# 



Department of Electrical and Computer Engineering & Computer Science

Tagliatela college of engineering

**CSYS 4483-01/CSYS 6683-01**

**Network Defense**

Fall 2025

Instructor: **Dr. Tirthankar Ghosh**

## **Lab 1: Packet crafting with Scapy**

# **Submission deadline: September 9. Upload the report on Lab 1 assignment folder under Assignments on Canvas. One report per group.**

## Lab Overview

TCP has some serious security flaws in its design. RFC 793 does not prevent payload being transported on a TCP connection request packet (with SYN flag set). However, this is not the normal operation of TCP. If payload is transported on a connection request packet, it is left to the implementation of the TCP/IP stack to craft a response. Nonetheless, the vulnerability can be exploited to port malicious code to a server. This exercise is designed to provide hands-on exposure to craft TCP SYN segments with payload, and study response.

## Objective

The main objective of the exercise is to craft TCP SYN segments with payload, and study response.

**Systems needed:**

* Ubuntu/Fedora Linux VM (target)
* Kali Linux VM (attacker)

## Implementation Steps

**Carry out the following steps on the Ubuntu/Fedora Linux VM**

1. Install apache web server
2. Create a test page (index.html under /var/www/)
3. Edit the httpd.conf or apache.conf file to listen on the interface IP address and port 80
4. Start apache2
5. Stop any firewall service that maybe be running (iptables, firewalld)
6. Install Wireshark
7. Launch Wireshark
8. On the Wireshark window, go to Capture, Interfaces, and choose appropriate interface to capture
9. Start capture

**Carry out the following steps on the Kali VM**

1. Open an editor and type the following code

A screenshot of a computer

Description automatically generated

1. Edit the **dst IP address** to change it to the Ubuntu’s/Fedora’s interface IP address.
2. Save the file as “TCP\_SYN\_with\_data.py” and close the file
3. Run it by typing (check permission):

**./ TCP\_SYN\_with\_data.py**

**Go back to the Ubuntu/Fedora Linux VM**

1. Analyze Wireshark logs
2. Make sure you can see the HTTP payload sent with TCP SYN packet
3. Study the response from the Ubuntu/Fedora VM, what TCP flags are set on the response packet?
4. How did the Kali VM respond?

# A screenshot of a computer Description automatically generated

## Deliverables

# Submit a report showing the following. Upload the report on Lab 1 assignment folder under Assignments on Canvas (one report per group).

# Snapshot of the Wireshark capture showing TCP SYN with data packets and response packets

* One paragraph explaining the response of the target machine to TCP SYN packets with data