PROJECT REPORT

Name Sudhir S Bhat

Title: Understanding Network Security & Basic Traffic Monitoring

1. Introduction

Networks form the backbone of modern communication, enabling data exchange between computers, servers, and applications. With the increasing dependency on networks, securing them has become critical. Network Security focuses on protecting data during transmission and preventing unauthorized access, misuse, or disruption of network services.

This task introduces interns to network security fundamentals and basic traffic monitoring, helping them understand how data flows across networks and how attackers attempt to exploit network weaknesses using only safe, legal, and ethical tools.

2. Objective

The main objectives of this task are:

- To understand how data travels across a network
- To learn basic network security concepts
- To identify common network threats
- To observe and analyze network traffic safely
- To understand how attackers exploit network vulnerabilities without performing any malicious activity

3. Network Security Overview

Network Security is the practice of protecting networks and data from unauthorized access, attacks, and misuse. It ensures.

- **Confidentiality** – Data is protected from unauthorized users
- **Integrity** – Data is not altered during transmission
- **Availability** – Network services remain accessible.

4. How Data Travels Across a Network

When data is sent from one device to another

- Data is broken into small units called packets
- Packets travel through routers and switches

Each packet contains

- Source IP address
- Destination IP address
- Protocol information

The packets are reassembled at the destination

5. Common Network Protocols Observed

- **HTTP / HTTPS** – Web communication
- **TCP** – Reliable data transfer
- **UDP** – Fast but unreliable communication
- **DNS** – Domain name resolution
- **ICMP** – Network diagnostics

6. Common Network Threats

- Packet sniffing
- Man-in-the-Middle (MITM) attacks
- Denial of Service (DoS) attacks
- IP spoofing
- Unauthorized network access

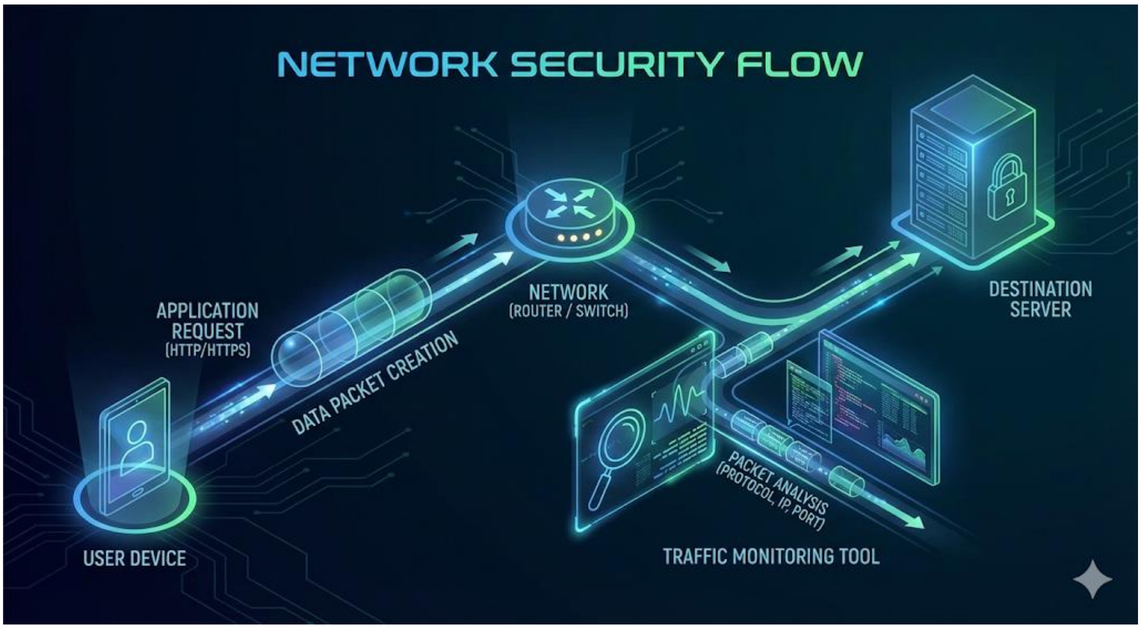
7. Basic Traffic Monitoring

It perform passive traffic observation using legal tools such as

- Wireshark (read-only packet analysis)
- System network monitors
- Activities Performed:
- Observed live network packets

- Identified common protocols
- Analyzed source and destination IP addresses
- Understood packet headers (no payload manipulation)

8. Network Security Flow Diagram


NETWORK SECURITY FLOW
APPLICATION REQUEST (HTTP/HTTPS)
DATA PACKET CREATION
NETWORK (ROUTER / SWITCH)
DESTINATION SERVER
USER DEVICE
PACKET ANALYSIS (PROTOCOL, IP, PORT)
TRAFFIC MONITORING TOOL

