

# Conestoga College

Course	INF08965 - Network and Security
Activity Title	Internet Traffic Analysis
Student Name	Twinkle Akhilesh Mishra
Student Number	8894858
Lab performed on (Date):	27-Jan-2025

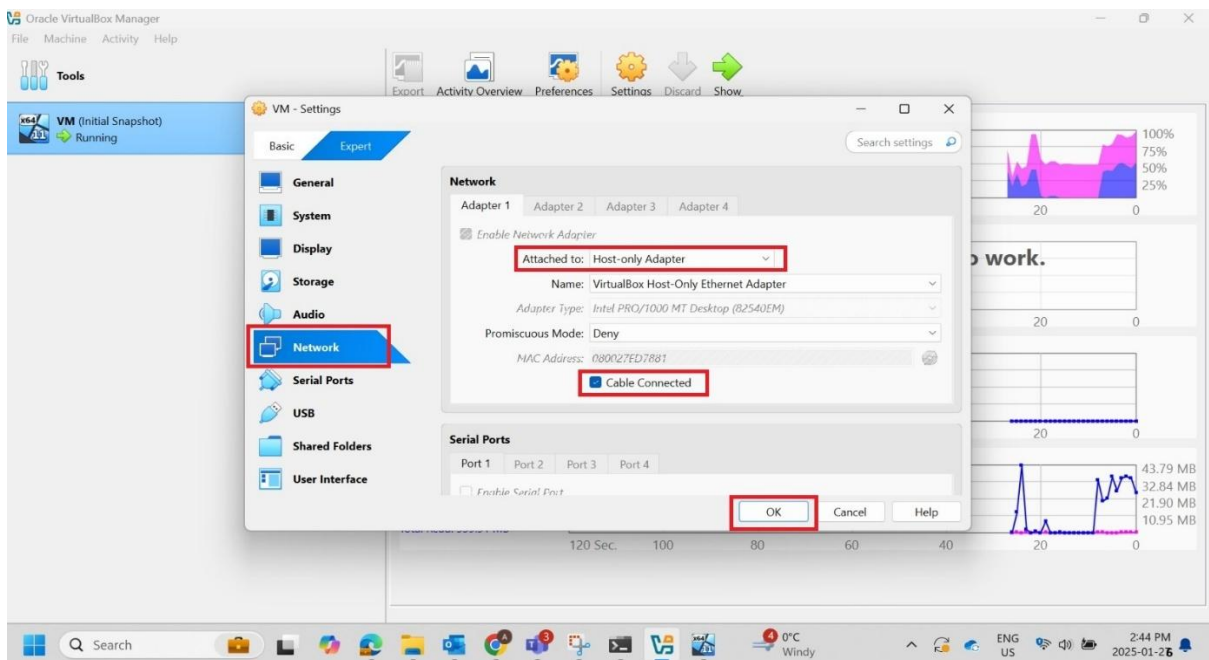
## Objectives

- Analyse network traffic using traffic capture utility like Wireshark.
- Setup an FTP server in a Virtual Machine
- For IP addressing in this lab, XY (58) represents the last two digits of your student ID.

