MINOR-1 PROJECT

SYNOPSIS REPORT

For

NETWORK PACKET SNIFFER

Submitted By

Specialization	SAP ID	Name
B.Tech-CSE (CSF HONS)	500084995	Divyansh Kumar
B.Tech-CSE(CSF NON-HONS)	500084412	Mitali Chaudhary
B.Tech-CSE(CSF NON-HONS)	500082568	Priyal Khurana

Department of Systemics

School Of Computer Science

UNIVERSITY OF PETROLEUM & ENERGY STUDIES,

DEHRADUN- 248007. Uttarakhand

Dr. Aakashdeep Bhardwaj
Project Guide

Dr. Neelu Jyothi Ahuja
Cluster Head

School of Computer Science
University of Petroleum & Energy Studies, Dehradun

SYNOPSIS REPORT

1. Project Title

Network Packet Sniffer- Tool to sniff incoming and outgoing data packets

2. Abstract

In recent years, the Intrusion Detection System (IDS) is an important detection technology and is used as a countermeasure to preserve data integrity and system availability from any malicious act.

An Intrusion Detection System or packet sniffer is a system for detecting intrusions and reporting them accurately to the administrator. 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 to provide security and maintain integrity.

The sniffed data and other information can be utilized for future studies on the events that took place or if any malicious activity is taking place or not.

3. Introduction

Network Packet Sniffer is a piece of software that monitors all incoming and outgoing 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 system is thus very useful to the users and a network administrator in particular who is generally responsible for monitoring actions on a network.

This system is a network analyzer (also known as protocol analyzer & packet sniffer), it performs real-time packet capturing, 24x7 network monitoring, advanced protocol analyzing, in-depth packet decoding and automatic expert diagnosing. It allows you to get a clear view of the complex network and conduct packet-level analysis.

4. Literature Review

The authors of [1] developed Traffic analysis using the internet is an activity to record data from user activities in using the Internet. This study aims to obtain data about the results of traffic in a graphical form so that it can find out the number of users who access the internet and uses bandwidth. Researchers can filter data packets from the http protocol application. Since, user activity is more dominant in finding and downloading sites on the Internet.

The authors in [2] introduce redundant sniffer deployment to combat against the unreliable channel conditions. This can be formulated as a non-linear integer program with the aim of maximizing the number of captured data packets. We propose both centralized and distributed algorithms to determine an optimal strategy. For unknown user behaviours.

The authors in [3] proposed technique is a good tool to study the delay and packet loss.

5. Problem Statement

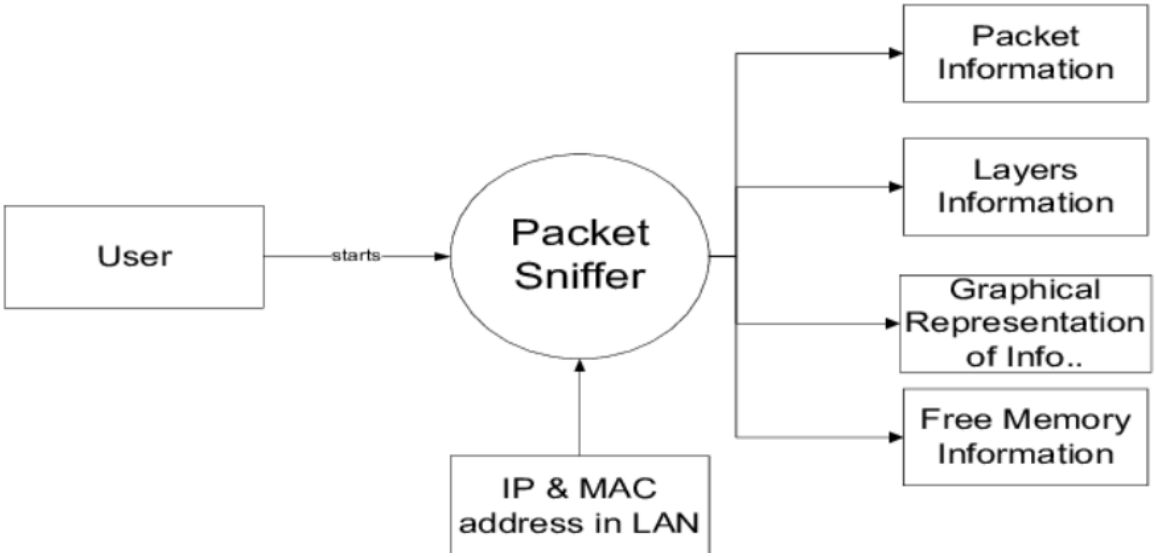
We have too much outgoing and incoming data while we are on the network and if we study these sniffed data packets we can get to know where all we are sending and what kind of data is being received by us, If use it for legitimate purposes we can detect if any malicious act is happening in our system. The aim is to collect this enormous amount of data packets generated to form a crisp report for the administrator to run a check on system.

