

# Lab-2 Report

**AIM:** Packet Capture and Network Traffic Analysis Using Wireshark & tcpdump

## 1. Introduction

The purpose of this lab is to provide hands-on experience in capturing and analyzing network traffic to identify potential security threats. Using tools like **Wireshark** and **tcpdump**, students will learn how to detect various types of attacks and security anomalies in a network, including **DoS attacks**, **port scanning**, **ARP spoofing**, **DNS spoofing**, and **cleartext data transmission**. These tools allow for detailed inspection of network traffic, providing insights into potential vulnerabilities and threats in a network environment.

## 2. Objective

- To use **Wireshark** and **tcpdump** for capturing and analyzing network traffic.
- To detect potential security threats and abnormal patterns such as SYN Floods, port scanning, ARP poisoning, DNS spoofing, and cleartext transmission of sensitive data.

## 3. Tools & Resources

- **Wireshark:** A graphical network protocol analyzer.
  - Official site: [Wireshark](#)
- **tcpdump:** A command-line network packet analyzer.
  - Installation for Linux: `sudo apt install tcpdump`
- **Kali Linux** (for simulating attacks)
- **Ubuntu/Windows** (for performing normal operations and being attacked)
- **Nmap** (for scanning and testing vulnerabilities)

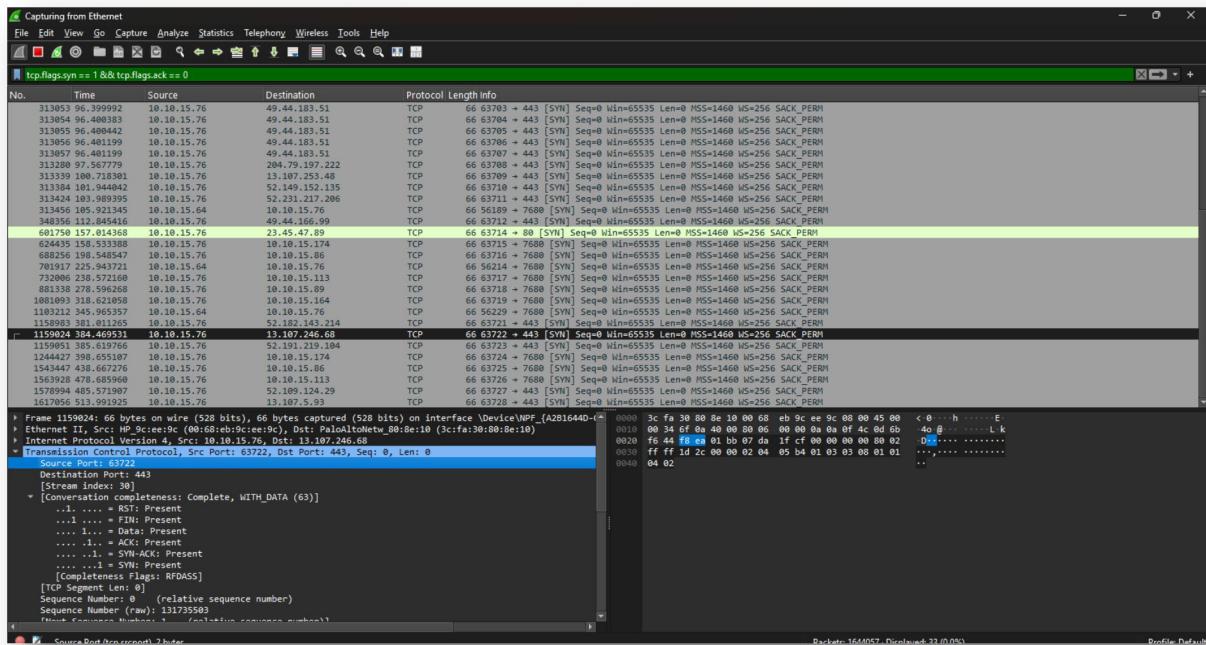
## 4. Methodology

### 4.1. Installation & Setup

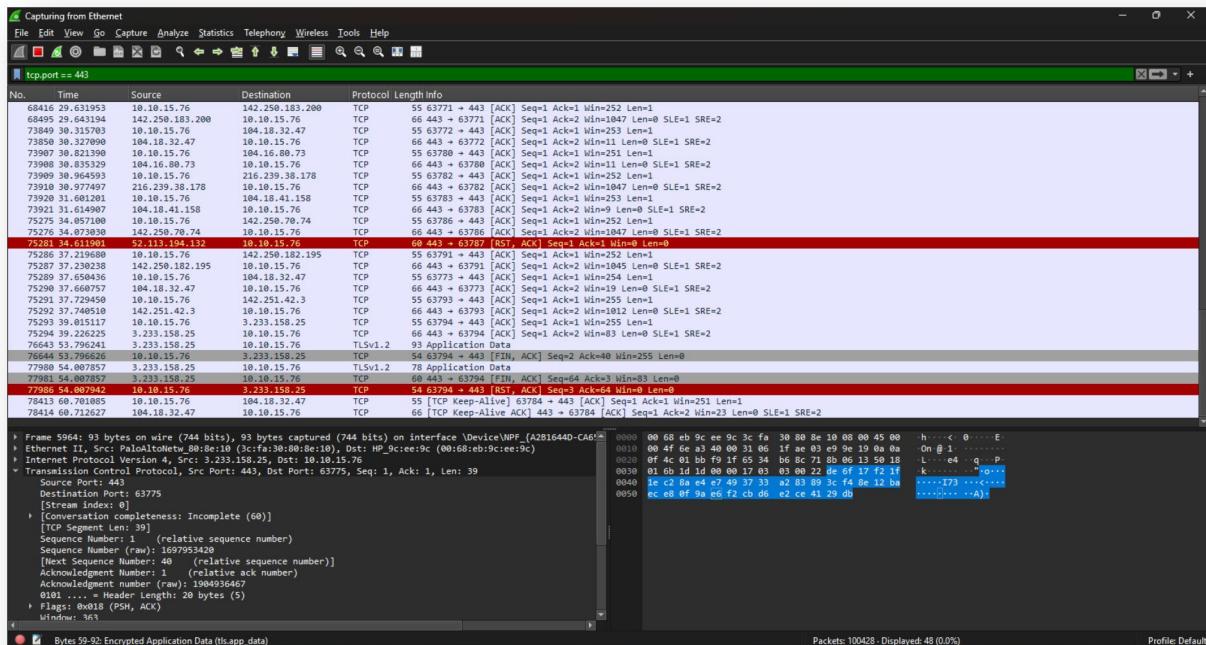
1. **Wireshark** was installed on the system, ensuring that the network interface was correctly selected for packet capture.
2. **tcpdump** was installed on both Kali Linux and Ubuntu systems to capture traffic from a command-line interface.
3. A **Virtual Lab Network** was created using virtual machines, assigning static IP addresses (e.g., Kali: 192.168.1.1, Ubuntu: 192.168.1.2) to allow safe and controlled testing of network behaviors.

## 5. Results

### SYN Flood Attack



### Port Scanning



## **6. Conclusion**

Packet capture and network traffic analysis using tools like Wireshark and tcpdump are essential for gaining deep insights into network performance, identifying issues, and ensuring security.