International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 7 ǁ 2021 ǁ PP. 77-82

Network Traffic Monitor and Analysis Using Packet Sniffer

Shivam Kumar[1], Suryansh Jigyasu[2], Vikas Singh[3]
[1] *Department of CSE, College of Engineering & Technology IILM AHL, Gr. Noida, U.P, India*
[2] *Department of CSE, College of Engineering & Technology IILM AHL, Gr. Noida, U.P, India*
[3]*Asst. Professor, Department of CSE, College of Engineering & Technology IILM AHL, Gr. Noida, U.P, India*

Abstract
Network traffic monitoring and analysis using packet sniffer is a software developed for personal home network, the purpose of this software is to monitor network traffics for all incoming and outgoing data this report primarily consist of four distinct chapters which start from the introduction to the final year project, on the second chapter the background of the product which is the different technology we have using this, the main purpose of this final year project to create a safe environment for our juniors and counter parts in this internet driven world.
Keywords – *Sniffing, packet, network, protocol, credentials*

Date of Submission: 21-06-2021 Date of acceptance: 06-07-2021

I. INTRODUCTION

Over the years the world has seen the next growth in the rate of internet penetration. According to the www, the global internet excess rate is 59.5% which continues to grow. With such growth, data sniffers are increasingly used to analyse and evaluate the network. Packet Sniffer is a device that can be a network or hardware monitoring system. Packet sniffing is a method used to track data packets transporting in a network. The administrator will detect the data packets and will monitor the packets and ensure secure network data transfer. The vulnerability of smoker's protection lies in the ability to monitor all incoming and outgoing messages, including passwords, usernames or something else sensitive. Network protocols use network packets that transmit data between network channel locations. Most network protocols such as HTTP, FTP that transmits data in plain text are suspected of attacks. Since then, the network packet contains confidential information of cyber criminals looking for confidential information in the packaging and may use packet information. Therefore, encryption technology is used when data is transmitted over networks.

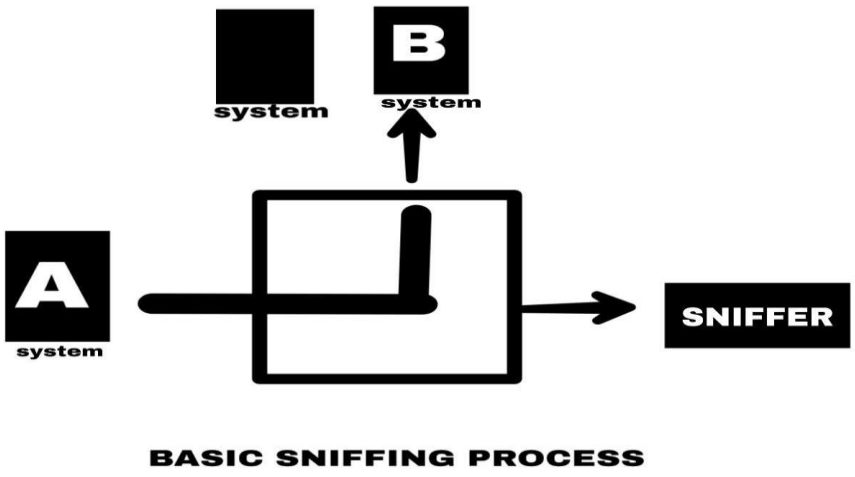


Figure 1: Basic sniffing process

1. Background and Literature Review

Packet Sniffer is a connected computer application that inactively accepts frames of all data connection layers that run through the system network adapter. This is also known as Ethernet Sniffer or Network Analyzer. A packet sniffer collects and stores continuous data transfer to other computers. This can legally be used to track and address network traffic by a network or device administrator. Using information collected

from the package, the administrator is able to detect incorrect packets and use them to identify issues and ensure secure transmission of network traffic. Sniffers protection focuses on all entities such as passwords and usernames and all data being transported in the network. This ensures a safer environment for the users and a detailed idea about the data.

1.1. Applications of Packet Sniffing Program

- Entering data throughout the network. Solve connectivity challenges (both machine and media transfer). Communication issues.
- Network release updates. Therefore, it is possible to find obstacles in the network or identify the part of the network where the data was not available.
- Finding access to a network.

2. Problem Definition

According to Google information the highest Internet penetration in India is in New Delhi at 68%. With this growing number, the burden of network monitoring has increased for network and security professionals. They rely heavily on traditional sniffer tools such as Wire shark, TCP dump. However, the data provided by such tools is very large and sometimes even network experts have a hard time filtering and getting the desired result. Also, these common tools in the industry require sound knowledge of network agreements that make them unsuitable for ordinary people and end users.