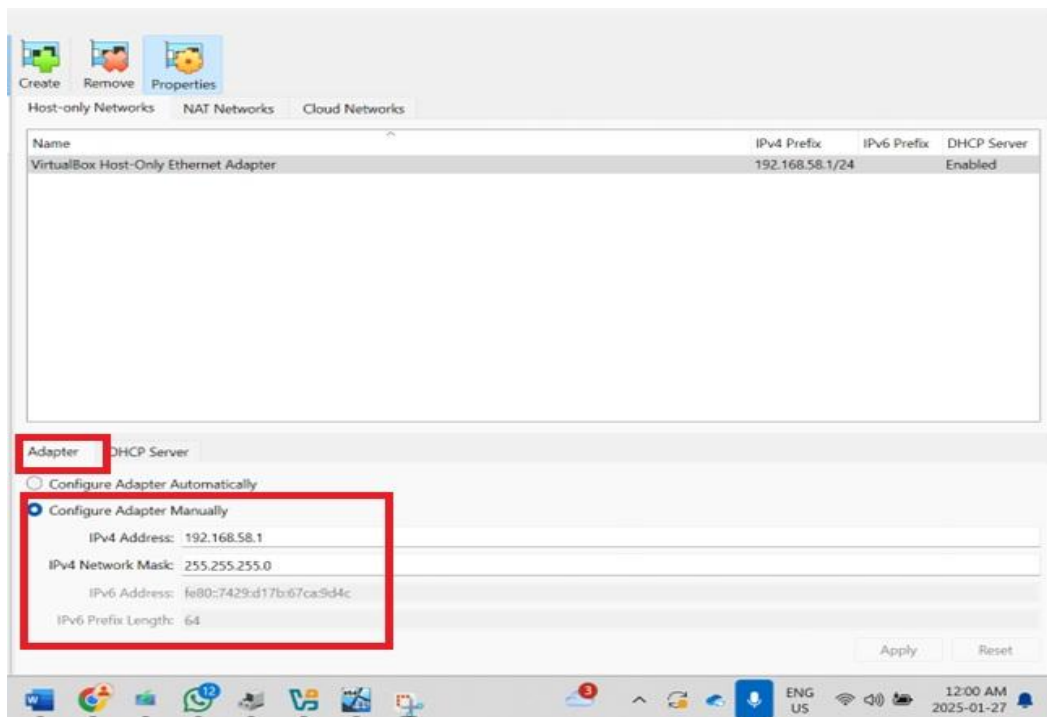
### Step 1: Install and Run FTP Server

#### 1. Configure Host-Only Adapter:

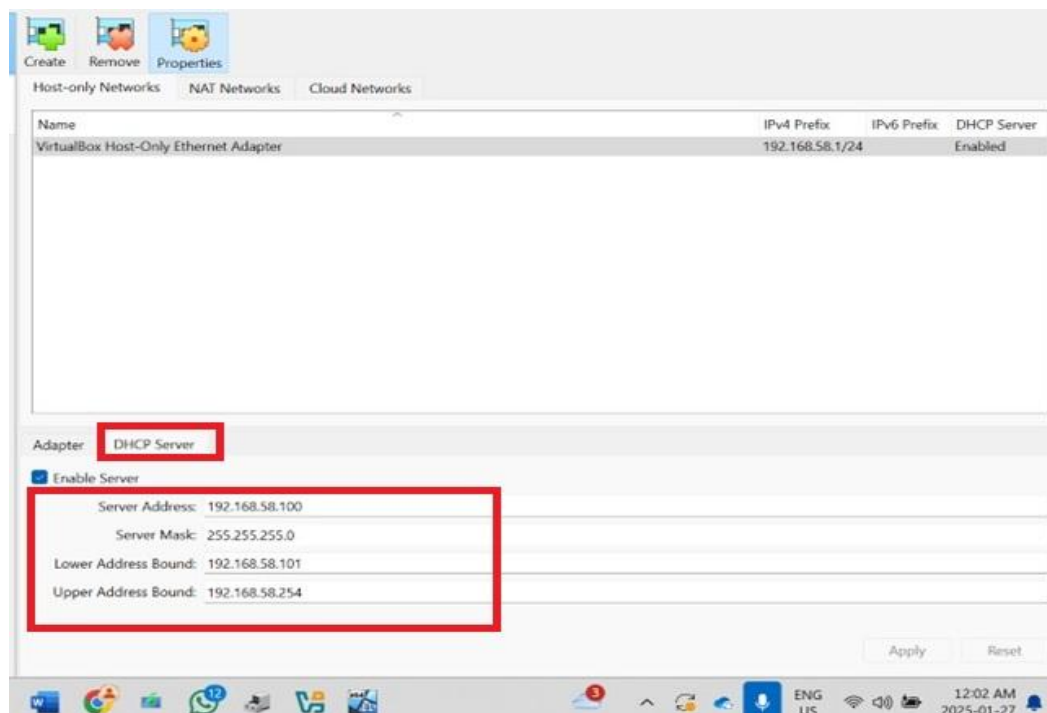
- Using VirtualBox, created a **Host-Only Ethernet Adapter**.
- Given the IP address **192.168.58.1** and the network mask **255.255.255.0**.
- Setup **DHCP** server with IP address **192.168.58.100**
- Lower/upper bounds: **192.168.58.101 - 192.168.58.254**



