CN Project:

Project Title: Packet Sniffer

Member Names:

1. Syed Baqar Ali Zaidi (19K-1033)
2. Khubaib Alam (19K-1050)

Section: BSE-5B

Instructor: Mr.Shoaib Raza

INTRODUCTION:

In IT operations, ensuring secure and reliable communications over different networks is a crucial requirement. IT administrators have to rely on different protocols, networking best practices, and network monitoring tools to ensure the flow of data in a network meets various standards for security and Quality of Service (QoS). One of these common practices is known as packet sniffing, which helps IT administrators keep track of packets (small formatted units of data) and ensure they're transferred smoothly. While the packet sniffing technique is often associated with cyberattacks, it's commonly used by internet service providers, government agencies, advertisers, and even large organizations for network monitoring. In this article, we'll discuss packet sniffing in detail and also explore commonly used tools by IT practitioners.

ADVANTAGES OF PACKET SNIFFER:

1. Detecting the Root Cause of a Network Issue
2. Troubleshooting Network Issues
3. Traffic Analysis
4. Bandwidth Management
5. Network Security and Compliance

FEATURES:

1. Ethernet frames unpacking:
    a. Destination MAC Address
    b. Source MAC Address
    c. Ethernet Protocol
    d. Formatting MAC addresses
2. Ipv4 frames unpacking:
    a. Version
    b. Header length
    c. Source
    d. Destination

3. TCP frames unpacking
    a. Flags
    b. Offset
    c. Source port
    d. Destination port
    e. Sequence number
    f. Acknowledgement
4. UDP frames unpacking
    a. Source port
    b. Destination port
5. ICMP frames unpacking
    a. Icmp category
    b. Code
    c. checksum
6. DNS packets
7. HTTP packets
8. HTTPS packets
9. IMAP packets
10. SMTP packets
11. Telnet packets

METHODOLOGY:

1. Building connection with the socket.
2. Then getting raw data from the socket directly from the physical layer.
3. Unpacking the data on the physical layer.
4. Unpacking the data on the IP layer.
5. Unpacking the data on the TCP layer.
6. Unpacking the data on the application layer.

FUNCTION DESCRIPTION & RESULTS:

1. ETHERNET:

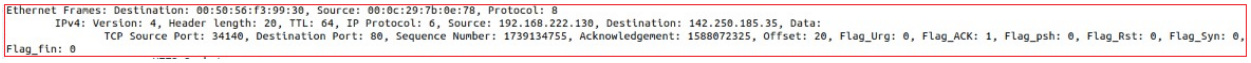

Fig1: Displaying Ethernet Frames with source and destination MACs

2. IPV4:

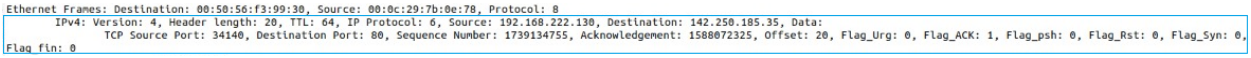

Fig2: Displaying ipv4 packets with source and destination IPs

3. TCP:

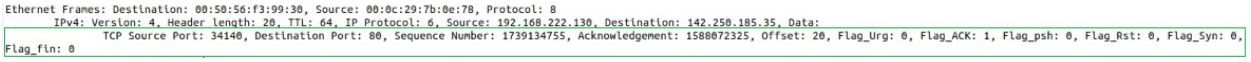

Fig3: Displaying TCP Packets with source and destination ports

4. UDP:

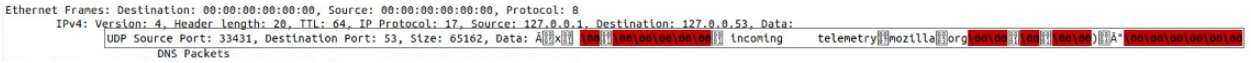

Fig4: Displaying packets with source and destination ports

5. ICMP:

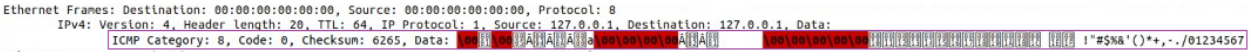

Fig5: Displaying ICMP with category, code, and checksum

6. DNS:

Fig6: Displaying DNS packets

7. HTTP:

Fig7: Displaying HTTP packets

8. HTTPS:

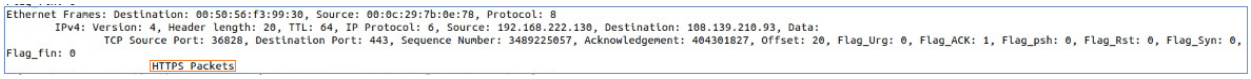

Fig8: Displaying HTTPS packets

CONCLUSION:

The program is unpacking the raw data on all layers and returning the packets in an understandable form to be printed to show sniffed packets.