# 



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 2: Network packet analysis with Wireshark**

# **Submission deadline: September 16. Upload the report in Lab 2 assignment folder under Assignments on Canvas. One report per group.**

## Objective

The main objective of the exercise is to analyze captured network packets to detect malicious activities.

**Systems needed:**

* Any system with Wireshark installed

## Implementation Steps

Part 1:

1. Download pcap.pcapng and exploit.pcapng from Canvas (uploaded under the Labs module)
2. Launch Wireshark
3. Open pcap.pcapng
4. What unwanted activities can you detect?

­ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. What is the attacker IP address?
2. What is the target IP address? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. What tactics and techniques from MITRE ATT&CK Framework can you map these activities to?

Tactics: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Techniques: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Part 2:

1. Launch Wireshark
2. Open exploit.pcapng
3. What unwanted activities can you detect?

­

1. What protocol was used for these unwanted activities? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. What tactics and techniques from MITRE ATT&CK Framework can you map these activities to?

Tactics: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Techniques: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Deliverables

# Submit this lab worksheet in the Lab 2 assignment folder under Assignments on Canvas.