

Mini Project Report

of

Computer Networks LAB

TITLE

TCP-IP Packet Sniffer

SUBMITTED

BY

STUDENT NAME REG. NO, ROLL NO, SECTION

Shyam Sundar Bharathi S 200905302, 53, B

Ajay Rajendra Kumar 200905390, 61, B

ABSTRACT:

A Packet Sniffer is a program that can record all network packets that travel past a given network interface, on a given computer, on a network. It can be used to troubleshoot network problems, as well as to extract sensitive information such as Credentials from unencrypted Login Session's.

Unlike telephone circuits, computer networks are shared communication channels. It is simply too expensive to dedicate local loops to the switch (hub) for each pair of communicating computers. Sharing means that computers can receive information that was intended for other machines. To capture the information going over the network is called sniffing.

Most popular way of connecting computers is through Ethernet. Ethernet protocol works by sending packet information to all the hosts on the same circuit. The packet header contains the proper address of the destination machine. Only the machine with the matching address is supposed to accept the packet. A machine that is accepting all packets, no matter what the packet header says, is said to be in promiscuous mode.

Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favourite weapon in the hacker's arsenal.

1. **INTRODUCTION**

**1.1 General Introduction to the topic**

A packet sniffer — also known as a packet analyzer, protocol analyzer or network analyzer — is a piece of hardware or software used to monitor network traffic. Sniffers work by examining streams of data packets that flow between computers on a network as well as between networked computers and the larger Internet. These packets are intended for — and addressed to — specific machines but using a packet sniffer in "promiscuous mode" allows IT professionals, end users or malicious intruders to examine any packet, regardless of destination. It's possible to configure sniffers in two ways. The first is "unfiltered," meaning they will capture all packets possible and write them to a local hard drive for later examination. Next is "filtered" mode, meaning analyzers will only capture packets that contain specific data elements.

**1.2 Hardware and Software Requirements**

To project has been made using the C programming language.

The software requirements include:

* GCC Compiler
* A text editor
* Linux Operating System

The Hardware requirements include:

* A computer / laptop running Linux OS

A good internet connection

**2. Problem definition**

The aim of this application is to read packets that travel across various layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) model of network architecture. The packet sniffer will analyze the network traffic to allow users to get a practical understanding of the flow of packets in a network.

It will be used to capture and analyze the following protocols’ header information from the packets:

Application Layer: HTTP, DNS Transport Layer: TCP, UDP Network Layer: IPv4, IPv6 Data Link Layer: ARP

The packets captured will be analyzed to extract and display the header information along with other relevant parameters for the selected protocols.

1. Objectives

The project objectives are as follows:

* To gain an understanding of what is packet sniffing.
* To understand how packet sniffing works.
* What are the different types of packet sniffing.
* How to perform packet sniffing.
* Analyzing the results obtained by performing packet sniffing.
* How sniffing attacks can illegally access and read unencrypted data.

1. Methodology

The main function opens a socket and listens for packets in the process. Information about the packets is passed on to a function that processes the ethernet protocol. It strips the header, and based on data fields, passes it on to appropriate higher-level protocols (IPv4, IPv6, ARP, etc.), from where similar process is followed and further higher-level protocols are called to be processed (TCP, UDP). Functions to parse DNS messages and HTTP headers are also written in the source code. All information retrieved at each layer from all the protocols are neatly printed into the log file that is generated as “log.txt”

1. Implementation Details

Packet number 1

Packet type: DNS

DNS message

DNS Header:

|-Identification Number : 54604

|-Recursion Desired : 1

|-Truncated Message : 0

|-Authoritative Answer : 0

|-Purpose of message : 0

|-Query/Response Flag : 0

|-Response code : 0

|-Checking Disabled : 0

|-Authenticated data : 0

|-Recursion available : 0

|-Number of question entries : 256

|-Number of answer entries : 0

|-Number of authority entries: 0

|-Number of resource entries : 0

UDP Header

|-Source Port : 39396

|-Destination Port : 53

|-UDP Length : 43

|-UDP Checksum : 15808

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 63 Bytes(Size of Packet)

|-Identification : 47443

|-TTL : 64

|-Protocol : 17

|-Checksum : 44182

Ethernet Header:

-->Destination Address : 30-E3-7A-10-DD-D5

|-Source Address : 48-BF-6B-DF-21-D8

|-Protocol : 8

Packet number 2

Packet type: DNS

DNS message

DNS Header:

|-Identification Number : 6650

|-Recursion Desired : 1

|-Truncated Message : 0

|-Authoritative Answer : 0

|-Purpose of message : 0

|-Query/Response Flag : 0

|-Response code : 0

|-Checking Disabled : 0

|-Authenticated data : 0

|-Recursion available : 0

|-Number of question entries : 256

|-Number of answer entries : 0

|-Number of authority entries: 0

|-Number of resource entries : 0

UDP Header

|-Source Port : 34148

|-Destination Port : 53

|-UDP Length : 43

|-UDP Checksum : 65342

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 63 Bytes(Size of Packet)

|-Identification : 45566

|-TTL : 64

|-Protocol : 17

|-Checksum : 35245

Ethernet Header:

