DATE: 30/1/2024

Location: Tinkerspace, Kochi

Project Documentation of

Network Traffic Analysis

BY: RAKHFAN JIMSHAF

COMPANY NAME
KERALA , INDIA

1.INTRODUCTION

The purpose of this Wireshark project was to capture and analyze network traffic in a real environment with multiple devices. The goal was to gain insights into the types of traffic present, identify protocols, and investigate packet details.

2. METHODOLOGY

NETWORK ENVIRONMENT SETUP

I used a real-world network environment with diverse devices, including computers, phones, and routers. Each device played a specific role in the network, contributing to varied traffic patterns.

TOOLS AND EQUIPMENT

Wireshark was the primary tool used for capturing and analyzing network traffic. The devices were connected to a hub or switch, allowing for efficient packet capture. No specific configurations were made on the devices to maintain a naturalistic environment.

3.CAPTURE PROCESS

Wireshark was utilized to capture network traffic. Filters were applied during capture to focus on specific protocols and enhance the relevance of the captured data.

4. ANALYSIS

IDENTIFICATION OF TRAFFIC TYPES

Captured data was analyzed to identify various types of traffic, such as HTTP, DNS, and FTP. Wireshark filters were instrumental in isolating specific protocols for in-depth analysis.

5.PACKET INVESTIGATION

SOURCE AND DESTINATION IP ADDRESSES

Packet details, including source and destination IP addresses, were investigated to understand communication patterns within the network.

PROTOCOL ANALYSIS

Wireshark's protocol analysis capabilities were leveraged to examine the protocols used in the captured traffic. This included a detailed investigation of the headers and payloads of relevant packets.

6. RESULTS

The analysis of the captured network traffic uncovered a rich tapestry of communication within the real-world environment. The predominant presence of HTTP traffic suggests active web browsing and data retrieval activities across the network.

TRAFFIC DIVERSITY

A diverse array of applications and services were identified, indicating a realistic mix of business and personal usage. This included not only standard HTTP and HTTPS traffic but also streaming services, file transfers, and various cloud-based applications.

ANOMALY DETECTION

While investigating DNS requests and responses, anomalies were detected, such as unusually high query rates and unexpected domains. These findings hint at potential security or configuration issues that demand attention in a genuine network environment. Further investigation into these anomalies could unveil security threats, misconfigurations, or unauthorized network access.

PROTOCOL UTILIZATION

In-depth analysis of the protocols used in the captured traffic highlighted the prevalence of modern communication standards. The presence of TLS within HTTP traffic underscored the encryption practices employed by applications, emphasizing the importance of securing data in transit.

COMMUNICATION PATTERN

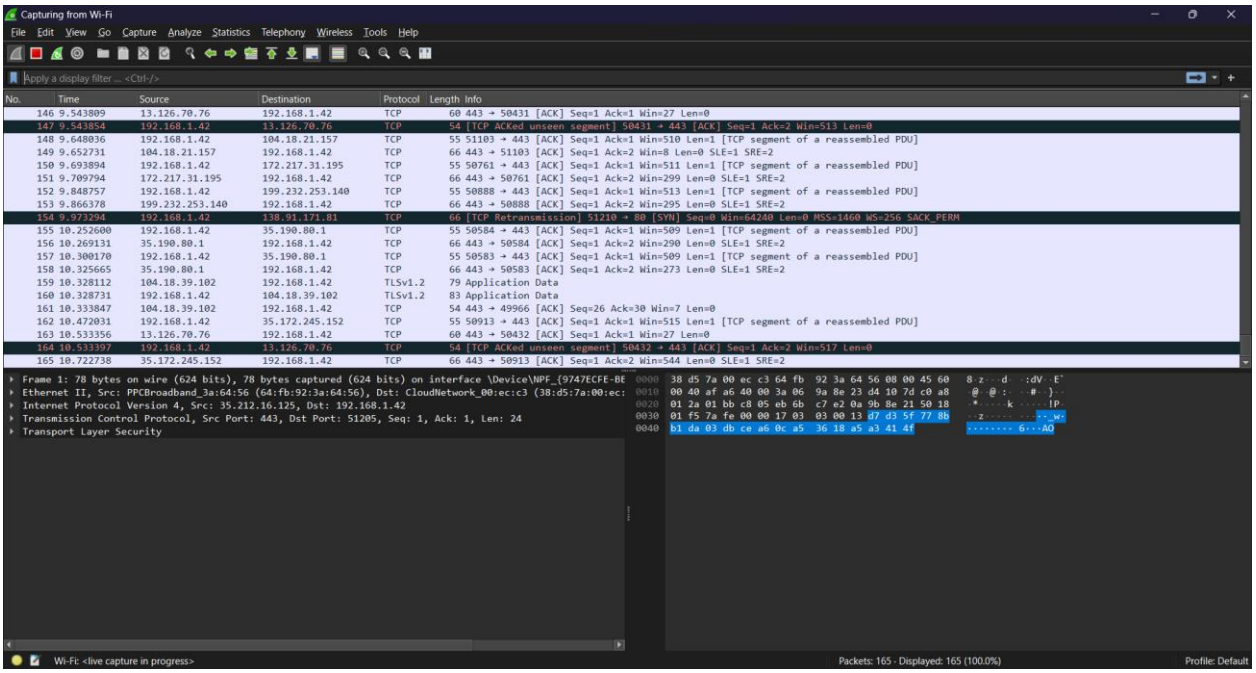
Source and destination IP addresses were scrutinized to discern communication patterns. The identification of frequent and irregular communication between specific devices could be indicative of organizational workflows, collaboration, or potential security concerns

