

PROFESSIONAL TRAINING REPORT
at
Sathyabama Institute of Science and Technology
(Deemed to be University)

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Technology in Information Technology

By
NITHISH KUMAR C.M

REG. NO. 39120077



DEPARTMENT OF INFORMATION TECHNOLOGY SCHOOL OF
COMPUTING

SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600119, TAMILNADU

NOVEMBER 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC

(Established under Section 3 of UGC Act, 1956)

JEPPIAAR NAGAR, RAJIV GANDHI SALAI

CHENNAI- 600119

www.sathvabama.ac.in



DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of NITHISH KUMAR C.M (Reg. No: 39120077) who carried out the project entitled "Network Sniffing" under my supervision from June 2021 to November 2021.

Internal Guide

Name of the Guide

Head of the Department

Submitted for Viva voce Examination held

on _____

Internal Examiner

External Examiner

DECLARATION

I, **NITHISH KUMAR C.M** hereby declare that the project report entitled **Network Sniffing** done by me under the guidance of **Dr. Y.BEVISH JINILA** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering Degree in Computer Science and Engineering.

DATE:

PLACE:

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph.D, Dean, School of Computing, Dr. R. Subhashini, M.E., Ph.D. Head of the Department of Information Technology** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. Y.BEVISH JINILA M.E., Ph.D.**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.

TRAINING CERTIFICATE



CERTIFICATE OF COMPLETION

CSW-I-10-081121 is given to

NITHISH KUMAR C M

For completing the Cyber Security training that includes basics of Cyber Security, Pentesting, Networking, and WebApp.

Aaron V Sandeen

AARON SANDEEN

CEO - CSW

N. Vengatesh

VENGATESH NAGARAJAN

MENTOR

ABSTRACT

The main objective of this system shows how real time network connection behavior can be modeled as chromosomes and how the parameters in genetic algorithm can be defined in this respect.

An Intrusion Detection System is a system for detecting intrusions and reporting them accurately to the proper authority. Intrusion Detection Systems are usually specific to the operating system that they operate in and are an important tool in the overall implementation of an organization's information security policy, which reflects an organization's statement by defining the rules and practices to provide security.

This system is useful for a network administrator who needs to identify, diagnose, and solve network problems, a company manager who wants to monitor user activities on the network and ensure that the corporation's communications assets are safe, or a consultant who has to quickly solve network problems for clients.

TABLE OF CONTENTS

CHAPTER No.	TITLE	PAGE No
	ABSTRACT	
1.	INTRODUCTION	
	1.1Main purpose	8
	1.2Objectives	8
2.	AIM AND SCOPE OF THE PRESENT INVESTIGATION	
	2.1 Aim	9
	2.2 Scope	9
3.	EXPERIMENTAL OR MATERIALS AND METHODS, ALGORITHM USED	
	3.1 The project discussion	10
	3.2 Methodology	10
	3.3 Algorithm used	11
	3.4 Advantages with propsed system	11
4.	RESULTS AND DISCUSSION	
	4.1 Results	12
5.	SUMMARY AND CONCLUSIONS	
	5.1 Referances	13
	5.2 Screen shots	13

CHAPTER 1

INTRODUCTION

1.1 Main purpose :

The main objective of this system shows how real time network connection behavior can be modeled as chromosomes and how the parameters in genetic algorithm can be defined in this respect.

1.2 Objectives :

- This project aims at developing a Network Packet Sniffer.
- Network Packet Sniffer is a piece of software that monitors all network traffic.
- The sniffer captures each packet and eventually decodes and analyzes its content using wireshark.
- For network monitoring purposes it may also be desirable to monitor all data packets in a LAN and to mirror all packets passing through a shared bus.
- This system provides a Summary view that provides general information of the entire network or the selected node in the explorer.
- In Summary view we can get a quick view of the total traffic, real-time traffic, broadcast traffic, multicast traffic and so on.
- When we switch among the node from the explorer, corresponding traffic information will be provided.

CHAPTER 2

AIM AND SCOPE OF THE PRESENT INVESTIGATION

2.1 AIM :

The aim of this project shows how network connection information can be modeled as chromosomes.

2.2 SCOPE :

In recent years, Intrusion Detection System (IDS) has become one of the hottest research areas in Computer Security. It is an important detection technology and is used as a countermeasure to preserve data integrity and system availability during an intrusion.

An Intrusion Detection System is a system for detecting intrusions and reporting them accurately to the proper authority. Intrusion Detection Systems are usually specific to the operating system that they operate in and are an important tool in the overall implementation an organization's information security policy, which reflects an organization's statement by defining the rules and practices to provide security.

