# Lab 3 - DOS not just an Operating System

CSEC 2324 - Network Security
Lab Guide v1.0

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

January 2023

Cybersecurity
UA LITTLE ROCK | Department of Computer Science

# Contents

## 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 note 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 temaplate Eisogel 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.

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

## Lab Assignment 3 - DOS not just an Operating System

### Overview

This lab will introduce you to Denial of Service Attacks. Don't just go through the motions in this lab, but try to understand what you are doing and how your could defend against these attacks.

**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, hping3
**Operating System:** Linux
**Terminal Emulator:** bash, shell, zsh, csh
**Environment** Cyber Arena
**Sudo Password** CSEC2324_Student!

## Part 1: Using hping3

1. Log into the Cyber Arena
2. Select CSEC2324 Labs
3. Install hping3 from the command line. 📷
4. Research a type of denial of service attack that can be performed with hping3.
5. Perform that attack with the following requirements. 📷
    1. Target: 172.16.0.254
    2. Use TCPdump to save the attack to your home directory.
    3. Stop this attack around 10 seconds
6. Open the saved pcap with Wireshark 📷
7. Using display filters and other options in Wireshark and search for information that shows that this was a denial of service attack.
    1. Add all of the steps performed to your lab report file.
    2. Add all of your thoughts/reasoning to defend your claim that this was a DOS attack.
    3. Add screenshots showing evidence of DOS attack.
    4. There is not a word count but enough information should be present to show that this attack happened.
8. Submit your Lab report file and PCAP for full credit.

## Part 2: Spoofing

1. Log into the Cyber Arena

2. Select CSEC2324 Workout
3. Go to liquidswrds.com then click the link labeled schools.

4. Next, find your class in the list and click the picture.
5. Download arpspoofing.pcap that is located in the Man in the Middle folder.
6. Open this pcap with any tool you choose on the host machine.
7. Identify the following: 📷

    1. What is the attackers MAC Address?
    2. What kind of filter would be used to identify the source of this attack?

8. Answer the following questions in detail and add it to your reflections.

    1. What kind of network interface card is the attacker using?
    2. How can you tell that this is an ARP Spoofing attack from the Packet capture?
    3. What is the source MAC address of the ARP packet? Is it the same as the MAC address of the device it claims to be from?
    4. Is the ARP packet requesting or responding to an ARP request?
    5. Are there any other ARP packets in the capture with conflicting information? If so, how many?
    6. Are there any other indicators of suspicious activity in the packet capture, such as unexpected network traffic or unusual behavior from network devices?