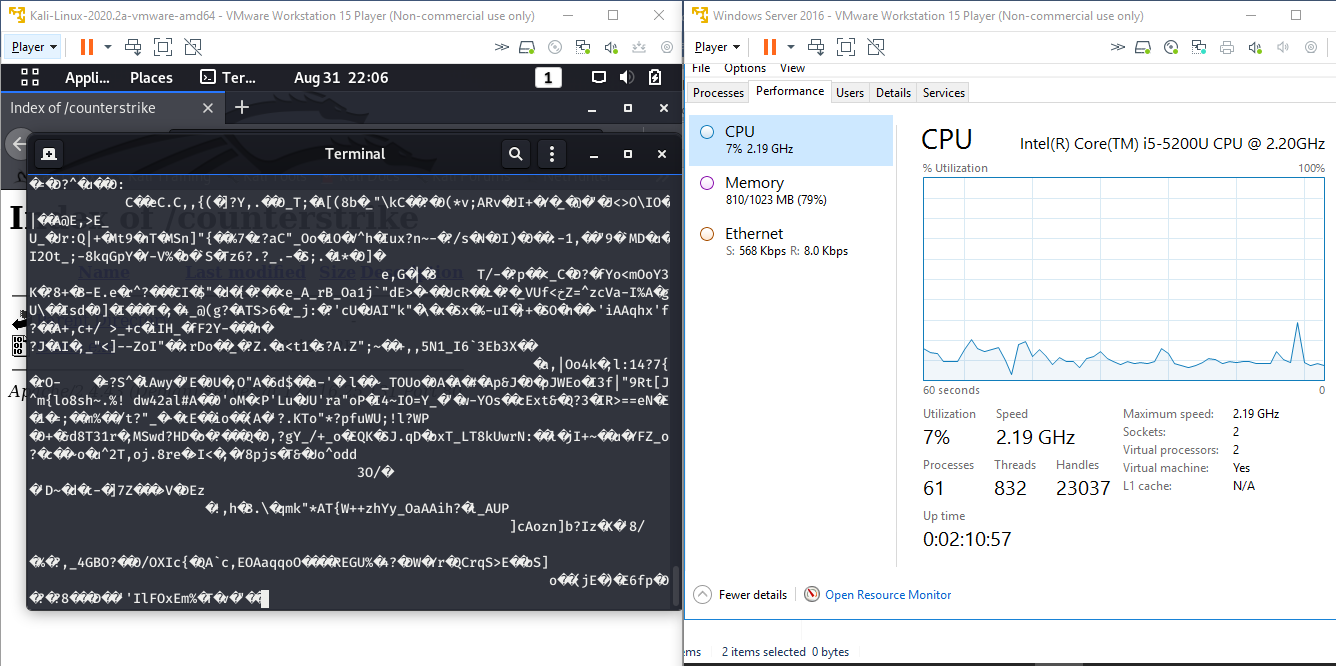
Upload and Download of the a.txt & b.txt in the Victim Machine successfully



Screenshot taken of the Victim Machine



Made the CPU memory a bit high by increasing the load from kali in the Victims Machine



**Question 2:**

1. ● Create an FTP server
2. ● Access FTP server from windows command prompt
3. ● Do an mitm and username and password of FTP transaction using wireshark and dsniff.

ANS

File Transfer Protocol

The File Transfer Protocol (**FTP**) is a standard network protocol used for the transfer of computer files between a client and **server** on a computer network. **FTP** is built on a client-**server** model architecture using separate control and data connections between the client and the **server**.

# **Man-in-the-middle attack**

In [cryptography](https://en.wikipedia.org/wiki/Cryptography) and [computer security](https://en.wikipedia.org/wiki/Computer_security), a **man-in-the-middle attack** (**MITM**) is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. One example of a MITM attack is active [eavesdropping](https://en.wikipedia.org/wiki/Eavesdropping), in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within the reception range of an unencrypted [Wi-Fi access point](https://en.wikipedia.org/wiki/Wireless_access_point) could insert themselves as a man-in-the-middle.[[1]](https://en.wikipedia.org/wiki/Man-in-the-middle_attack#cite_note-:0-1)[[2]](https://en.wikipedia.org/wiki/Man-in-the-middle_attack#cite_note-:1-2)[[3]](https://en.wikipedia.org/wiki/Man-in-the-middle_attack#cite_note-3)

