**Network Security Lab 1**

**Traffic Investigation**

Lab Objective: Experience working with captured packet data, which is a crucial aspect of network security.

Lab Mission: Investigate a PCAP, answer the questions, and design a secure architecture based on the material you learned.

Environment and Tools: Wireshark

LAB TASK 1: Locate the Attacker

While investigating the data in Wireshark I noticed at Packet 148 a 220 FTP response code reading, “220 Service of UnBreakers.” A 220 FTP response code is sent in response to a new user connecting to the FTP server to indicate that the server is ready for a new client. Graphical user interface, text, application, email

Description automatically generated I then right clicked on packet 148 and navigated to the ***follow*** tab. While in the ***follow*** tab I clicked on ‘TCP stream.’ The following information was displayed:

A picture containing text, screenshot, computer, computer

Description automatically generated

In the above listed information, it is shown that USER ‘janed’ was utilized to try and access the system. Several password attempts were tried and were unsuccessful. At packet 421 login in time was exceeded and the control connection was closed.

1. Which protocol was used in the attack? FTP (File Transfer Protocol)
2. What is the number of the packet at which the attack began? Packet 148
3. Which user was under attack? User ID: janed
4. What is the number of the packet that supports your answer? Packet 202 shows that USER “janed” was being used to try and gain access.

202 UTF8 mode is always enabled. No need to send this command.

USER janed

1. What was the attacker’s source IP? The attackers source IP is ***212.179.252.98***. Packet 153 shows the attacker’s IP address as the source.
2. Did the attack succeed? No, if you look at packet 421 login time was exceeded, and the control connection was closed.

421 Login time exceeded. Closing control connection.