-->Destination Address : 00-00-00-00-00-00

|-Source Address : 00-00-00-00-00-00

|-Protocol : 8

Packet number 3

Packet type: DNS

DNS message

DNS Header:

|-Identification Number : 6650

|-Recursion Desired : 1

|-Truncated Message : 0

|-Authoritative Answer : 0

|-Purpose of message : 0

|-Query/Response Flag : 0

|-Response code : 0

|-Checking Disabled : 0

|-Authenticated data : 0

|-Recursion available : 0

|-Number of question entries : 256

|-Number of answer entries : 0

|-Number of authority entries: 0

|-Number of resource entries : 0

UDP Header

|-Source Port : 34148

|-Destination Port : 53

|-UDP Length : 43

|-UDP Checksum : 65342

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 63 Bytes(Size of Packet)

|-Identification : 45566

|-TTL : 64

|-Protocol : 17

|-Checksum : 35245

Ethernet Header:

-->Destination Address : 00-00-00-00-00-00

|-Source Address : 00-00-00-00-00-00

|-Protocol : 8

Packet number 4

Packet type: DNS

DNS message

DNS Header:

|-Identification Number : 6650

|-Recursion Desired : 1

|-Truncated Message : 0

|-Authoritative Answer : 0

|-Purpose of message : 0

|-Query/Response Flag : 1

|-Response code : 5

|-Checking Disabled : 0

|-Authenticated data : 0

|-Recursion available : 1

|-Number of question entries : 256

|-Number of answer entries : 0

|-Number of authority entries: 0

|-Number of resource entries : 0

UDP Header

|-Source Port : 53

|-Destination Port : 34148

|-UDP Length : 43

|-UDP Checksum : 65342

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 63 Bytes(Size of Packet)

|-Identification : 14192

|-TTL : 64

|-Protocol : 17

|-Checksum : 1084

Ethernet Header:

-->Destination Address : 00-00-00-00-00-00

|-Source Address : 00-00-00-00-00-00

|-Protocol : 8

Packet number 5

Packet type: DNS

DNS message

DNS Header:

|-Identification Number : 6650

|-Recursion Desired : 1

|-Truncated Message : 0

|-Authoritative Answer : 0

|-Purpose of message : 0

|-Query/Response Flag : 1

|-Response code : 5

|-Checking Disabled : 0

|-Authenticated data : 0

|-Recursion available : 1

|-Number of question entries : 256

|-Number of answer entries : 0

|-Number of authority entries: 0

|-Number of resource entries : 0

UDP Header

|-Source Port : 53

|-Destination Port : 34148

|-UDP Length : 43

|-UDP Checksum : 65342

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 63 Bytes(Size of Packet)

|-Identification : 14192

|-TTL : 64

|-Protocol : 17

|-Checksum : 1084

Ethernet Header:

-->Destination Address : 00-00-00-00-00-00

|-Source Address : 00-00-00-00-00-00

|-Protocol : 8

Packet number 6

Packet type: DNS

DNS message

DNS Header:

|-Identification Number : 54604

|-Recursion Desired : 1

|-Truncated Message : 0

|-Authoritative Answer : 0

|-Purpose of message : 0

|-Query/Response Flag : 1

|-Response code : 5

|-Checking Disabled : 0

|-Authenticated data : 0

|-Recursion available : 1

|-Number of question entries : 256

|-Number of answer entries : 0

|-Number of authority entries: 0

|-Number of resource entries : 0

UDP Header

|-Source Port : 53

|-Destination Port : 39396

|-UDP Length : 43

|-UDP Checksum : 48442

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 63 Bytes(Size of Packet)

|-Identification : 13894

|-TTL : 64

|-Protocol : 17

|-Checksum : 61347

Ethernet Header:

-->Destination Address : 48-BF-6B-DF-21-D8

|-Source Address : 30-E3-7A-10-DD-D5

|-Protocol : 8

Packet number 7

Packet type: DNS

DNS message

DNS Header:

|-Identification Number : 20058

|-Recursion Desired : 1

|-Truncated Message : 0

|-Authoritative Answer : 0

|-Purpose of message : 0

|-Query/Response Flag : 0

|-Response code : 0

|-Checking Disabled : 0

|-Authenticated data : 0

|-Recursion available : 0

|-Number of question entries : 256

|-Number of answer entries : 0

|-Number of authority entries: 0

|-Number of resource entries : 0

UDP Header

|-Source Port : 46146

|-Destination Port : 53

|-UDP Length : 43

|-UDP Checksum : 5609

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 63 Bytes(Size of Packet)

|-Identification : 55249

|-TTL : 64

|-Protocol : 17

|-Checksum : 36376

Ethernet Header:

-->Destination Address : 30-E3-7A-10-DD-D5

|-Source Address : 48-BF-6B-DF-21-D8

|-Protocol : 8

Packet number 8

Packet type: DNS

DNS message

DNS Header:

|-Identification Number : 24238

|-Recursion Desired : 1

|-Truncated Message : 0

|-Authoritative Answer : 0

|-Purpose of message : 0

|-Query/Response Flag : 0

|-Response code : 0

|-Checking Disabled : 0

|-Authenticated data : 0

|-Recursion available : 0

|-Number of question entries : 256

|-Number of answer entries : 0

|-Number of authority entries: 0

|-Number of resource entries : 0

UDP Header

|-Source Port : 25561

|-Destination Port : 53

|-UDP Length : 43

|-UDP Checksum : 65342

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 63 Bytes(Size of Packet)

|-Identification : 45567

|-TTL : 64

|-Protocol : 17

|-Checksum : 35244

Ethernet Header:

-->Destination Address : 00-00-00-00-00-00

|-Source Address : 00-00-00-00-00-00

|-Protocol : 8

Packet number 9

Packet type: DNS

DNS message

DNS Header:

|-Identification Number : 24238

|-Recursion Desired : 1

|-Truncated Message : 0

|-Authoritative Answer : 0

|-Purpose of message : 0

|-Query/Response Flag : 0

|-Response code : 0

|-Checking Disabled : 0

|-Authenticated data : 0

|-Recursion available : 0

|-Number of question entries : 256

|-Number of answer entries : 0

|-Number of authority entries: 0

|-Number of resource entries : 0

UDP Header

|-Source Port : 25561

|-Destination Port : 53

|-UDP Length : 43

|-UDP Checksum : 65342

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 63 Bytes(Size of Packet)

|-Identification : 45567

|-TTL : 64

|-Protocol : 17

|-Checksum : 35244

Ethernet Header:

-->Destination Address : 00-00-00-00-00-00

|-Source Address : 00-00-00-00-00-00

|-Protocol : 8

Packet number 10

Packet type: DNS

DNS message

DNS Header:

|-Identification Number : 24238

|-Recursion Desired : 1

|-Truncated Message : 0

|-Authoritative Answer : 0

|-Purpose of message : 0

|-Query/Response Flag : 1

|-Response code : 5

|-Checking Disabled : 0

|-Authenticated data : 0

|-Recursion available : 1

|-Number of question entries : 256

|-Number of answer entries : 0

|-Number of authority entries: 0

|-Number of resource entries : 0

UDP Header

|-Source Port : 53

|-Destination Port : 25561

|-UDP Length : 43

|-UDP Checksum : 65342

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 63 Bytes(Size of Packet)

|-Identification : 14193

|-TTL : 64

|-Protocol : 17

|-Checksum : 1083

Ethernet Header:

-->Destination Address : 00-00-00-00-00-00

|-Source Address : 00-00-00-00-00-00

|-Protocol : 8

Packet number 11

Packet type: DNS

DNS message

DNS Header:

|-Identification Number : 24238

|-Recursion Desired : 1

|-Truncated Message : 0

|-Authoritative Answer : 0

|-Purpose of message : 0

|-Query/Response Flag : 1

|-Response code : 5

|-Checking Disabled : 0

|-Authenticated data : 0

|-Recursion available : 1

|-Number of question entries : 256

|-Number of answer entries : 0

|-Number of authority entries: 0

|-Number of resource entries : 0

UDP Header

|-Source Port : 53

|-Destination Port : 25561

|-UDP Length : 43

|-UDP Checksum : 65342

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 63 Bytes(Size of Packet)

|-Identification : 14193

|-TTL : 64

|-Protocol : 17

|-Checksum : 1083

Ethernet Header:

-->Destination Address : 00-00-00-00-00-00

|-Source Address : 00-00-00-00-00-00

|-Protocol : 8

Packet number 12

Packet type: DNS

DNS message

DNS Header:

|-Identification Number : 20058

|-Recursion Desired : 1

|-Truncated Message : 0

|-Authoritative Answer : 0

|-Purpose of message : 0

|-Query/Response Flag : 1

|-Response code : 5

|-Checking Disabled : 0

|-Authenticated data : 0

|-Recursion available : 1

|-Number of question entries : 256

|-Number of answer entries : 0

|-Number of authority entries: 0

|-Number of resource entries : 0

UDP Header

|-Source Port : 53

|-Destination Port : 46146

|-UDP Length : 43

|-UDP Checksum : 38243

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 63 Bytes(Size of Packet)

|-Identification : 13895

|-TTL : 64

|-Protocol : 17

|-Checksum : 61346

Ethernet Header:

-->Destination Address : 48-BF-6B-DF-21-D8

|-Source Address : 30-E3-7A-10-DD-D5

|-Protocol : 8

Packet number 13

Packet type: HTTP

HTTP message

.............3.)........