- **Change Adapter IP to .58:**

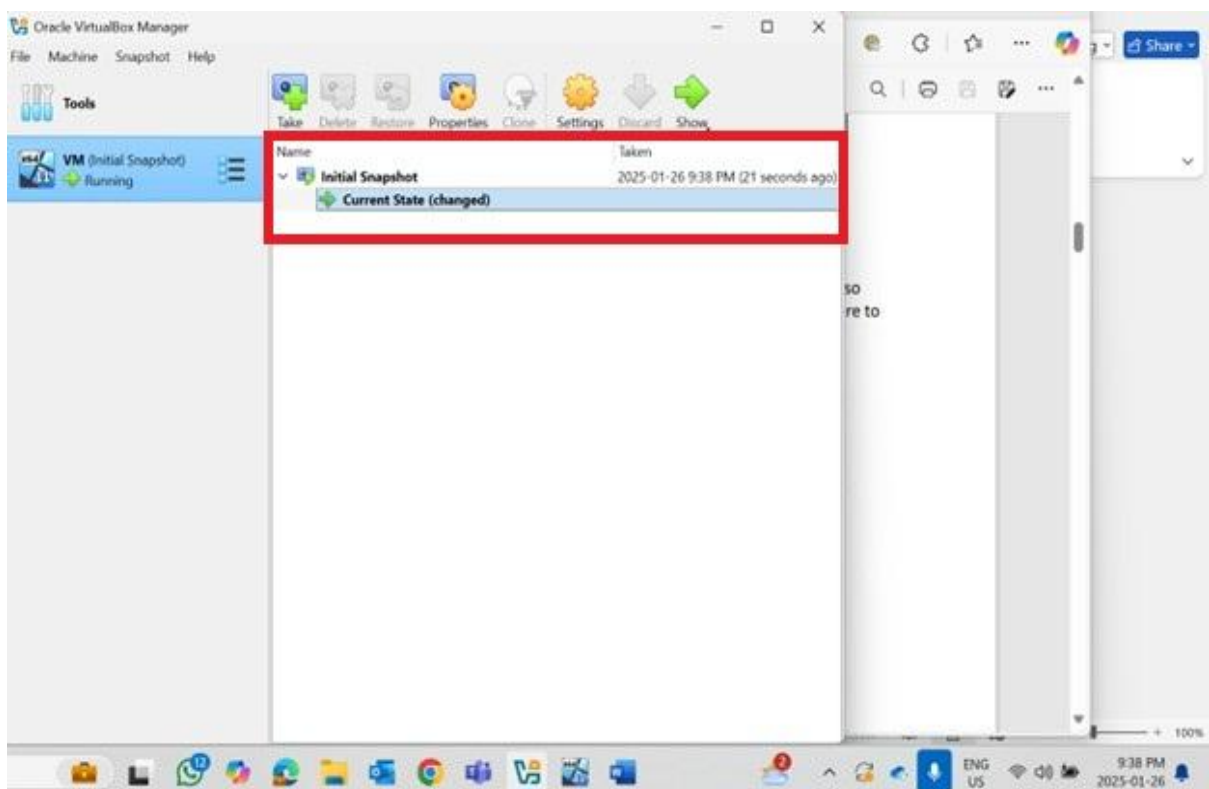
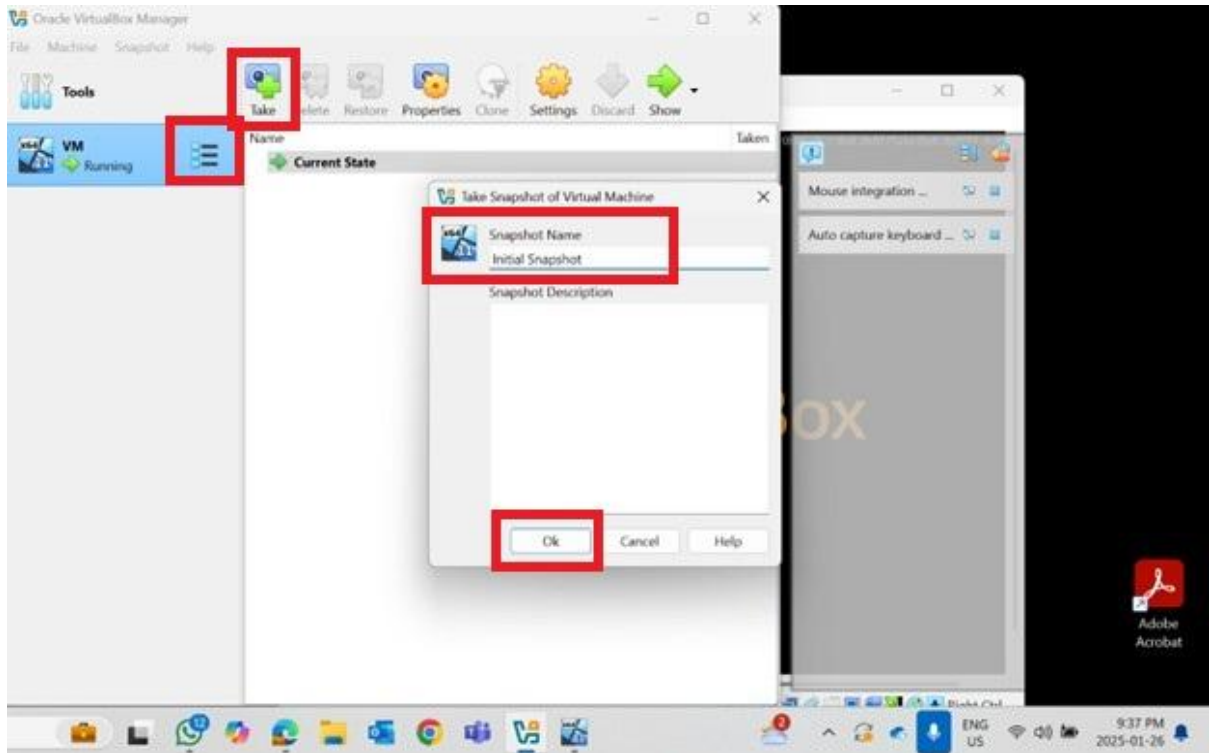


- **Change DHCP Server to .58**



## 2. Take a Snapshot:

- Created an initial snapshot of the Windows 10 VM for backup.