6. Objectives

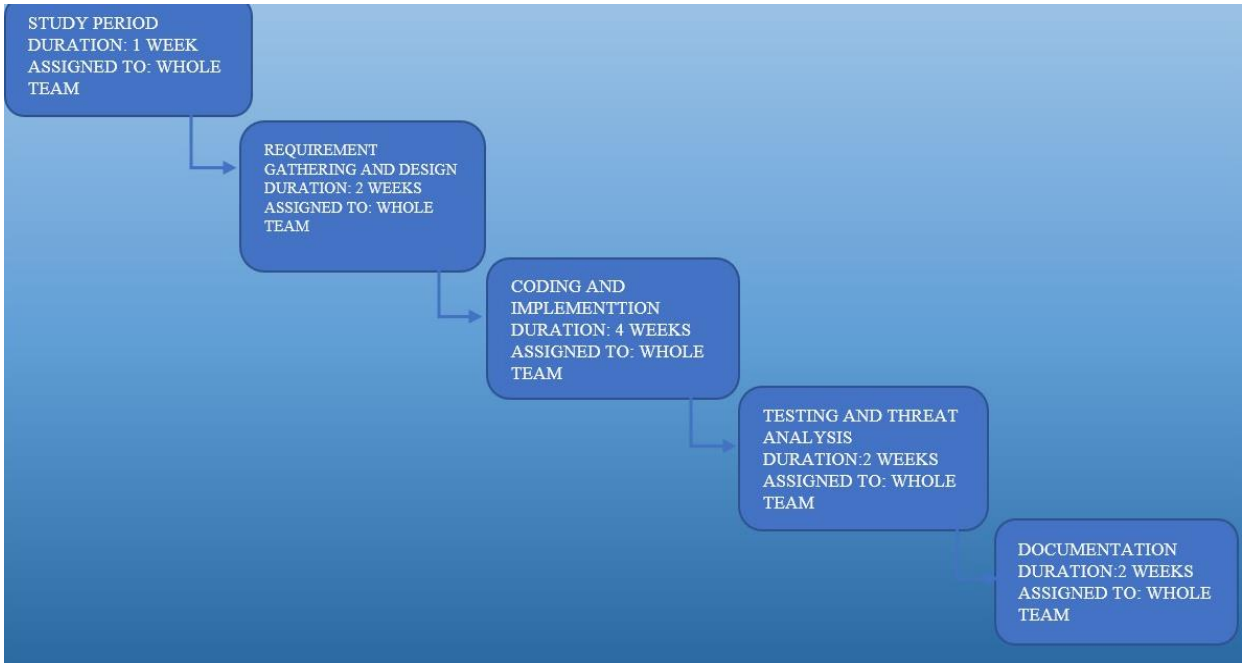
- To capture all the incoming and outgoing data
- To increase feasibility of use to work in IT firms
- To perform real packet capturing
- To perform 24*7 network and security monitoring
- To create a new set of rules during run time

7. Methodology

Basic methodology of packet sniffer:



8. PERT Chart



9. References

[1] A. Siswanto, A. Syukur, E. A. Kadir and Suratin, "Network Traffic Monitoring and Analysis Using Packet Sniffer," *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2019, pp. 1-4, doi: 10.1109/COMMNET.2019.8742369

[2] J. Xu, S. Gong, Y. Zou, W. Liu, K. Zeng and D. Niyato, "Redundant Sniffer Deployment for Multi-Channel Wireless Network Forensics With Unreliable Conditions," in *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 1, pp. 394-407, March 2020, doi: 10.1109/TCCN.2019.2937487.

[3] X. Guo, T. Gao, C. Dong, K. Cao, Y. Nan and F. Yu, "A Real-time Network Monitoring Technique for Wireless Sensor Networks," *2022 IEEE 12th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, 2022, pp. 32-36, doi: 10.1109/ICEIEC54567.2022.9835059

[4] Network Analysis using Wireshark 2 Cookbook: Practical recipes to analyze and secure your network [Online]. Available: https://www.pdfdrive.com/network-analysis-using-wireshark-2-cookbook-practical-recipes-to-analyze-and-secure-your-network-using-wireshark-2-2nd-edition-e184639568.html

[5] Wireshark & ethereal network protocol Analyzer Tool Kit. [Online]. Available: https://www.pdfdrive.com/wireshark-ethereal-network-protocol-analyzer-toolkit-e158830603.html

10. GitHub Link

https://github.com/priyalkhurana/MinorProject1