

**Lab 5: Sniffing Networks (5%)**

**Overview:**

The goal of this lab is to show you how easy it is to look at traffic on a network. In particular we will be looking at SSH and TLS traffic.

**Objective:**

1. Demonstrate how to sniff secured SSH connections
2. Demonstrate how to sniff secured TLS connections

**Resources**

For this lab you’ll be using the applications *Wireshark* and *PuTTy*.

*Unfortunately, there is an issue with the installed version of Wireshark. Find the Win64 version 2.0.0 of Wireshark and install that.*

Note: If you do not know how to use the tools, please look at the manual.

**The Lab Activities**

**Part 1: Capturing a secure SSH connection**

Here we will be logging into Matrix using *PuTTy* (PuTTy if you are using windows and terminal if you are using Linux or MacOS) and capturing the traffic. The descriptions are for Windows, as the instructions for Linux and MacOS are almost similar.

**Steps**

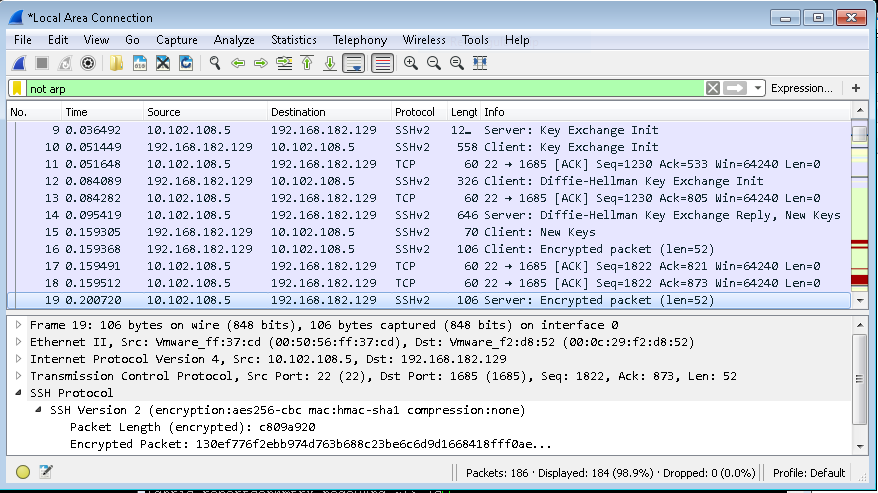
1. Open *PuTTy* and enter Host Name for Matrix
2. Begin another screen capture in **Wireshark**. You may want to set the **Capture Filters** to ‘*not ARP and no DNS’ to reduce the amount of data generated.*
3. Click the ‘**Start’** button.
4. Click the ‘**Open’** button on Putty Configuration. You will notice a Security Alert window. Click’ **Yes’** to add the server’s public key to the registry.
5. Login to **Matrix** using your real username and password.
6. Type the **ls** command.
7. Click ‘**Stop’** capture.
8. Scroll to the beginning of the capture window and review the communication between the client and server.

* Notice that SSHv2 uses the Diffie-Hellman protocol to exchange keys.
* Notice that a session key and handshake are agreed to by the client and server before the exchange of data.
* Notice that each packet is encrypted within an encrypted tunnel which protects the login information from replay attacks.

1. Take two screen shots:

* A screen shot similar to the one given below (Figure 1). Name the file **<<MySenecaUsername>>\_SSH.jpg**.
* A screen shot that has both the Wireshark capture (as above) and the Matrix/PuTTy window open (i.e. with you logged in) beside it. Name the file **<<MySenecaUsername>>\_SSHandPutty.jpg**

1. Insert a heading titled “SSH Connection” into the lab report and insert your two (2) captured screenshot below it.



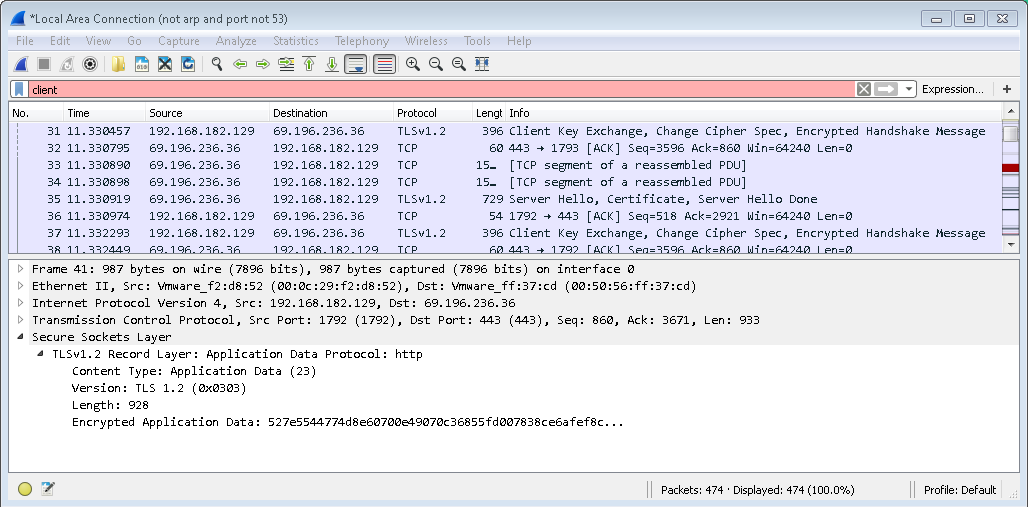
**Figure 1: SSH Connection**

**Part 2: Capturing a TLS Transmission**

Here we will be doing a capture of secure web traffic that use the TLS protocol.

**Steps**

1. Bring up the My Seneca website
2. Open **Wireshark** and begin a packet capture session.
3. Login using your real user name and password
4. **Stop** the capture and examine the captured packets.
   * Look at the packets that appear below "**Client Hello**" and "**Server Hello**".
   * Find a packet labeled "**TLSv1.2 Application Data**" and click on it in the top pane to select it. Details about the packet will appear in the middle pane. Click the **+** sign to expand **Secure Socket Layer**. Expand the layer inside (labeled " **TLSv1.2 Record Layer**" so that the **Encrypted Application Data** is visible. Your user name and password are concealed in that encrypted data. Even though the packet sniffer can see the data go by, it cannot be read. This is how TLS protects you. Notice that the process that the SSH and TLS screen shots look very similar in structure and format.
5. In Wireshark make sure the lines such as “Client Key Exchange…” are visible and the Encrypted Application Data is visible as well (see Figure 2 below) and take a screen shot and save the file as **<<MySenecaUsername>>\_TLS.jpeg**
6. Insert a heading titled “TLS Connection” into the lab report and insert you just taken screenshot beneath it.



**Figure 2: Client Key Exchange and Encrypted Application Data**

**Lab Report Write-up**

No template will be provided for this lab, so create your own template based on Lab’s 1 and 2. Ensure it includes Student Name and Student Number.

Submit your lab results using the template provided with the lab. Save the report as <<MySenecaUsername>> \_L5.docx

**Deliverable**

To submit your lab report to Blackboard under the appropriate week.

Note:

* Labs submitted late will be assigned a grade of ‘F’.
* Late labs still need to be satisfactorily completed and submitted by Study Week..