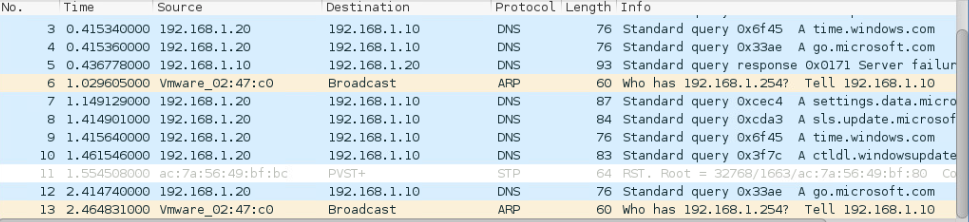
Lab 06: Capturing and Analyzing Network Traffic Using a Sniffer

Lab report template Name: Kevin Ubilla

This Lab is required for Unit 4. It is worth 15 points. The Challenge exercise is worth 2.5 Extra Credit points.

1. **Starting the Sniffer, Step 14:** Please display a portion (no more than a single screen capture) of the packets that first appeared on your packet list when Wireshark was started. Capture it and paste it here:

**→  ←**

1. **Generating the Traffic, Step 14:** Now that you have moved **2008.jpg** to local disk C:, capture an image of the contents of Local Disk (C:), showing the presence of **2008.jpg**. (Please crop the image small enough to allow you to expand it on the page for the text to be readable.)

**→ A screenshot of a computer

Description automatically generated ←**

1. **Generating the Traffic, Step 20:** Please explain, in your own words, why you think that the system asked you about sending your password to a remote computer.

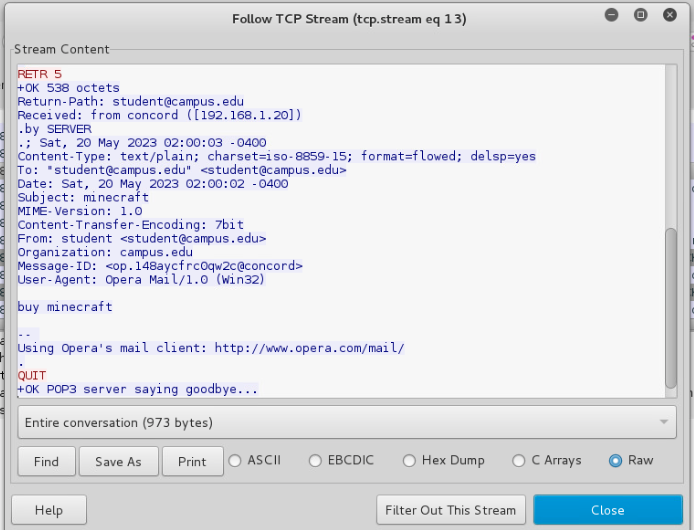
**→ I think its because password sent to a remote server can always be intercepted.←**

1. **Analyzing the Traffic, Step 2:** Now that you are examining the packets that you captured, please capture the result of your search for the packet that contains the user password for "zombie" and paste it here, showing the search filter, the packet number, time, source, destination, protocol, length and information.

**→ A screenshot of a computer

Description automatically generated with medium confidence←**

1. **Analyzing the Traffic, Step 6:** Capture the screen that displays the assembled email about "buying Minecraft" that you obtained by following the TCP stream in the packets you captured and paste it here:

**→ ←**

1. **Analyzing the Traffic, Step 10:** Please find the place in the TCP stream where the Creeper account is created and added to the ‘admins’ domain, capture it (with surrounding text) as an image and paste it here:

**→A screenshot of a computer

Description automatically generated with medium confidence ←**

1. **Analyzing the Traffic, the whole section:** Please explain what I meant when I asked for you to find the place “in the TCP stream”. What is a TCP stream?

**→ A TCP (Transmission Control Protocol) stream is plaintext protocol packets. TCP packets were sent and I was able to intercept them, convert them into human readable format to understand what the user on the target computer is doing. ←**

**If you encountered any issues, either positive or negative, with this Lab, please let me know by commenting here. (This IS an experiment, after all.) I am tuning this according to what you say.**

**→ ←**