As it aims to circumvent mutual authentication, a MITM attack can succeed only when the attacker impersonates each endpoint sufficiently well to satisfy their expectations. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, TLS can authenticate one or both parties using a mutually trusted [certificate authority](https://en.wikipedia.org/wiki/Certificate_authority)

# **dSniff**

**dsniff** is a set of password sniffing and network traffic analysis tools written by security researcher and startup founder Dug Song to parse different application protocols and extract relevant information. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data (passwords, e-mail, files, etc.). arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker (e.g., due to layer-2 switching). sshmitm and webmitm implement active [man-in-the-middle](https://en.wikipedia.org/wiki/Man-in-the-middle_attack) attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.

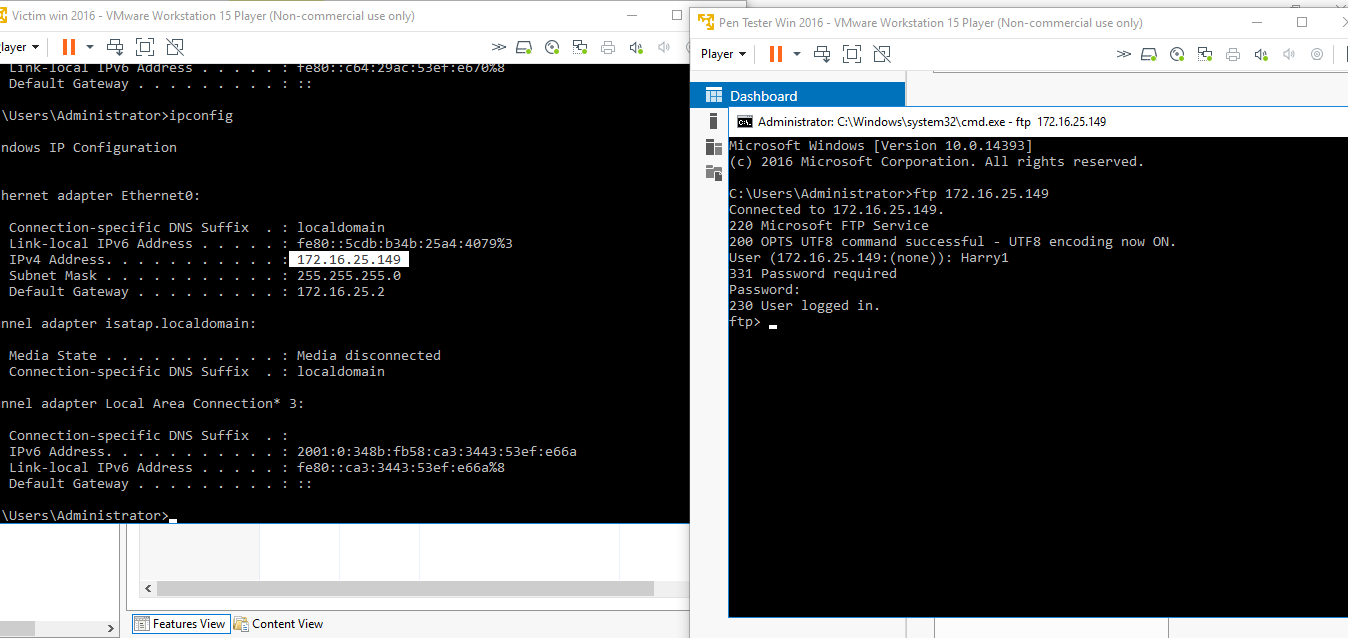
# **Wireshark**

**Wireshark** is a [free](https://en.wikipedia.org/wiki/Free_software) and [open-source](https://en.wikipedia.org/wiki/Open-source_software) [packet analyzer](https://en.wikipedia.org/wiki/Packet_analyzer). It is used for [network](https://en.wikipedia.org/wiki/Computer_network) troubleshooting, analysis, software and [communications protocol](https://en.wikipedia.org/wiki/Communications_protocol) development, and education. Originally named **Ethereal**, the project was renamed Wireshark in May 2006 due to trademark issues.[[4]](https://en.wikipedia.org/wiki/Wireshark#cite_note-4)

