**Software Requirements Specification**

For

Network Packet Sniffer

15th September, 2022

Prepared by

|  |  |  |
| --- | --- | --- |
| **Specialization** | **SAP ID** | **Name** |
| CSF(HONS) | 500084995 | Divyansh Kumar |
| CSF(NON-HONS) | 500084412 | Mitali Chaudhary |
| CSF(NON-HONS) | 500082568 | Priyal Khurana |



Department of Systemics

School Of Computer Science

UNIVERSITY OF PETROLEUM & ENERGY STUDIES,

DEHRADUN- 248007. Uttarakhand

Table of Contents

|  |  |  |
| --- | --- | --- |
| **Topic** | | **Page No** |
| Table of Content | |  |
| Revision History | |  |
| 1 | Introduction | 4 |
|  | 1.1 Purpose of the Project | 4-5 |
|  | 1.2 Target Beneficiary | 5 |
|  | 1.3 Project Scope | 5 |
|  | 1.4 References | 5-6 |
| 2 | Project Description | 6-7 |
|  | 2.1 System Envisioned | 6 |
|  | 2.2 SWOT Analysis | 6-7 |
|  | 2.3 Project Features | 7 |
|  | 2.4 Design and Implementation Constraints | 7 |
|  | 2.5 Design diagrams | 7 |
|  |  |  |
| 3 | System Requirements | 8 |
|  | 3.1 User Interface | 8 |
|  | 3.2 Modules Used | 8 |
|  | 3.3 Hardware Specifications | 8 |
|  | 3.4 Software Specifications | 8 |
|  |  |  |
| 4 | Non-functional Requirements | 9 |
|  | 4.1 Security requirements | 9 |
|  | 4.2 Software Quality Attributes | 9 |
|  |  |  |
| Appendix A: Glossary | | 10 |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Change** | **Reason for Changes** | **Mentor Signature** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. INTRODUCTION

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.

A methodology of applying a genetic algorithm to 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 the identification of network anomalous behaviours.

1.1 Purpose of the Project

This project aims at developing a Network Packet Sniffer. 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 project will be comprised of three modules namely the User Interface module, Statistics module, and Packet Analysis module. The 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 data 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 produces information that can be understood by the administrator.

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.

This provides an administrator with a full set of reports such as Summary view, Endpoints view, and Protocols view.

1.2 Target Beneficiary

The proposed packet sniffer software makes it easy to identify, diagnose, and solve network problems for IT individuals. It 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. With the software’s information-rich and intuitive tab views, it can track all incoming and outgoing calls over the network.

1.3 Project Scope

For the feasibility of IT tech firms, the proposed network packet sniffer software will work as a network administrator can monitor the packets anywhere throughout the world. System performance will be enhanced and traffic will be controlled. Further, reports can be generated immediately and graphical data is readily available to analyze the network. The main objective of this project shows how network information can be modeled. The objective is to capture incoming and outgoing data. The objective of the system is to create a new set of rules during run time. So, the intruder cannot be able to attack the system with a virus.

1.4 References

[1] 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>

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

[3] freecodecamp YouTube course (JAVA)

2. PROJECT DESCRIPTION

2.1 SYSTEM ENVISIONED

**Existing System:**

In the existing system, network administration and monitoring are done by an admin. They are mainly assigned the task of identifying, diagnosing, and solving network problems, but with the amount of data flowing in the network, it is a very tedious task as network administration needs to put a lot of effort to identify traffic and report back the malicious ones. Also, the existing system is very time taking and uneconomical. There is no such thing as automatic network control because the network administrator has to be always present to monitor traffic over the network.

**Proposed System:**

As a network analyzer, the proposed packet sniffer software makes it easy to identify, diagnose, and solve network problems. With the software’s information-rich and intuitive tab views, it can track all incoming and outgoing calls over the network. can track all incoming and outgoing calls over the network. The key features of the packet sniffer application that can be listed are   real-time packet capturing, advanced protocol analyzing, comprehensive packet decoding, automatic diagnosing, and complex network analysis.

2.2 SWOT Analysis

Strength: The proposed project will capture all the incoming and outgoing data without the presence of an administrator by generating alerts if multiple logins or any malicious activity is done

Weakness: There is zero possibility of automatic network control and the presence of an administrator is compulsory, even if there are automatic diagnoses the reports still need to be analyzed by the administrator.

 Opportunities: It can have many more modules included in it that will boost its performance and will increase its feasibility of use to work in IT firms. The wide range of valid possibilities that this project can evolve into some bigger network trafficking project or maybe subsume under some higher application which helps in securing the networks. This project can also be used for educational purposes, say, to demonstrate working Wireshark and show the capture of real-time packets.

