ITIS 6200/8200 Principles of Information Security and Privacy

Project 3: Packet Eavesdropping and Analysis

Objective

The objective of the project is to provide a hands-on experience to students so that they have a better understanding of the information transmitted in the Internet. At the same time, we want to show how powerful the packet eavesdropping and analysis tools are. Through the usage of the wiretapping tool such as WireShark, students can learn about the network packets and how information is encapsulated. In real life, many network administrators and security engineers depend on such tools to capture suspicious activities and then analyze them.

Tasks

1. Locate and install a wiretapping software tool such as WireShark. It can eavesdrop on both wired and wireless networks. Make sure that you are downloading from the reliable source such as *www.wireshark.org*. Do not use third party websites since attackers may embed malware in it.
2. Locate a software tool that will allow you to initiate both telnet and ssh sessions; (one of such tools is PuTTY); Please notice that PuTTY is an executable file and you can directly run it (under Windows environment). CCI's Windows 10 machine's "Software Center" has the tool. For MacOS user with OS version lower than mojave, you can start telnet and ssh connection from terminal utility, you do not need any additional tools. For MacOS mojave and high sierra user, you have to install telnet by using command 'brew install telnet' to use telnet from terminal utility.
3. Make sure that your computer is NOT connected to the UNCC campus network (including on the UNCC VPN). Your home network should be good enough.
4. Start your wiretapping tool, then start to telnet to the server: **telehack.com** (use port 23). On Windows, see the figure below on how to connect to the telnet server using PuTTY. On MacOS or Linux, type the command line 'telnet telehack.com 23' in a terminal window. When you see the welcome message from the server, type command 'login' and provide your username as 'uncc2020'. When it asks you for the password, guess a password, type it, and remember it. Most likely, the site will show "Password not correct" and ask you for the password again. That's normal. Just press 'Ctrl + C' and then type 'quit'. Please DO NOT guess the password more than once because your machine may be blocked by the site!

- Now stop the packet capture operation. You will see a group of packets captured by WireShark (around 100 packets). Frequently, you will see many packets and you will need to use the Filter functionality in WireShark to view only the ones you need. On the top of the tool you will see the "expression" window where you can input your filter. See the figure in the end of this document for some examples.
- Now go through the packets one by one, the packet contents will appear at the bottom of the tool. Pay close attention to the packets that are labeled as "TELNET" or "TCP". Try to figure out the IP address of **telehack.com** and use it as a filter. Some of the packets will contain the page materials in clear-text. Do you see the packets that contain the user name/password that you type? It is very possible that each TELNET packet contains only one character of your input. Now take a series of screenshots to show the traffic between your machine and the server. If you are using PuTTY, the figure below shows where to fill in the domain name and where to choose the protocol. The provided figure uses "eisner.decus.org" as hostname, however, you have to use **telehack.com** as hostname for this project.

5. Start you wiretapping tool again, then use ssh to login to **sdf.org**. Interact with the window following displayed instructions on the screen. Use the user name "new".
6. Now stop the packet capture operation. Can you see the username, password, or contents in plaintext in the captured packets?

Submission Instructions

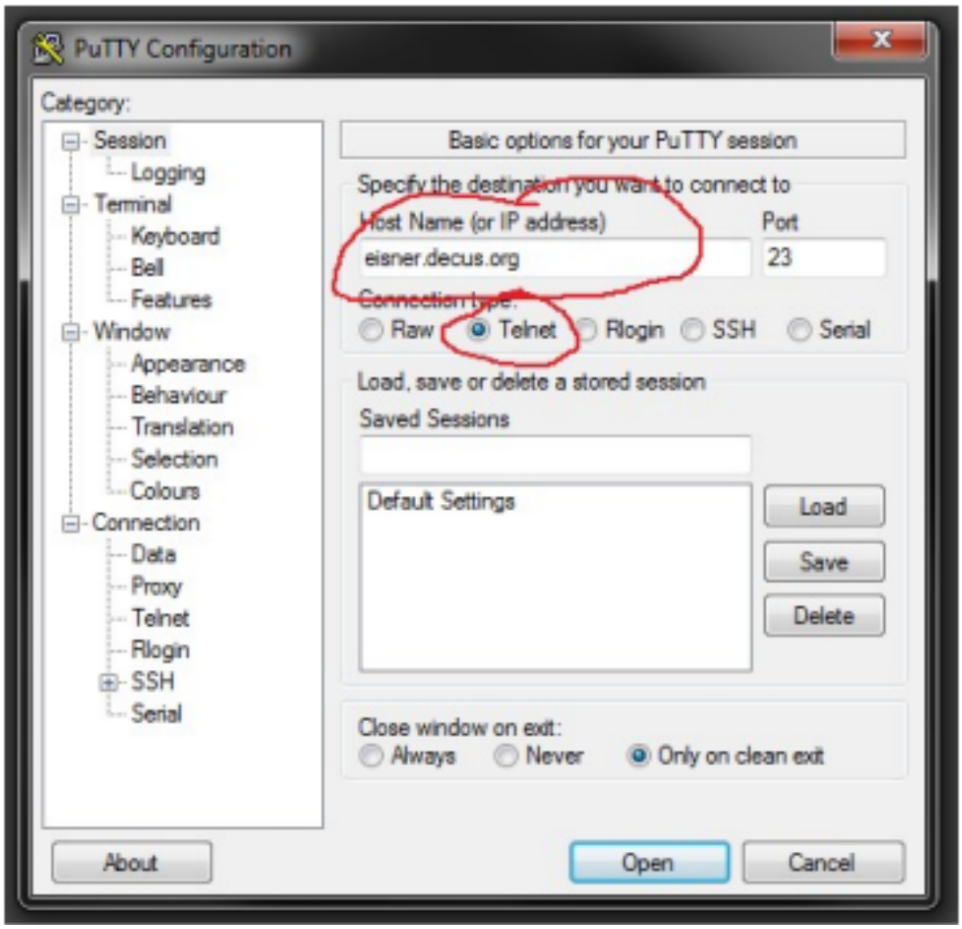
The packet capture tool could dump out the contents of the packets in steps (3), (4), and (5) as files. Store these captures as separate files for your subsequent analysis. You need to turn in the following:

A. What are the IP addresses of **telehack.com** and **sdf.org**?
B. Screenshots of the packet dump for the TELNET operation and the SSH operation. Please choose the packets with relatively large size (i.e., greater than 300 bytes) so that we can see the data contents.
C. Please answer, which protocol does PuTTY use to establish encryption key with the SSH server (i.e., which key exchange algorithm is used)? It is okay to consult external sources such as textbooks, online videos, or the web to find the answer to this question.
D. Shortly analyze the packet dump and explain why SSH is more secure than TELNET.
E. Now open the packet capture for the TELNET operations again. You will notice that there are many other types of packets such as DNS, TCP, etc. Please answer: (1) List all different IP addresses that you see in these captured packets; (2) List all the MAC addresses that you see in these captured packets; (3) List all TCP connections between the IP addresses that you

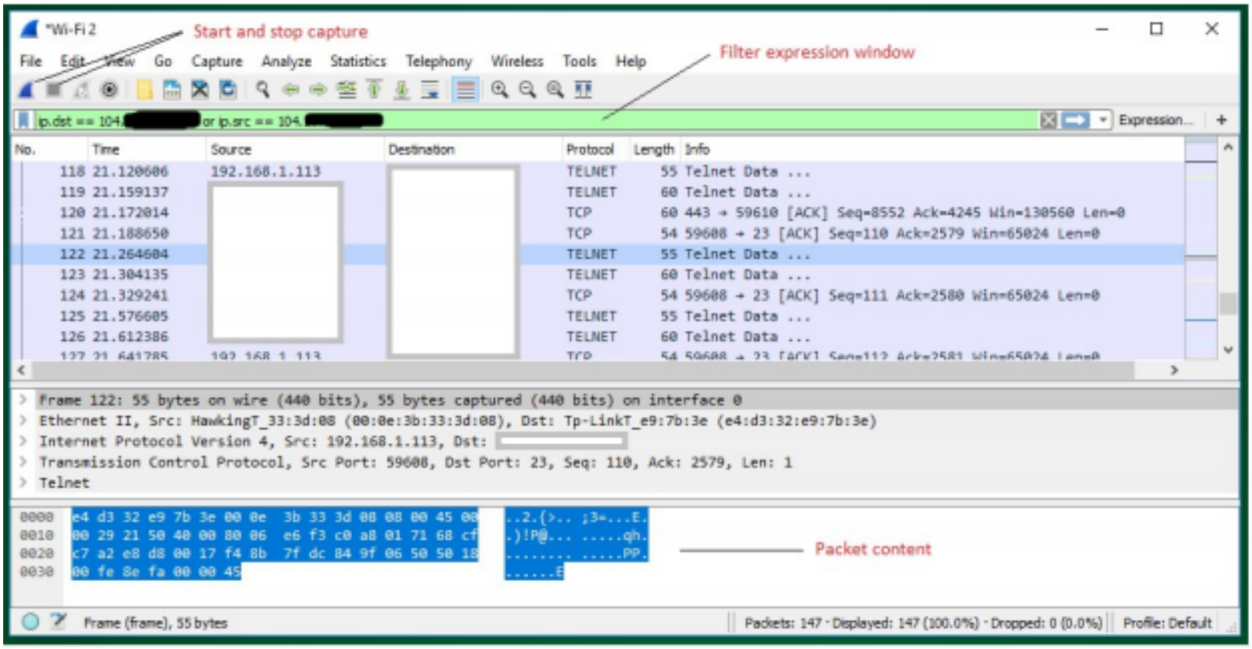
capture. Please note that for a TCP connection, you need to provide (Source IP, Source PORT, Destination IP, Destination PORT).

To accomplish these tasks, you need to use the analysis tools in WireShark. In the top tool bar, locate the entry called “Statistics”. Everything you need should be there. I will recommend you to look at the entries such as “Protocol Hierarchy”, “EndPoints”, and “Conversations”.

Tip: WireShark can run on Windows and Linux machines. I believe there are wiretap tools for Mac as well. In Windows, when you start Wireshark and if you see “no interface can be found”, close the application, right click “WireShark”, choose “Run as administrator” and you should be fine.



How to use PuTTY to telnet



Screenshot from WireShark