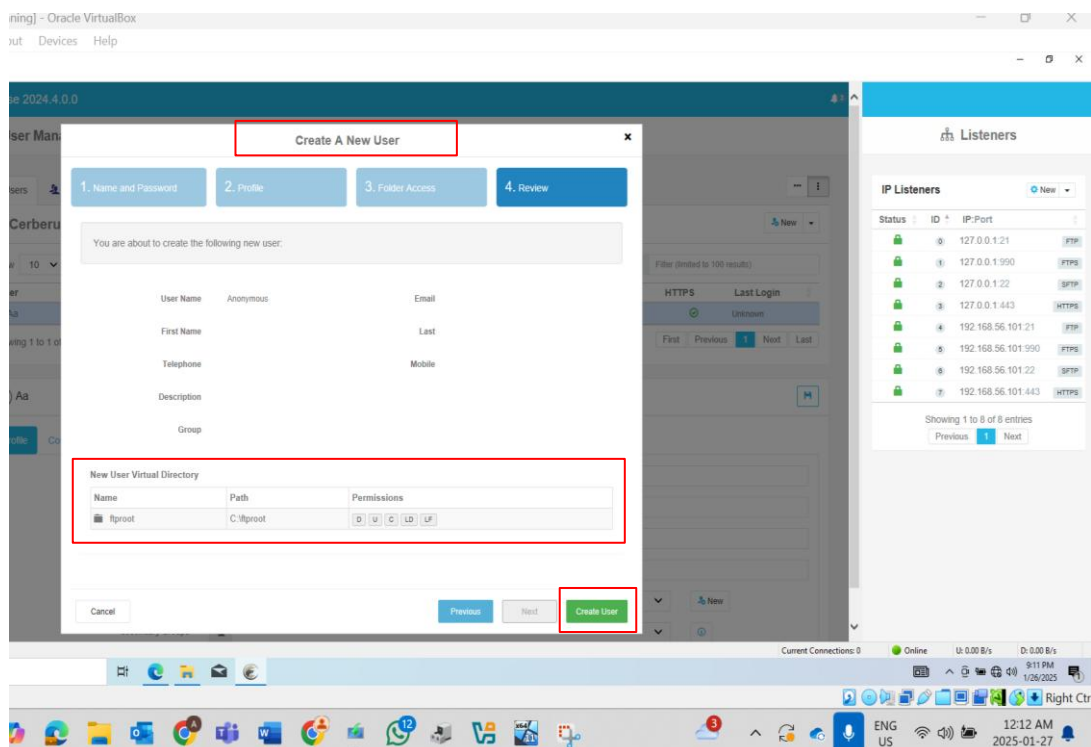
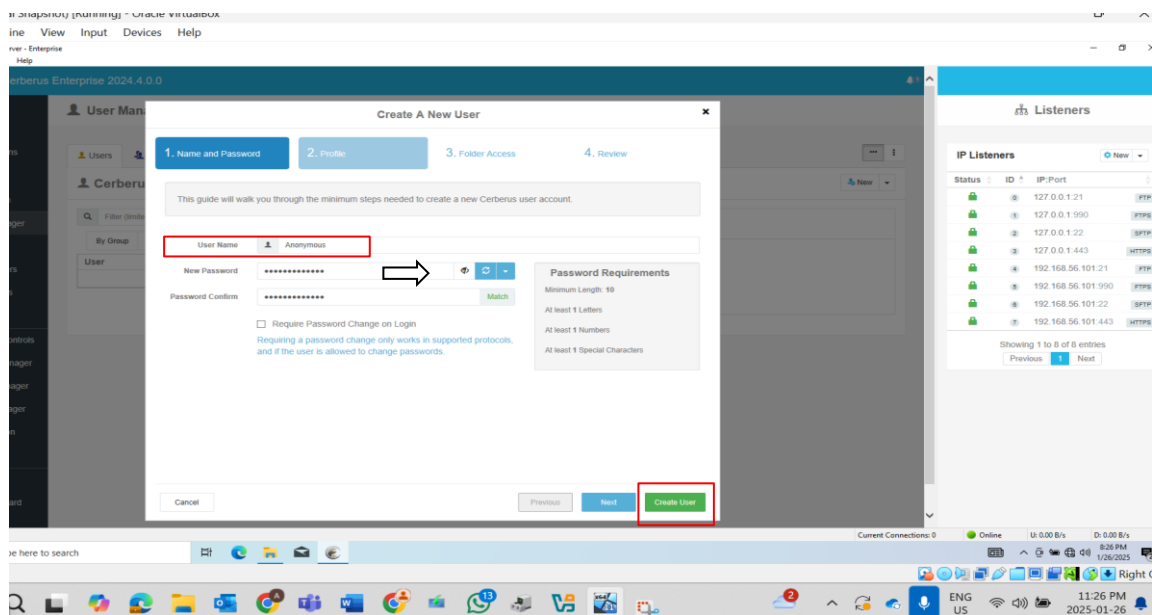


### 3. Install Cerberus FTP Server:

- Installed Cerberus on the VM with default settings.
- Allowed unencrypted FTP traffic and disabled SSL/TLS.
- Set up the Anonymous user with a password.
- Verified the FTP server IP address.

### 4. Create and Test File:

- Created a text file named after Cerberus in **C:\ftproot**.



- Checked the box for FTP to not allow unsecured FTP server connections

The screenshot shows the Cerberus Enterprise 2024.4.0.0 User Manager interface. The 'User Manager' tab is selected in the left sidebar. The 'Anonymous' user is selected in the user list. The 'Allowed Protocols' tab is active, showing the 'Permitted Login Protocols' section. The 'Allow FTP' checkbox is checked, and the 'Require Secure Control' checkbox is unchecked. The 'Update User' button is highlighted in the bottom right corner.

