Part B 1: To capture and analyze FTP login packets between a client and server using Wireshark and understand how credentials are transmitted over the network.

Description:

- ✓ FTP (File Transfer Protocol) is used for transferring files between client and server.
- ✓ FTP typically uses port 21 for control commands.
- ✓ FTP transmits username and password in plaintext, which can be easily captured.
- ✓ Wireshark is a packet-sniffing tool used to monitor network traffic and analyze protocol behavior.

Tools Required:

- ✓ Kali Linux (Client)
- ✓ Ubuntu Linux (FTP Server)
- ✓ Wireshark
- ✓ FTP client (command line)

Part A — Setup FTP Server on Ubuntu—In Ubuntu VM

1. **Start Ubuntu VM.**
2. **Install FTP server:**

   ```
   sudo apt-get install vsftpd.
   ```

3. **Start FTP service:**

   ```
   sudo systemctl start vsftpd.
   ```

4. **Enable service on boot:**

   ```
   sudo systemctl enable vsftpd.
   ```

   If the service is not running..

   ```
   Sudo ufw allow 21/tcp
   ```

5. **Create a test user:**

   `sudo adduser ftpuser` (password: 12345).

Part B — Capture Traffic Using Wireshark on Kali

7. Start Kali VM.

8. Launch Wireshark and select network interface (eth0).
9. Start capture.

Part C — FTP Client Login

11. Open terminal on Kali: ftp <ubuntu-ip> (example: ftp 192.168.56.105).
12. Enter username: ftpuser.
13. Enter password: 12345.
14. Optionally, execute a command like ls, pwd…
15. Exit FTP: bye.
16. Stop Wireshark capture.

Part D — Analyze Packets

17. Apply display filter: ftp.
18. Locate USER command packet → verify username.
19. Locate PASS command packet → verify password.
20. Check server responses:

- 331 User name okay, need password
- 230 Login successful

21.Observe the sequence of authentication packets.

Observations:

- Username and password appear in plaintext in Wireshark.
- FTP packets can be filtered using tcp.port==21 or ftp.
- Server response codes are 331 (password required) and 230 (login successful).
- The login sequence is clearly visible:
    1. USER → ftpuser
    2. Server → 331
    3. PASS → 12345
    4. Server → 230