Wireshark is [cross-platform](https://en.wikipedia.org/wiki/Cross-platform), using the [Qt](https://en.wikipedia.org/wiki/Qt_(software)" \o "Qt (software)) [widget toolkit](https://en.wikipedia.org/wiki/Widget_toolkit) in current releases to implement its user interface, and using [pcap](https://en.wikipedia.org/wiki/Pcap" \o "Pcap) to capture packets; it runs on [Linux](https://en.wikipedia.org/wiki/Linux), [macOS](https://en.wikipedia.org/wiki/MacOS" \o "MacOS), [BSD](https://en.wikipedia.org/wiki/BSD), [Solaris](https://en.wikipedia.org/wiki/Solaris_(operating_system)), some other [Unix-like](https://en.wikipedia.org/wiki/Unix-like) operating systems, and [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows). There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are [free software](https://en.wikipedia.org/wiki/Free_software), released under the terms of the [GNU General Public License](https://en.wikipedia.org/wiki/GNU_General_Public_License).

**Steps: -**

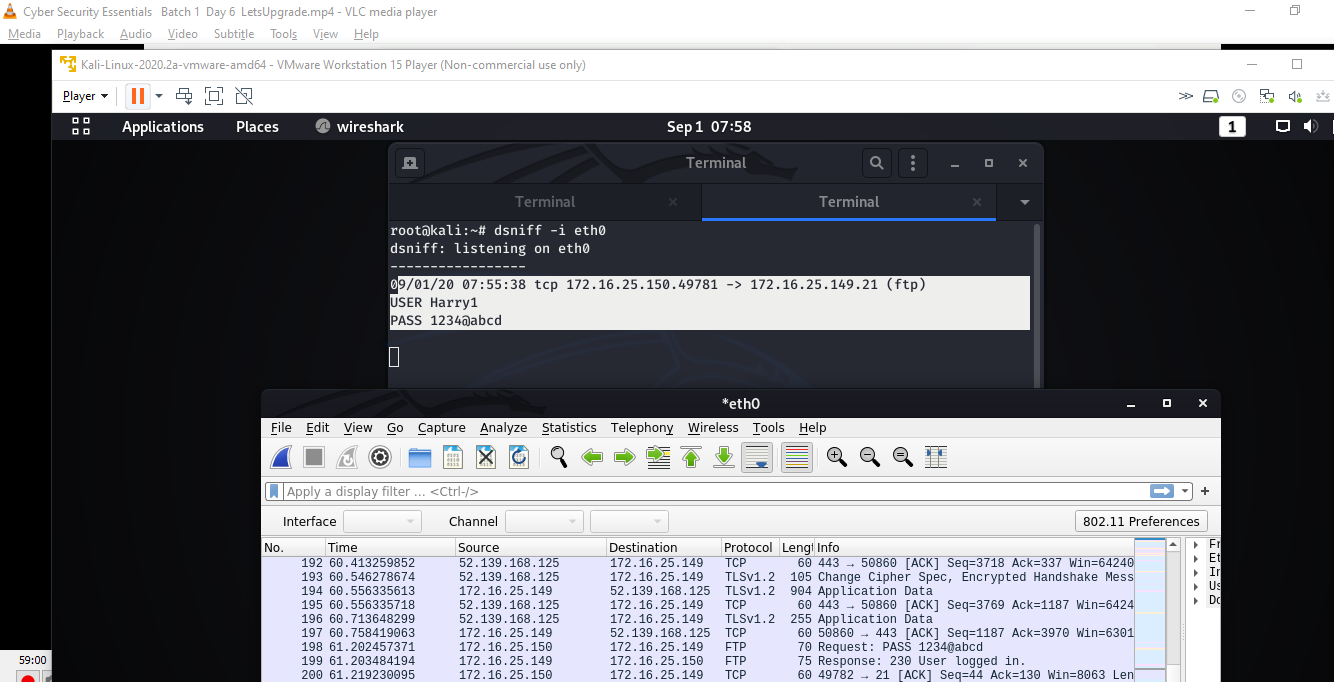
Created FTP in Victim and Able to log in in FTP from Pen Tester System



Using dsniff Username & Password of Ftp transaction is displayed below

Username of FTP: - Harry1

Password: - 1234@abcd



Using Wireshark Username & Password of Ftp transaction is displayed below

Username of FTP: - Harry1

Password: - 1234@abcd