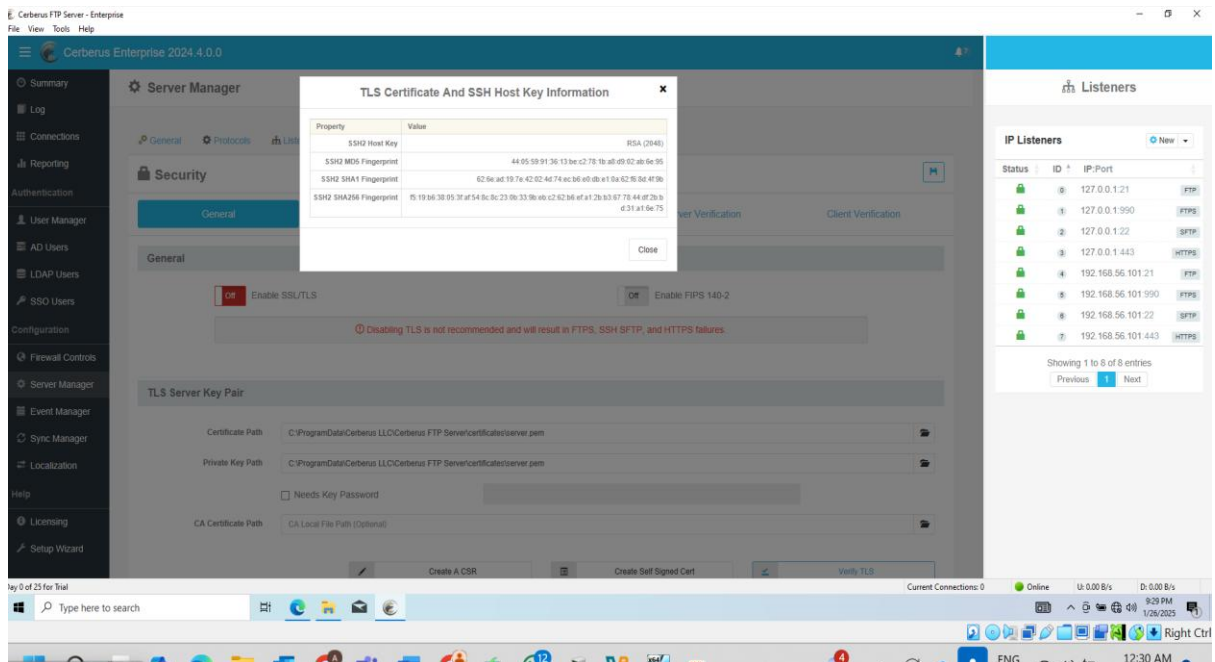
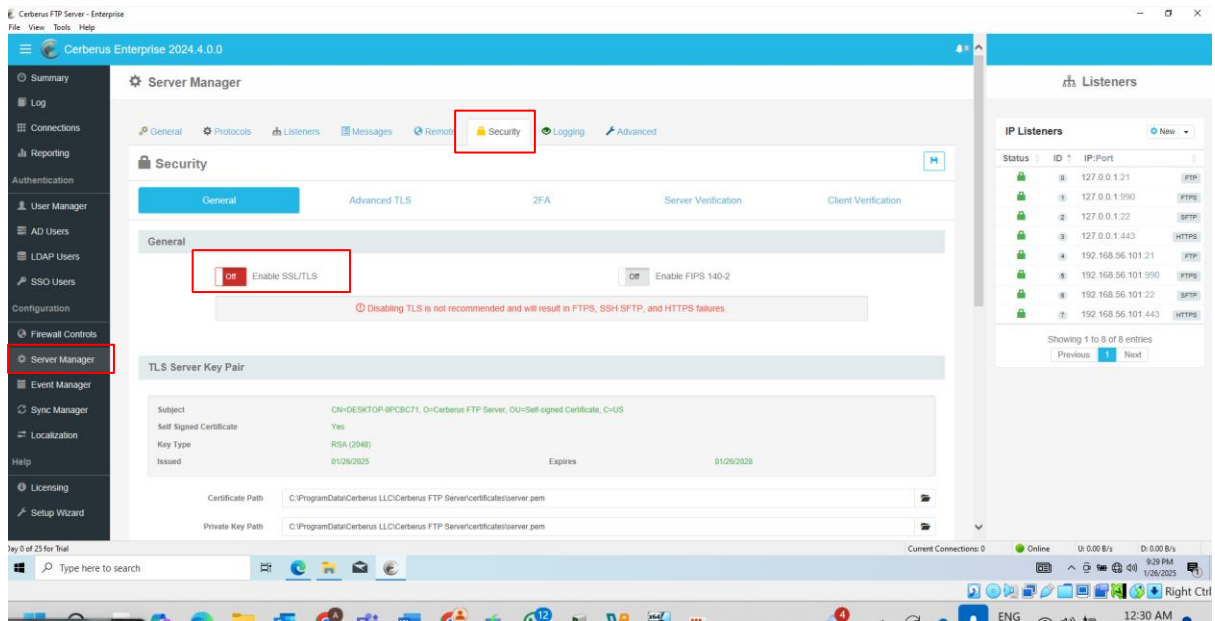
User	Full Name	Group	Logins	Email	FTP	FTPS	SFTP	HTTP	HTTPS	Last Login
Aa			No Limit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Unknown