Threats: Our proposed project network packet sniffer can record any transmitted data and send it to command and control for further analysis. It’s then possible for hackers to attempt packet injection or man-in-the-middle attacks, along with compromising any data that was not encrypted or that was not captured before being sent.

2.3 Project Features

 The key **features** of the packet sniffer application are listed below:

·      It performs real-time packet capturing

·        24×7 network monitoring

·        Advanced protocol analyzing

·        Comprehensive packet decoding

·        Automatic expert diagnosing

·        Complex network analyzing

·        Conduct packet level analysis

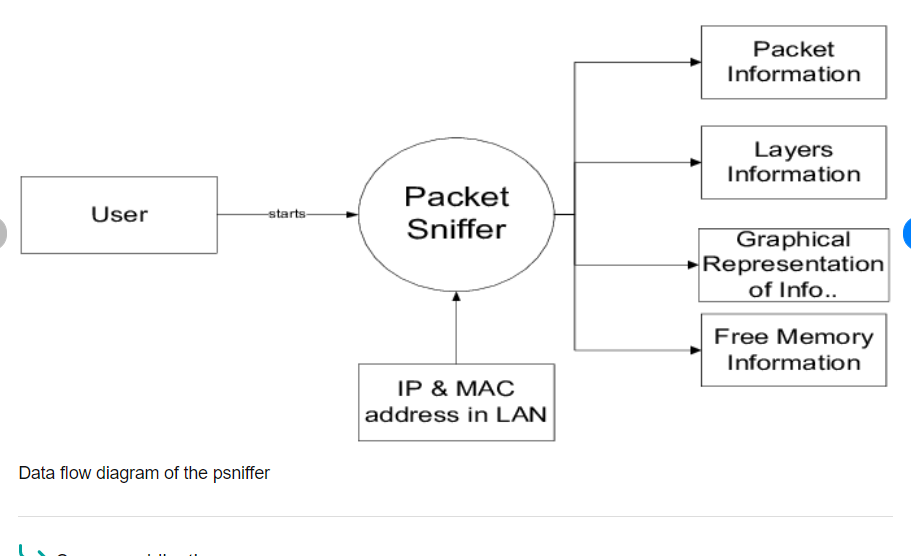
·        Solve network problems

·   Immediate generation of reports on demand.

2.4 Design and Implementation Constraints

* Networking issues
* Storage restrictions
* Complexity in Capturing all the incoming and outgoing data
* Managing all the data logs
* Not capturing all the incoming and outgoing data

 2.5 Design Diagram



3. SYSTEM REQUIREMENTS

 3.1 User Interface

Our project requires a user interface so that it is easier for the users to look at their respective data. We will use the basic java utility Library for basic figure charts. Also, we will use jpcap. For the design and implementation of the User Interface, we needed: Visual Studio Code.

 3.2 Modules Used:

The network packet sniffer is made up of 3 **modules**:

1.        **User Interface Module**: It provides all the Graphical Interfaces components required by the user to interact with the system.

2.        **Packet Analysis Module**: It analyzes all the incoming packets on the desktop, and upon proper identification and clarification, passes the data into the statistics module.

3.        **Statistics Module**: This module is responsible for all the necessary calculations based on the data, information, or content received from the packet analysis module. It then produces information that can be understood by the system user.

 3.3 Hardware Specifications:

·        Processor: Pentium IV with 800 MHZ Clock Speed

·        Hard Disk: 40 GB

·        RAM: 256 MB

3.4 Software Specifications:

·        Operating System: WINDOWS

·        Languages/Packages: Java, Jpcap

·        JDK version: JDK1.6.0

·        Communication Protocol: HTTP Protocol

4. NON-FUNCTIONAL REQUIREMENTS

4.1 Security requirements

The security measure we intend to take for our project is to make sure that the network packet sniffer is not available for use by hacker/s and is only put for the use of security by legitimate users.

4.2 Software Quality Attributes

Availability: Our project performs real-time packet capturing, and packets and modules are used for network trafficking. Packet sniffers are plugged directly into a network, which is useful if you want to analyze a specific part of a network rather than the whole thing which is useful for the tech in IT industry.

Usability:  Immediate generation of reports on demand of the sniffer on scene.

Efficiency: It performs real-time packet capturing to monitor the network ad gain valuable insights.

Integrity: The packets shown will be personal to the viewing authority

APPENDIX A: GLOSSARY