



Lab 2 - Sniffing all the Trons

CSEC 2324 - Network Security
Lab Guide v1.0

William Cox, M.S.
Visiting Assistant Professor
wcox@ualr.edu or wcox@uaptc.edu

January 2023




Contents

Lab Guide Instructions	4
Lab File Formatting	4
Markdown How-To	5
Suggested Setup	5
Lab Assignment 2 - Sniffing all the Trons	5
Overview	5
Lab Artifacts	6
Lab Software	6
Part 1: Using TCPDump	6
Part 2: Filtering with TCPDump	6
Part 3 - Wireshark	7
Part 4 - Wireshark Exercises	8

Lab Guide Instructions

The labs included in this guide will help you understand the principles of Network Security.

When you see a  you will be required to take a screenshot of that step.

Included is the requirement for a Lab Report file.

Follow the formatting instructions for full credit.

Note: Using Markdown is only required for the first lab.

Lab File Formatting

When completing your labs please follow these instructions.

1. All Labs created using Markdown & will use the Eisvogel template. Labs files created in another word processing program will use Times New Roman, 12 Font, Double Space.
Get Eisvogel here: <https://github.com/Wandmalfarbe/pandoc-latex-template>
2. Create a title page with the following details:
 1. Title of the Lab
 2. Class Name
 3. Your name
 4. Date
3. Section 2 will have all screenshots and questions/answers for the lab.
 1. Each question must be listed with its question number.
 2. Answers will be indented on the next line and start with an "a."
 3. If answer includes a picture, make sure picture is big enough for your instructor to interpret, but not too big to distract from the quality of your work.
4. Section 3 will be labeled Reflection.
 1. This is where you add any reflections needed.
 2. Make sure to quote your sources with parenthetical citations.
 3. Do not use quotes, but instead rewrite the quote in your own words. *Remember to still give credit to the author.*
5. Section 4 will be References
 1. All references should be in alphabetical order
 2. Use either APA or IEEE formatting

Markdown How-To

Below you will find a quick reference on how to use Markdown. This is not all inclusive and you may need to research steps that are particular to your situation. IE. Operating System, IDE, etc...

Suggested Setup

(You don't need to follow if you know Markdown)

1. Download and install following programs:
 1. VSCode Download
 2. Pandoc Install Instructions **Note: make sure to install all of the required dependencies**
 3. Eisvogel Template Download
2. Once you have downloaded and installed the required applications, you will need to set up your template and environments.
 1. VSCode Setup - Install following extensions:
 1. Markdown All in One, Author: Yu Zhang
 2. Dictionary Completion, Author: Yu Zhang
 3. markdownlint, Author: David Anson
 2. Setup Pandoc template Eisvogel Install Instructions
3. Basic Markdown syntax can be found at Markdown Guide
4. Convert Markdown to PDF syntax
 1. Open terminal and navigate to your markdown location
 2. Execute the following command replacing the file names with your information.

```
1 pandoc filename.md -o filename.pdf --from markdown --template  
   eisvogel --listings
```

Lab Assignment 2 - Sniffing all the Trons

Overview

This lab will introduce you to using protocol analyzers.

Lab Artifacts

Build a Lab report file with the requested answers or screenshots presented in this lab. Follow the Lab file format found in the beginning of the Lab Guide Manual.

Lab Software

Programs tcpdump, Wireshark




Operating System: Linux

Terminal Emulator: bash, shell, zsh, csh




Environment Cyber Arena

Sudo Password CSEC2324_Student!

Part 1: Using TCPDump






1. Check to see what interfaces you can use for TCPDump 
2. Use the -i switch to collect data on the 172.16.0.0/23 network. 
Note -The -i option is used to identify the interface you want to use for collecting data.
3. Stop TCPDump with CTRL + C
4. Start TCPDump and collect only 10 packets on the 172.16.0.0/23 network. 

Part 2: Filtering with TCPDump

1. Start TCPDump but only collect ICMP traffic.
2. Take a screenshot of the output showing the results and add to your lab report.
3. Stop TCPDump with CTRL + C
4. Accomplish steps 1-3 again but with the following protocols:
 1. HTTP
 2. FTP
5. Capture packets coming from Host 172.16.0.50 to anywhere. Limit the capture to 20 packets. 
6. Capture packets only going to port 80. Limit the capture to 5 packets. 
7. Start TCPDump and save the output to a file named student_tcpdump.pcap 
8. Research how to create a rotating capture file.
9. Start TCPDump using a rotating capture file that are only 20MB in size and stop at 10 files.
10. Research how to use TCPDump to create a Ring Buffer trace.
11. Use TCPDump to perform a Ring Buffer Trace with the following parameters.

1. File Name: ring.pcap
 2. Create 3 files only
 3. run TCPDump in the background
 4. No host names
 5. No verbose
12. Write 300 words on how TCPDump can be used for malicious activities and add it to your reflections.

Part 3 - Wireshark

1. Start Wireshark by double clicking on the icon located to the left of your screen.
2. Next, open the three-way-handshake.pcap located in the pcap folder on your desktop.
3. Answer the following questions and add the questions and answers to your lab report file:
 1. What IP address started the conversation?
 2. What kind of session establishment is taking place? (hint: not looking for 3 way handshake)
 3. In a few words, explain why the three way handshake is important.
4. Close Wireshark
5. Start Wireshark again.
6. Click on the menu item Capture, then Options.
7. Select the interface that is associated with the 172.16.0.0/23 network
8. Make sure that promiscuous mode has a check mark. 
9. Now click Start located on the bottom right of the options screen.
10. Run the capture for 20 seconds, then click stop located towards the top left of the program. 
11. Why is promiscuous mode needed for capturing traffic?
12. Add question and answer to your lab report file.
13. Apply a display filter that only shows your hosts traffic as the source of the communication. 
14. Clear the display filter.
15. Search through the traffic and find all of the following Protocols with a display filter: 
 1. HTTP
 2. DNS
 3. ICMP
 4. ARP
16. Search through the traffic and find all of the following with a display filter: 
 1. DNS A records
 2. FTP Content

3. Unusual ICMP Traffic
4. Username of the FTP connection
5. Filename of FTP file transfer

Part 4 - Wireshark Exercises

In this section you will answer the following questions and add them to your lab report file.

1. Open “Wireshark”, then use the “File” menu and the “Open” command to open the file “Exercise One.pcap”. You should see 26 packets listed.
This set of packets describes a ‘conversation’ between a user’s client and a central server. This entire conversation happens automatically, after a user types something and hits enter. Look at the packets to answer the following questions in relation to this conversation.
2. In answering the following questions, use brief descriptions. For example, “In frame X, the client requests a web page, and in frame Y, the server delivers the content of the page.”
 1. What is the IP address of the client that initiates the conversation?
 2. Use the first two packets to identify the server that is going to be contacted. List the common name, and three IP addresses that can be used for the server.
 3. What is happening in frames 3, 4, and 5?
 4. What is happening in frames 6 and 7? Client is requesting a webpage and the server is acknowledging that request.
Ignore frame eight. However, for your information, frame eight is used to manage flow control.
 5. What is happening in frames nine and ten? How are these two frames related?
 6. What happens in packet 11?
 7. After the initial set of packets is received, the client sends out a new request in packet 12. This occurs automatically without any action by the user. Why does this occur? See the first “hint” to the left.
 8. What is occurring in packets 13 through 22?
 9. Explain what happens in packets 23 through 26.
 10. In one sentence describe what the user was doing (Reading email? Accessing a web page? FTP? Other?).
3. Write a 2 paragraphs (200 wordsish) reflecting on Wireshark and what you have learned.