- Disable secure control and data

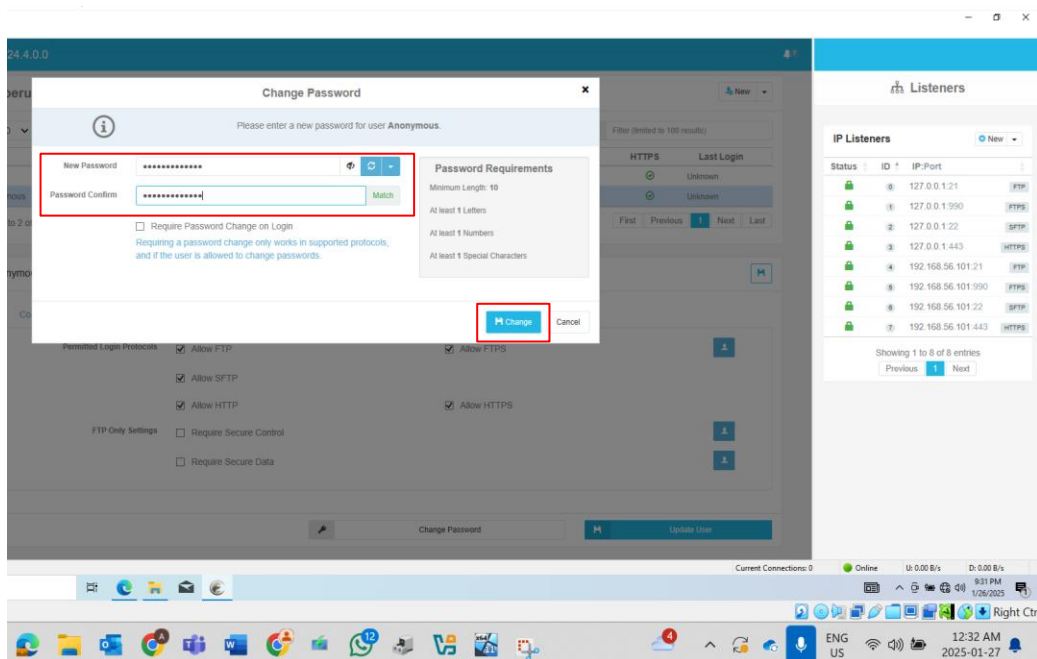
The screenshot shows the Cerberus Enterprise 2024.4.0.0 Server Manager interface. The 'Server Manager' tab is selected in the left sidebar. The 'New FTP Defaults' configuration window is open. The 'Allow Login' checkbox is checked, and the 'Require Secure Control' and 'Require Secure Data' checkboxes are unchecked. The 'Update User' button is highlighted in the bottom right corner.

Status	ID	IP:Port	Protocol
<input checked="" type="checkbox"/>	0	127.0.0.1:21	FTP
<input checked="" type="checkbox"/>	1	127.0.0.1:990	FTPS
<input checked="" type="checkbox"/>	2	127.0.0.1:22	SFTP
<input checked="" type="checkbox"/>	3	127.0.0.1:443	HTTPS
<input checked="" type="checkbox"/>	4	192.168.56.101:21	FTP
<input checked="" type="checkbox"/>	5	192.168.56.101:990	FTPS
<input checked="" type="checkbox"/>	6	192.168.56.101:22	SFTP
<input checked="" type="checkbox"/>	7	192.168.56.101:443	HTTPS