A methodology of applying genetic algorithm into network intrusion detection technique is unique as it considers both temporal and spatial information of network connections during the encoding of the problem; therefore, it should be more helpful for identification of network anomalous behaviors.

CHAPTER 3

EXPERIMENTAL OR MATERIALS AND METHODS, ALGORITHMS USED

3.1 THE PROJECT DISCUSSION :

This project aims at developing a Network Packet Sniffer. Network Packet Sniffer is a piece of software that monitors all network traffic. This is unlike standard network hosts that only receive traffic sent specifically to them. As data streams flow across the network, the sniffer captures each packet and eventually decodes and analyzes its content. For network monitoring purposes it may also be desirable to monitor all data packets in a LAN and to mirror all packets passing through a shared bus.

This project will be comprised of three modules namely the User Interface module, Statistics module and Packet Analysis module. User Interface module provides all the Graphical Interface components necessary for the user to interact with the System. The Analysis Module will analyze the incoming packets into a computer, identify them and passes the information into the Statistics module. Finally the statistics module does the necessary calculation based on the information and produce information that can be understood by the user.

This system is useful for a network administrator who needs to identify, diagnose, and solve network problems, a company manager who wants to monitor user activities on the network and ensure that the corporation's communications assets are safe, or a consultant who has to quickly solve network problems for clients.

3.2 METHODOLOGY :

NETWORK PACKET SNIFFER is a desktop application which facilitates online monitoring of packets which are traveling over the network..

NETWORK PACKET SNIFFER I is a tool in which the packets source and destination addresses and other information is captured

The source and destination address protocols that are used by a connection are also monitored and detected

The graph or charts displayed on the valuation and need .

The monitored packets source and destination address is captured. This shows the traffic on a network.

3.3 ALGORITHM USED :

As a network administrator who needs to identify, diagnose, and solve network problems, a company manager who wants to monitor user activities on the network and ensure that the corporation's communications assets are safe, or a consultant who has to quickly solve network problems for clients. It is difficult to identify the problems if the network traffic is not tracked, as an administrator in general we depend on the analyzer provided by the operating system (if any) or the anti virus software that is installed to provide real-time network security. However, it is identified that these systems provide specific set of reports which may not be enough for an administrator to trace all the problems. To handle these types of issues we want to implement a specific network analyzer that can track all the incoming and outgoing calls.

3.4 Advantages with the proposed system :

Network Admin can monitor the packets any where through out the world.

- Traffic can be controlled
- System performance will be increased
- Immediate generation of reports on demand.
- Graphical data is available to analyze the network.

CHAPTER 4

RESULT AND DISCUSSION, PERFORMANCE ANALYSIS:

4.1 RESULT:

As a network analyzer (as a. packet sniffer), this system make it easy for us to monitor and analyze network traffic in its intuitive and information-rich tab views. With this system network traffic monitor feature, we can quickly identify network bottleneck and detect network abnormalities. This article is to discuss how we can monitor network traffic with this network traffic monitor feature.

This system provides a Summary view that provides general information of the entire network or the selected node in the explorer. In Summary view we can get a quick view of the total traffic, real-time traffic, broadcast traffic, multicast traffic and so on. When we switch among the node from the explorer, corresponding traffic information will be provided.

The Endpoints view; we can monitor network traffic information of each node, both local and remote. With its easy sorting feature we can easily find out which host is generating or has generated the largest traffic.

The Protocols view will list all protocols applied in network transmission. In Protocols view we can monitor network traffic by each protocol. By analyzing network traffic by protocol, we can understand what applications are using the network bandwidth, for example "http" protocol stands for website browsing, "pop3" stands for email, etc.