3. Proposed Solution

After all, the biggest problem is that today's teens have grown up with the internet, laptops and smart phones for the rest of their lives. Texting is a common way to communicate with teens. However, the majority of parents grew up when laptops couldn't do much and cell phones were often used to make calls without texting. Therefore, there are differences of opinion about how teens should use technology and how their parents have used technology over the years. Especially, because when most parents were young the technology itself was not very popular. There are many examples of cyber bullying and examples of youths committing suicide as a result of cyber bullying. There is evidence of child molesters using the internet to hunt teens. There is also evidence that teens are more likely to access suspicious webs and engage in sexting and sending sexually explicit photographs of themselves via the Internet and texting.

This definitely proves that most end users are not aware of the basic security concepts regarding SSL and encryption. Similarly, much of the information provided by a traditional sniffer package is virtually useless. To scan a basic cookie or password in network packets, traditional tools provide seven layers. It is difficult to filter when collectors are working long hours to find the secret price values. Therefore, a packet sniffer for sniffing out personal information can be a useful tool for network and security professionals can be both problem solving and sniffing out the network we know our teens or teens.

4. Aim and Objectives

The main purpose of this paper is to improve the sniffing private certifications; unlike a traditional tool that provides a lot of data and spends a lot of time filtering out the required results.

In order to complete our aim we will follow the following objectives are:

- In-depth research on network protocols such as TCP, UDP, and ICMP etc. on sniffer development.
- Extensive research on data sniffing from various sources such as IEEE, SANS, the research portal for reading relevant journals and research papers.
- A practical approach will be taken to incorporate conceptual evidence and real-time lessons as part of the report.
- Significant assessments of advantages, disadvantages and restrictions on sniffing packages will be conducted.

5. Case Study

This definitely proves that most end users are not aware of the basic security concepts regarding *SSL* and encryption. Similarly, much of the information provided by a traditional sniffer package is virtually useless. To scan a basic cookie or password in network packets, traditional tools provide seven layers. It is difficult to filter when collectors are working long hours to find the secret price values. Therefore, a packet sniffer for sniffing out personal information can be a useful tool for network and security professionals can be both problem solving and sniffing out the network we know our teens or teens.

5.1. Analysis of Case Study

Problem on IP phone solved with network shooting problem. Packet Sniffers were used during the trouble shooting phase. While the RTCP problem solving packages were taken and the problem was discovered. Problem identification and extraction available for VOIP calls is made easier by the Packet Sniffing technique. The Sniff Pack can be used in more complex situations like intelligence.

5.2. Open Systems Interconnection Model (OSI Model)

The OSI model thinking strategy describes how data and information flow across the internet. It consists of seven sub-layers that control contracts with network devices. The model works from the top as an application framework and ends up in the body layer. Various protocols can be web protocols such as HTTP, FTP or network protocols such as ARP operating according to the OSI Model policy. The OSI model was originally designed to provide device manufacturers with a set of communication design definitions. The OSI model describes a building framework that logically separates the functions required to facilitate system communication.

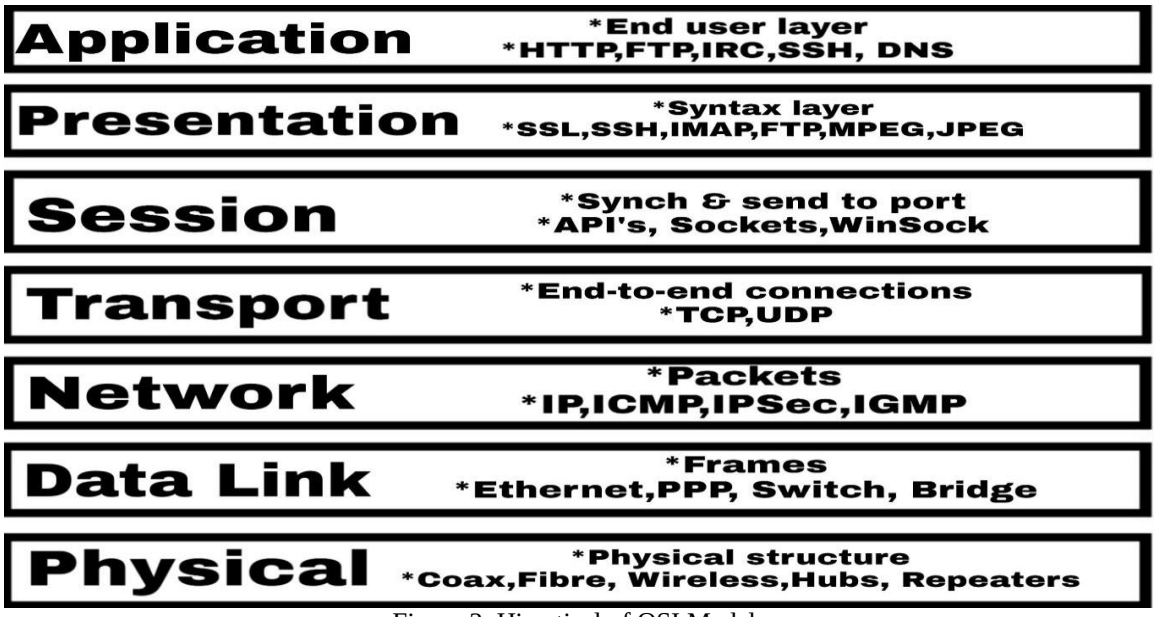


Figure 2: Hieratical of OSI Model

The basic functions of OSI layers are as follows:

7. Application: Application background enables a user - a person or software - to communicate with an application or network whenever a user chooses to read messages, transfer files or perform other network-related tasks.

6. Presentation: The presentation layer translates or creates application layer data based on the semantics or syntax of the receiving system. This layer also handles encryption and decryption required by the application layer.

5. Session: This layer determines how long the system will wait for another application to respond.

4. Transport: The transport layer is responsible for transferring data to the network and provides error detection methods and data flow controls. It determines how much data should be sent, where it is sent and at what rate.

3. Network: The function of this network is to move data to other networks. Network layers protocols achieve this by entering the data with the correct network details, selecting the correct network paths and sending the integrated data at the top of the stack to the transport layer.

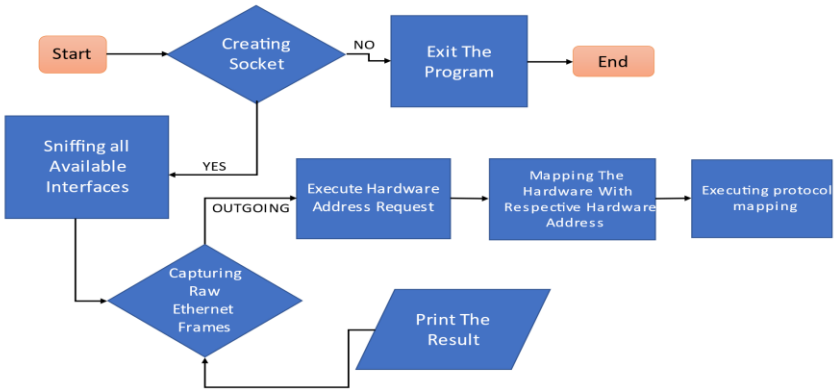
2. Data Link: This layer manages to move data in and out of the physical link to the network. This layer handles problems that occur due to minor transmission errors.

1. Physical: The layer transmits information using electricity, machinery or a process of integration. This layer is responsible for sending computer fragments from one device to another network.

5.3. Capture Network Packages with Java

jpcap is a collection of Java classes that provide interface and application to download a network packet. Follow-up library and visual tool network traffic is included.jpcap hides low data packet capture details by releases many types of network packets and protocols in Java studies. Internally, jpcap uses binding to the libpcap system library via JNI (Java Native Interface). jpcap uses libpcap, a widely shared library of downloads

packets at user level. libpcap must be installed on your system respectively to use jpcap.jpcap has a small shared library that wraps libpcap and a collection of Java classes. The shared library section provides the event hooks, connections and data conversion between Java VM running an libpcap. The 'capture' package contains a basic scanning program. The 'net' package contains the output of several types of network packets and agreements. The 'simulator' package contains a network simulator. Jpcap is licensed under the Mozilla public license.



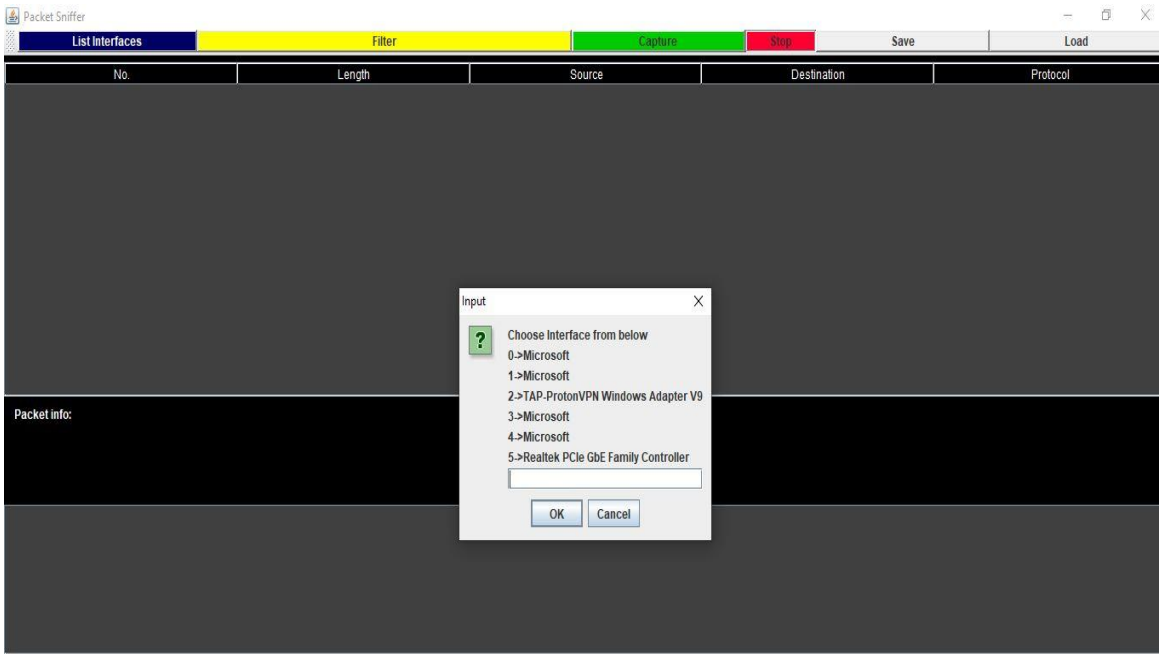
FlowChart (capturing incoming packets only)