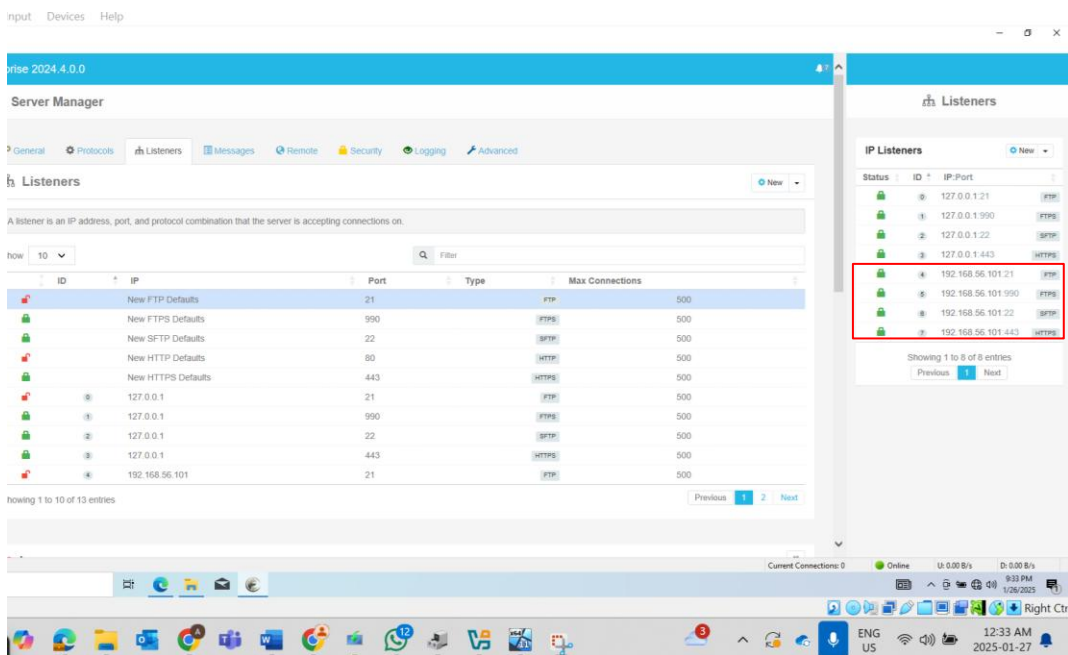
- Disable SSL/TLS



## Setting password for Anonymous user:



## IP address for Cerberus FTP Server:





## Step 2: Download File and Capture FTP Traffic

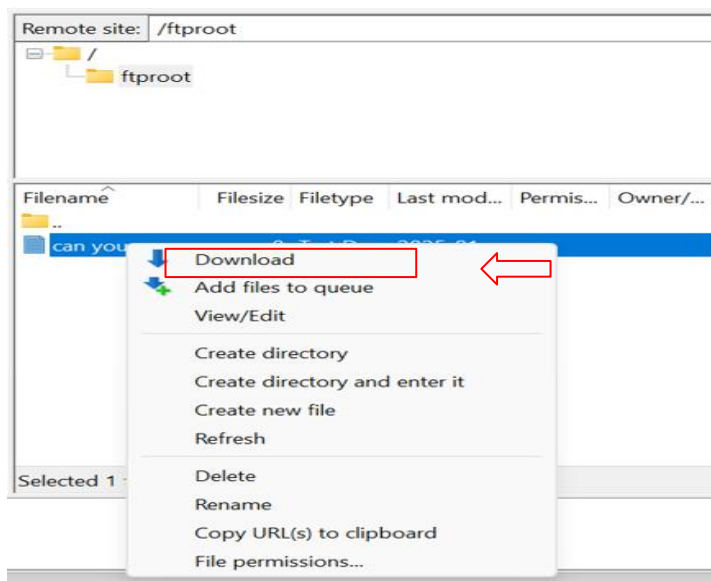
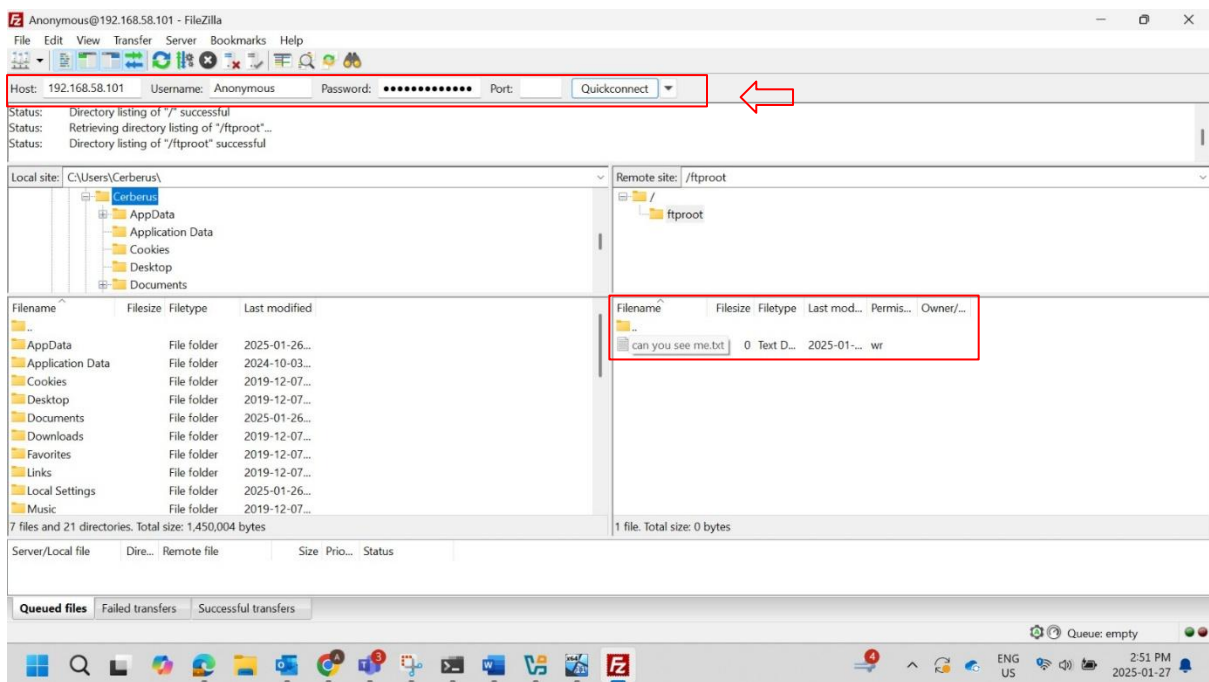
### 1. Install FileZilla Client:

- Installed FileZilla Client on the host machine.

### 2. Capture FTP Traffic with Wireshark:

- Started Wireshark on the host and captured traffic on the Host-Only Network.
- Used FileZilla to connect to the FTP server, login, and download the test file.
- Verified server logs in Cerberus.