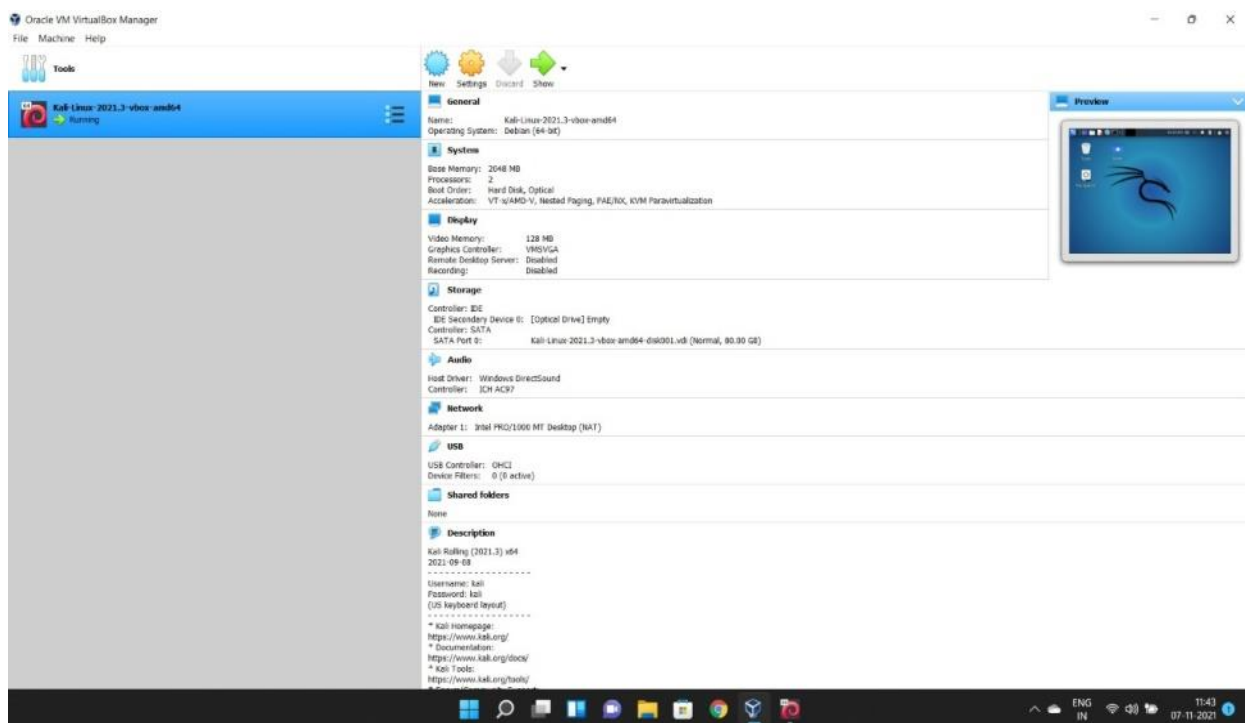
CHAPTER 5

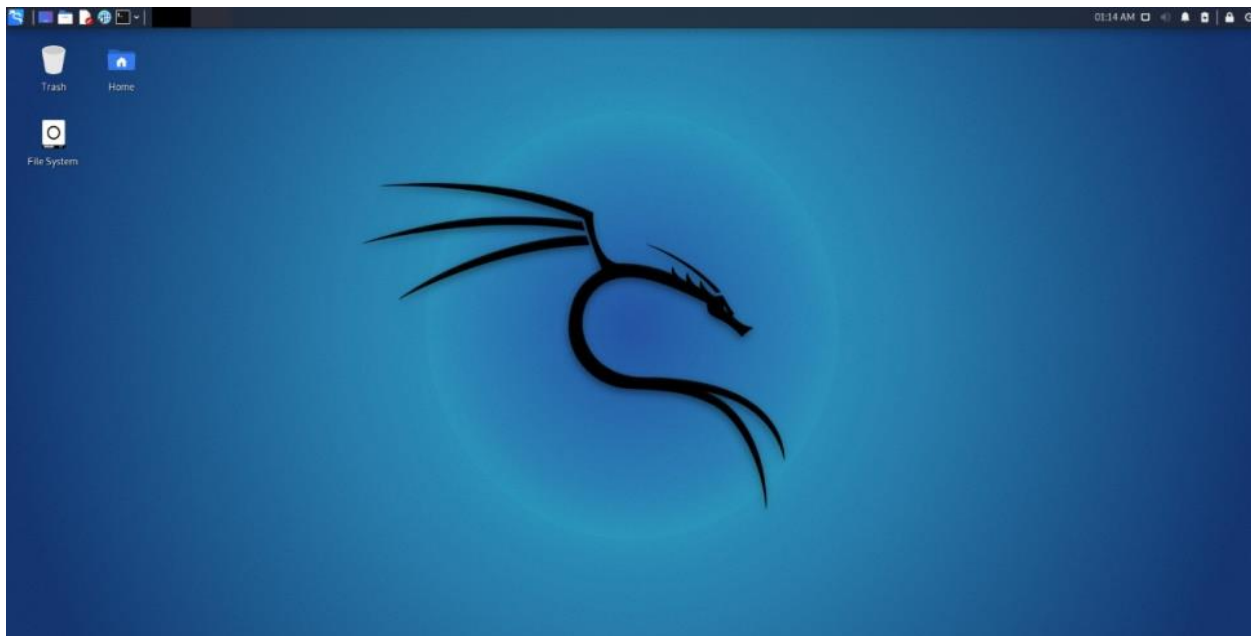
SUMMARY AND CONCLUSION:

5.1 REFERENCES :

- Kevin J. Connolly (2003). Law of Internet Security and Privacy. [Aspen Publishers](#). p. 131. [ISBN 978-0-7355-4273-0](#).
- ["Network Segment Definition"](#). [www.linfo.org](#). Retrieved January 14, 2016.
- ["Packet Sniffing"](#). [www.networksecurity.org](#). Retrieved October 12, 2019.

