

# Exploring Network Protocols with Scapy and Wireshark

Course Title: CSCI 297E: Ethical Hacking

Due Date: 2024-05-08

## Objective

This assignment aims to reinforce your understanding of network protocols and packet analysis using Scapy and Wireshark. You will practice crafting and sending packets, sniffing network traffic, and analyzing the results.

## Instructions

1. **Setup Wireshark for Packet Capture:** Open Wireshark with administrator privileges by executing `sudo -E wireshark` in the terminal. Select 'Capture' then 'Options', and choose to capture on 'any' interface to monitor all network traffic. Start the capture before beginning the exercises with Scapy.

2. **Scapy Interactive Tutorial:**

Follow the interactive tutorial available at [Scapy Documentation](#). Focus on sections that involve packet sniffing and spoofing. Execute at least 5 different commands, document the process, and analyze the traffic captured in Wireshark.

## Tasks

- Document each command used, describe its function, and analyze the resulting packet captures.
- Include screenshots from both Scapy and Wireshark as part of your report.
- Submit the pcap files along with your report to demonstrate the packet flows captured during your exercises.

## Submission Guidelines

- Submit a comprehensive report in PDF format including descriptions, screenshots, analyses, and a zip file containing the relevant pcap files.
- Ensure your submission is clear, organized, and thorough.

## Evaluation Criteria

- Accuracy and depth of command execution and packet analysis.
- Clarity and organization of the final report.
- Ability to identify and explain packet characteristics and potential security implications.