### ■ Downloading file hosted on the FTP Server using FileZilla:

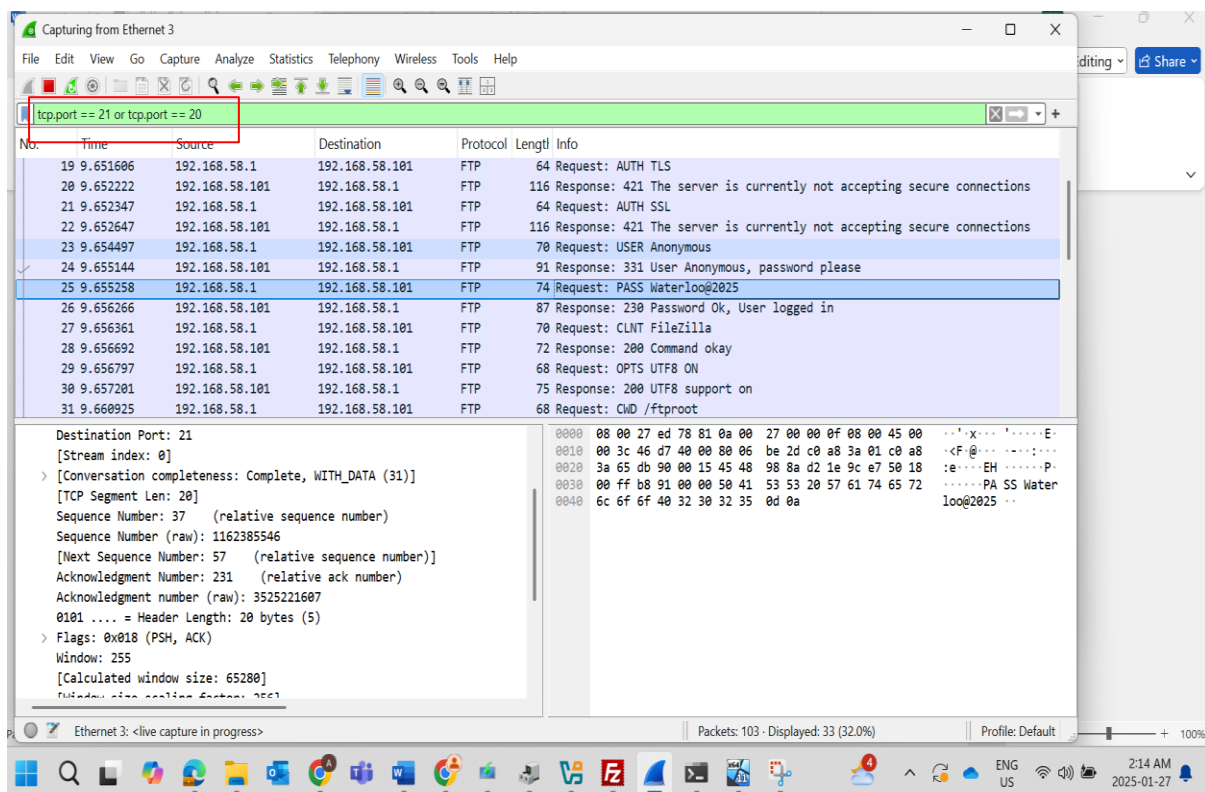




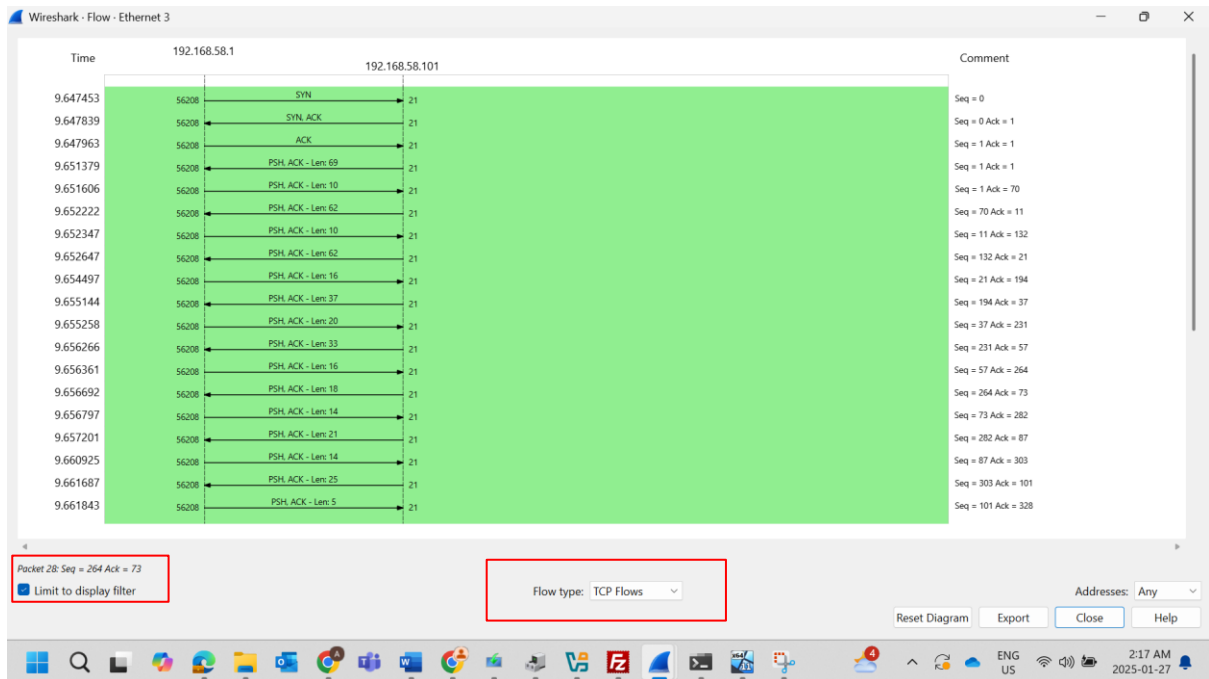
### 3. Analyze Wireshark Data:

- Applied tcp.port == 21 or tcp.port == 20 to display FTP traffic.
- Captured clear-text username and password during login.
- Verified successful 3-way handshakes (SYN, SYN-ACK, ACK).
- Observed file transfer in plain text in captured packets.
- Visualized communication and handshakes between client and server.

#### Output #1: Apply filter to view only FTP related traffic



## Output #2: Flow graph in Wireshark



## Output#3: Wireshark Capture of File Transfer in Clear Text

