**Network Traffic Analysis with Wireshark**

**Task 5: Capture and Analyze Network Traffic Using Wireshark**

This repository contains the deliverables for a comprehensive network packet capture and analysis exercise using Wireshark on Kali Linux.

**Objective**

Capture live network packets using Wireshark and identify basic protocols and traffic types. This exercise demonstrates:

* Network packet capture techniques
* Protocol identification and analysis
* Traffic pattern recognition
* Security assessment of network communications
* Practical use of Wireshark filtering and analysis tools

**Installation on Kali Linux**

# Update package repositories  
sudo apt update  
  
# Install Wireshark (if not already installed)  
sudo apt install wireshark  
  
# Add user to wireshark group to avoid running as root  
sudo usermod -a -G wireshark $USER  
  
# Logout and login again for group changes to take effect

**1. Basic Packet Capture**

# Start Wireshark with GUI  
sudo wireshark  
  
# Or use command-line capture with tshark  
sudo tshark -i eth0 -a duration:60 -w network\_capture.pcap

**2. Generate Network Traffic**

While capturing, perform these activities:

# Web browsing traffic  
curl -I https://google.com  
curl -I https://github.com  
  
# DNS queries   
nslookup google.com  
dig github.com  
  
# Ping tests  
ping -c 5 8.8.8.8  
ping -c 3 1.1.1.1  
  
# Port scanning (limited)  
nmap -p 80,443 google.com

**3. Analysis Commands**

# View capture file statistics  
capinfos network\_capture.pcap  
  
# Extract specific protocols  
tshark -r network\_capture.pcap -Y "http"   
tshark -r network\_capture.pcap -Y "dns"  
tshark -r network\_capture.pcap -Y "tcp"  
  
# Protocol hierarchy statistics  
tshark -r network\_capture.pcap -q -z io,phs

**Detailed Analysis**

**Common Wireshark Filters**

# HTTP traffic only  
http  
  
# DNS queries and responses  
dns  
  
# TCP handshakes  
tcp.flags.syn==1  
  
# Large packets (>1000 bytes)  
frame.len > 1000  
  
# Specific IP address  
ip.addr == 8.8.8.8  
  
# Port-specific traffic  
tcp.port == 80 or tcp.port == 443

**Common Issues**

**Permission Denied Errors:**

# Add user to wireshark group  
sudo usermod -a -G wireshark $USER  
# Then logout/login  
  
# Alternative: run with sudo (not recommended)  
sudo wireshark

**No Packets Captured:**

# Check network interfaces  
ip link show  
  
# Verify interface is active  
sudo tshark -D  
  
# Test with different interface  
sudo tshark -i any -c 10

**Large Capture Files:**

# Limit capture size  
sudo tshark -i eth0 -a filesize:10000 -w capture.pcap  
  
# Limit by packet count   
sudo tshark -i eth0 -c 1000 -w capture.pcap