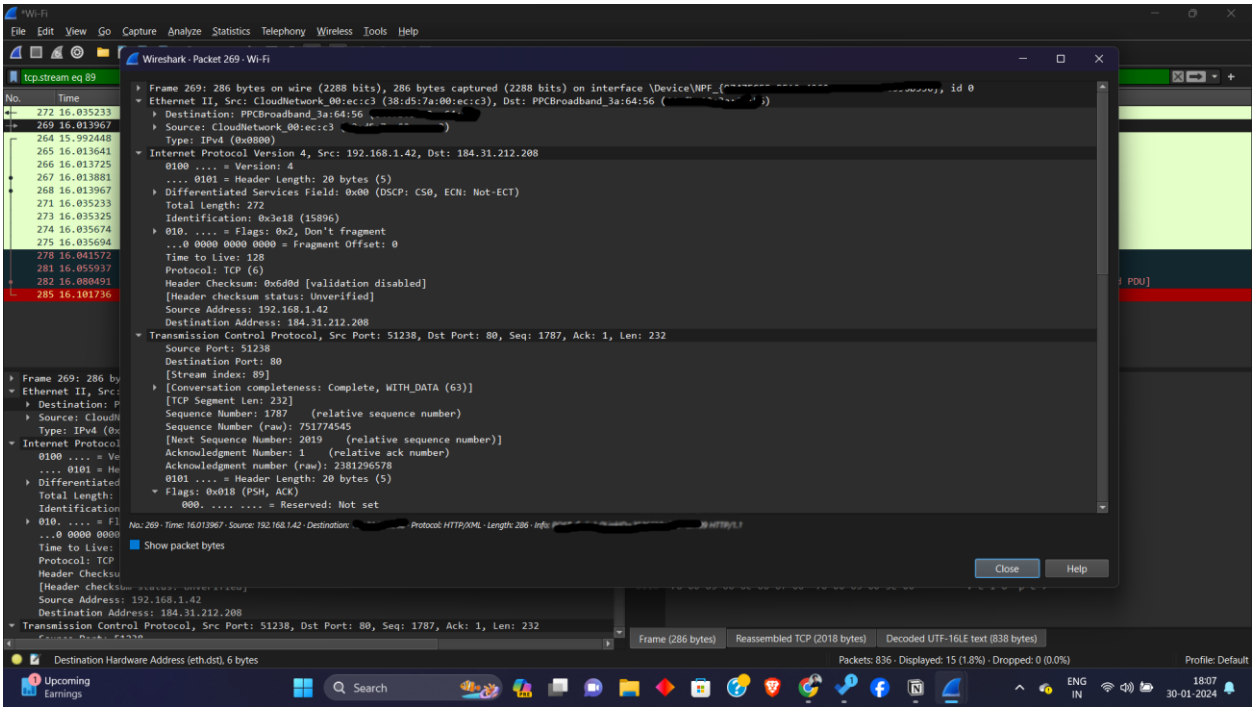
7. CONCLUSION

In conclusion, the results obtained from this Wireshark project provide a realistic depiction of network activities in a diverse and dynamic environment. The identified anomalies and communication patterns not only reflect common scenarios but also offer a foundation for informed decision-making to enhance both security and performance in a real-world network setting.

8. APPENDIX

SCREENSHOTS





GLOSSARY

Author: Rakhfan Jimshaf

A

Anomalies: Irregularities or deviations from the expected behavior within the network traffic, potentially indicating security threats, misconfigurations, or unauthorized activities.

D

DNS (Domain Name System): A decentralized naming system that translates human-readable domain names into IP addresses, facilitating the identification of resources on a network.

H

HTTP (Hypertext Transfer Protocol): A protocol used for transmitting hypertext (web) content over the Internet. HTTPS (Hypertext Transfer Protocol Secure) is a secure version of HTTP.

I

IP Address: A numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication.

P

Packet: A unit of data transmitted over a network. In Wireshark, packets represent the fundamental units of information captured during network traffic analysis.

Protocol: A set of rules that defines the format and sequence of messages exchanged between devices in a network.

T

TLS (Transport Layer Security): A cryptographic protocol that ensures the privacy and data integrity of communications over a computer network, commonly used to secure web browsing.

U

URL (Uniform Resource Locator): A web address that specifies the location of a resource on the internet, such as a website or file.