5.3 SCREEN SHOTS :





Web Scraper Testing Ground - Mozilla Firefox

testing-ground.webscraping.pro/login?mode=login

WEB SCRAPER TESTING GROUND

LOGIN

Often in order to reach the desired information you need to be logged in to the website. Most of today's websites use so-called form-based authentication which implies sending user credentials using POST method, authenticating it on the server and storing user's session in a cookie.

This simple test shows scraper's ability to:

1. Send user credentials via POST method
2. Receive, Keep and Return a session cookie
3. Process HTTP redirect (302)

How to test:

1. Enter **admin** and **12345** in the form below and press **Login**
2. If you see **WELCOME ;)** then the user credentials were sent, the cookie was passed and HTTP redirect was processed
3. If you see **ACCESS DENIED!** then either you entered wrong credentials or they were not sent to the server properly
4. If you see **THE SESSION COOKIE IS MISSING OR HAS A WRONG VALUE!** then the user credentials were properly sent but the session cookie was not properly stored or passed
5. If you see **REDIRECTING...** then the user credentials were properly sent but HTTP redirection was not processed
6. Click **GO BACK** to start again

Please, login:

User name: Password:

The image shows a Wireshark packet capture analysis of an HTTP POST request. The top pane displays a list of captured packets, with packet 63 selected. The middle pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol sections. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
63	15.425122373	10.0.2.15	185.221.154.249	HTTP	601	POST /login?mode=login HTTP/1.1 (application/x-www-form-urlencoded)
67	15.897620138	185.221.154.249	10.0.2.15	HTTP	2144	HTTP/1.1 200 OK (text/html)

Frame 63: 601 bytes on wire (4808 bits), 601 bytes captured (4808 bits) on interface eth0, id 0

- Interface id: 0 (eth0)
- Encapsulation type: Ethernet (1)
 - Arrival Time: Nov 7, 2021 05:39:59.102917727 EST
 - [Time shift for this packet: 0.000000000 seconds]
 - Epoch Time: 1636261599.102917727 seconds
 - [Time delta from previous captured frame: 0.000021317 seconds]
 - [Time delta from previous displayed frame: 0.000000000 seconds]
 - [Time since reference or first frame: 15.425122373 seconds]
- Frame Number: 63
- Frame Length: 601 bytes (4808 bits)
- Capture Length: 601 bytes (4808 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: ethiethertype:ip:tcp:http:urlencoded-form]
- [Coloring Rule Name: HTTP]
- [Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: PcsCompu43:73:bc (08:00:27:43:73:bc), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

- Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
- Source: PcsCompu43:73:bc (08:00:27:43:73:bc)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 185.221.154.249

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 547

Hypertext Transfer Protocol

Packets: 95 - Displayed: 2 (2.1%) - Dropped: 0 (0.0%) Profile: Default

The image shows a Wireshark packet capture analysis of an HTTP POST request, focusing on the TCP segment details. The top pane displays a list of captured packets, with packet 63 selected. The middle pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol sections. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
63	15.425122373	10.0.2.15	185.221.154.249	HTTP	601	POST /login?mode=login HTTP/1.1 (application/x-www-form-urlencoded)
67	15.897620138	185.221.154.249	10.0.2.15	HTTP	2144	HTTP/1.1 200 OK (text/html)

Type: IPv4 (0x0800)

- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 185.221.154.249
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 507
- Identification: 0x2339 (9017)
- Flags: 0x40, Don't Fragment
- 0... = Reserved bit: Not set
- .1. = Don't fragment: Set
- ..0. = More fragments: Not set
- Fragment Offset: 0
- Time to Live: 64
- Protocol: TCP (6)
- Header Checksum: 0xb40e [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.0.2.15
- Destination Address: 185.221.154.249

Transmission Control Protocol, Src Port: 52138, Dst Port: 80, Seq: 1, Ack: 1, Len: 547

- Source Port: 52138
- Destination Port: 80
- [Stream Index: 0]
- [TCP Segment Len: 547]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 1534236211

Hypertext Transfer Protocol

Packets: 95 - Displayed: 2 (2.1%) - Dropped: 0 (0.0%) Profile: Default