TCP Header:

|-Source Port : 51173

|-Destination Port : 80

|-Sequence Number : 2836641336

|-Acknowledge Number : 0

|-Header Length : 11 DWORDS or 44 BYTES

|-Urgent Flag : 0

|-Acknowledgement Flag : 0

|-Push Flag : 0

|-Reset Flag : 0

|-Synchronise Flag : 1

|-Finish Flag : 0

|-Window : 65535

|-Checksum : 44408

|-Urgent Pointer : 0

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 64 Bytes(Size of Packet)

|-Identification : 62322

|-TTL : 64

|-Protocol : 6

|-Checksum : 43167

Ethernet Header:

-->Destination Address : 30-E3-7A-10-DD-D5

|-Source Address : 48-BF-6B-DF-21-D8

|-Protocol : 8

Packet number 14

Packet type: TCP

TCP Header:

|-Source Port : 51168

|-Destination Port : 443

|-Sequence Number : 3910365137

|-Acknowledge Number : 0

|-Header Length : 11 DWORDS or 44 BYTES

|-Urgent Flag : 0

|-Acknowledgement Flag : 0

|-Push Flag : 0

|-Reset Flag : 0

|-Synchronise Flag : 1

|-Finish Flag : 0

|-Window : 65535

|-Checksum : 45689

|-Urgent Pointer : 0

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 64 Bytes(Size of Packet)

|-Identification : 38687

|-TTL : 64

|-Protocol : 6

|-Checksum : 1267

Ethernet Header:

-->Destination Address : 30-E3-7A-10-DD-D5

|-Source Address : 48-BF-6B-DF-21-D8

|-Protocol : 8

Packet number 15

Packet type: HTTP

HTTP message

.............3..........

TCP Header:

|-Source Port : 51173

|-Destination Port : 80

|-Sequence Number : 2836641336

|-Acknowledge Number : 0

|-Header Length : 11 DWORDS or 44 BYTES

|-Urgent Flag : 0

|-Acknowledgement Flag : 0

|-Push Flag : 0

|-Reset Flag : 0

|-Synchronise Flag : 1

|-Finish Flag : 0

|-Window : 65535

|-Checksum : 43408

|-Urgent Pointer : 0

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 64 Bytes(Size of Packet)

|-Identification : 17442

|-TTL : 64

|-Protocol : 6

|-Checksum : 22512

Ethernet Header:

-->Destination Address : 30-E3-7A-10-DD-D5

|-Source Address : 48-BF-6B-DF-21-D8

|-Protocol : 8

Packet number 16

Packet type: TCP

TCP Header:

|-Source Port : 51168

|-Destination Port : 443

|-Sequence Number : 3910365137

|-Acknowledge Number : 0

|-Header Length : 11 DWORDS or 44 BYTES

|-Urgent Flag : 0

|-Acknowledgement Flag : 0

|-Push Flag : 0

|-Reset Flag : 0

|-Synchronise Flag : 1

|-Finish Flag : 0

|-Window : 65535

|-Checksum : 44689

|-Urgent Pointer : 0

IP Header:

|-IP Version : 4

|-Type Of Service : 0

|-IP Total Length : 64 Bytes(Size of Packet)

|-Identification : 7059

|-TTL : 64

|-Protocol : 6

|-Checksum : 32895

Ethernet Header:

-->Destination Address : 30-E3-7A-10-DD-D5

|-Source Address : 48-BF-6B-DF-21-D8

|-Protocol : 8

1. Contribution Summary

Ajay

Application layer: DNS

Transport layer: UDP

Network layer: IPv4

Shyam

Application layer: HTTP

Transport layer: TCP

Network layer: IPv6

Common

Coding and ARP (data link layer protocol)

1. REFERENCES

* <https://www.tutorialandexample.com/scan-disk-scheduling-algorithm>
* <https://www.paessler.com/it-explained/packet-sniffing>
* <https://www.geeksforgeeks.org/what-is-packet-sniffing/>
* <https://www.netscout.com/what-is/sniffer>