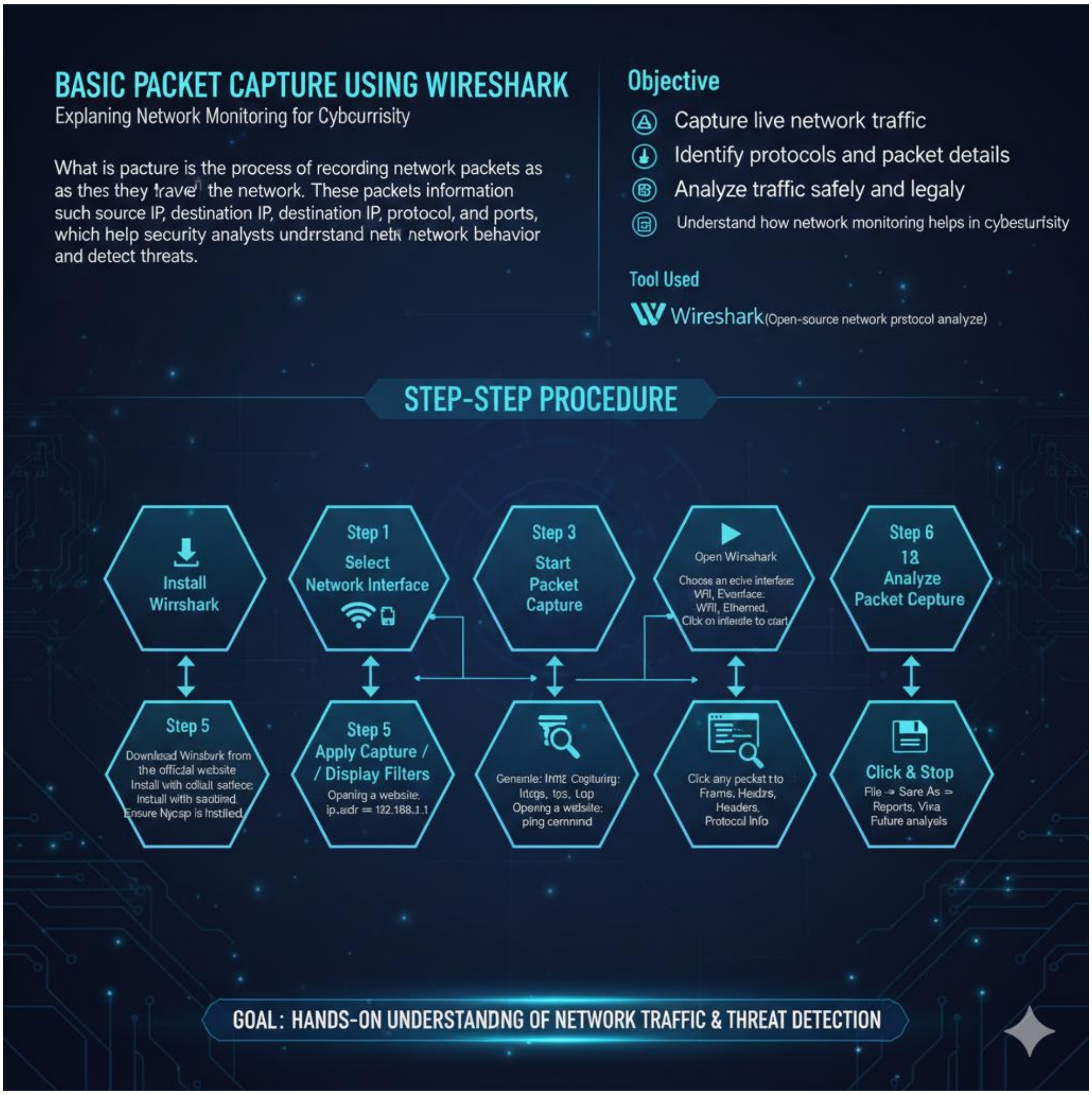
9. Attacker Exploitation

Attackers may exploit

- Unencrypted traffic
- Open ports
- Weak authentication
- Misconfigured network devices

Understanding these concepts helps in preventing attacks, not performing them.

10. Basic Packet Capture Using Wireshark (Step-by-Step)



BASIC PACKET CAPTURE USING WIRESHARK

Explaning Network Monitoring for Cybcurrisity

What is pacture is the process of recording network packets as as thes they 'rave' the network. These packets information such source IP, destination IP, destination IP, protocol, and ports, which help security analysts undrrstand netk network behavior and detect threats.

Objective

- Capture live network traffic
- Identify protocols and packet details
- Analyze traffic safely and legaly
- Understand how network monitoring helps in cybesturisity

Tool Used

Wireshark(Open-source network prstocol analyze)

STEP-STEP PROCEDURE

Install Wirrshark
Step 1 Select Network Interface
Step 3 Start Packet Capture
Open Wirsahark
Choos an ecive interfase: WFI, Everiface: WFII, Elherned. Clck on inleiste to ctart
Step 6 12 Analyze Packet Cepture
Step 5 Download Winsburk from the officdal website Install with cdllall satfece: Install with saotimd. Ensure Nycsp is Instlled
Step 5 Apply Capture / / Display Filters Opanirg a website: ip.aidr == 122.188.1.1
Genenle: Inmz Cogituring: Intcgs, tps, Lop Opening a website: ping cemnnd
Click any peckst tto Frams, Heidzs, Headers, Protocol Info
Click & Stop File → Sare As ⇒ Reports, Vira Future analyels

GOAL: HANDS-ON UNDERSTANDNG OF NETWORK TRAFFIC & THREAT DETECTION

What is Packet Capture?

Packet capture is the process of recording network packets as they travel across a network. These packets contain information such as source IP, destination IP, protocol, and ports, which help security analysts understand network behavior and detect threats.

Objective

- Capture live network traffic
- Identify protocols and packet details
- Analyze traffic safely and legally

- Understand how network monitoring helps in cybersecurity

Tool Used

- Wireshark (Open-source network protocol analyzer)

Step-by-Step Procedure

Step 1 Install Wireshark

- Download Wireshark from the official website
- Install with default settings
- Ensure Npcap is installed (required for packet capture)

Step 2 Select Network Interface

Open Wireshark

Choose an active interface

- Wi-Fi (for wireless traffic)
- Ethernet (for wired traffic)
- Click on the interface to start capture

Select the interface showing live packet movement.

Step 3 Start Packet Capture

Click Start Capturing Packets

Wireshark begins capturing real-time traffic

Generate traffic by

- Opening a website
- Running a ping command
- Using any internet application

Step 4 Apply Capture / Display Filters

Examples

- **http** → View HTTP traffic
- **https** → Encrypted web traffic
- **tcp** → TCP packets
- **udp** → UDP packets
- **ip.addr** == 192.168.1.1 → Specific IP

Filters help reduce noise and focus analysis.

Step 5 Analyze Packet Details

Click any packet to view

- Frame – Packet size and time
- Ethernet Header – MAC addresses
- IP Header – Source & destination IP
- Transport Layer – TCP/UDP ports
- Protocol Info – HTTP, DNS, etc.

Step 6 Stop & Save Capture

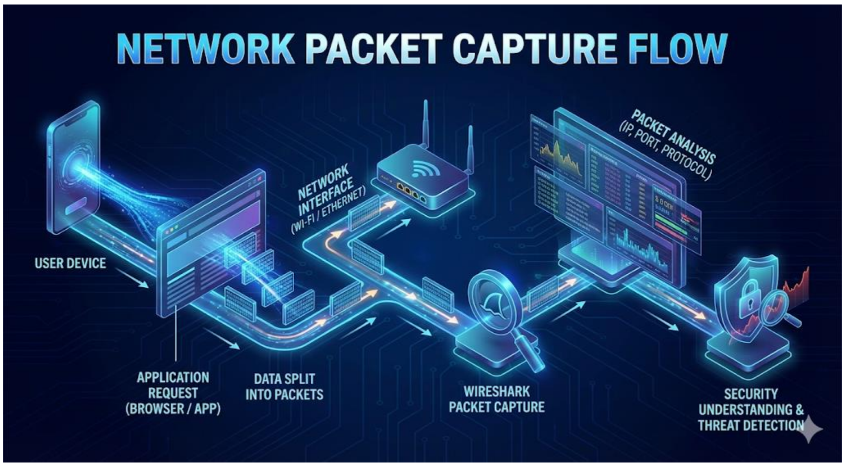
Click Stop

File → Save As → .pcap

This file can be used for

- Reports
- Future analysis

Network Packet Capture Flow Diagram


NETWORK PACKET CAPTURE FLOW
USER DEVICE
APPLICATION REQUEST (BROWSER / APP)
DATA SPLIT INTO PACKETS
NETWORK INTERFACE (WI-FI / ETHERNET)
WIRESHARK PACKET CAPTURE
PACKET ANALYSIS (IP, PORT, PROTOCOL)
SECURITY UNDERSTANDING & THREAT DETECTION

11. Challenges Faced

Understanding packet-level data initially

- Identifying protocols correctly
- Interpreting IP addresses and ports
- Differentiating normal vs suspicious traffic

These challenges were overcome through practice and guided learning.

12. Project Outcomes

After completing the following outcomes were achieved

- Clear understanding of network security basics
- Knowledge of data packet flow
- Ability to identify common network protocols
- Awareness of network-based attacks
- Hands-on exposure to traffic monitoring tools
- Ethical understanding of safe network analysis

13. Lessons Learned

- Network security is critical for protecting data in transit
- Even simple traffic analysis reveals valuable insights
- Encryption (HTTPS) plays a major role in security
- Misconfigured networks are easy targets
- Ethical monitoring is essential in cybersecurity

14. Conclusion

This task successfully introduced the fundamentals of network security and basic traffic monitoring. By understanding how data flows across networks and how attackers exploit weaknesses, interns gain a strong foundation for advanced cybersecurity concepts. The task emphasizes ethical learning, awareness, and prevention, which are essential for a cybersecurity professional.