5.4. Working of Application Layer

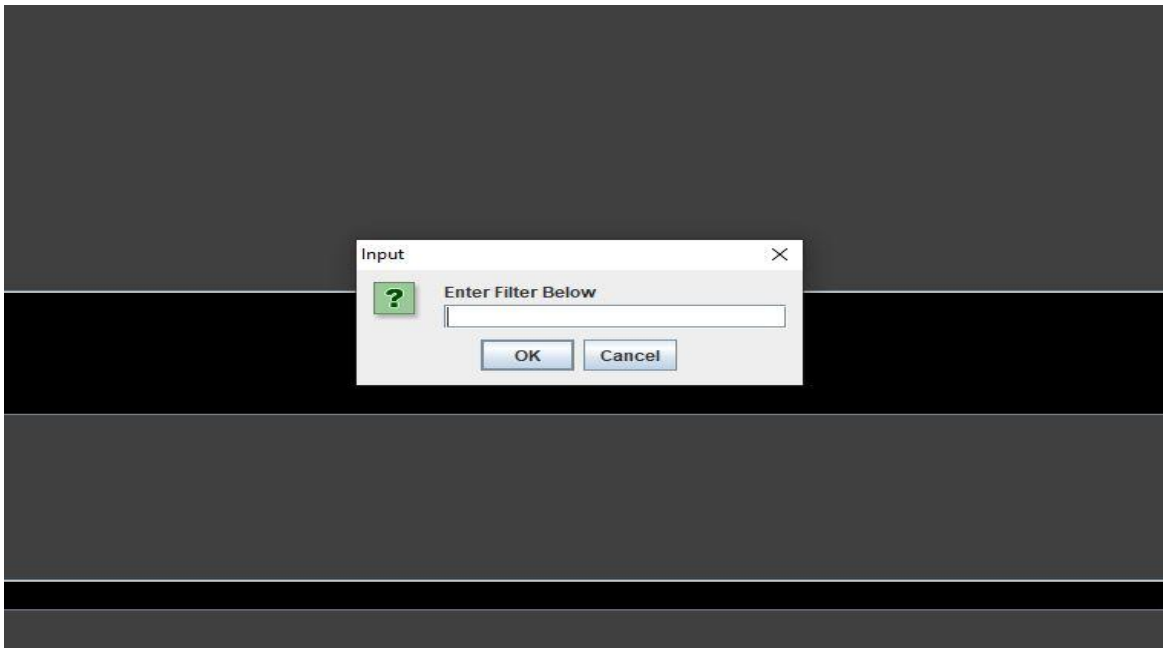
In this section the practical demonstration of sniffer program is performed. It will basically capture live packets. It can make choice between all interfaces present in your system. It will also filter packets. You will be able to see the packets of your choice.

Phase 1:

In this phase the sniffer program will choose the interface.



Phase 2:
We will apply filter of our choice, for eg. If we want to see only UDP packets, we will apply UDP filter.



Phase 3:
In this phase, the performance and working of sniffer program is demonstrated. Since the secret credentials are entered into the interface, we will tap on capture.it will start capturing the data.

5.5 Prevention against Packet Sniffing
Package Sniffing a serious problem and encryption stand with us in this regard. The prevention methods are:

- All confidential and confidential information should only be transmitted through a secure channel. Using HTTPS, the encrypted HTTP standard, stops smelling packets from accessing data on the domains we use.

- Another effective way to protect yourself from packers sniffers is to access the tunnel via a private VPN network. A VPN encrypts the connection between your device and the location

5.6 Ethical Guidelines

Working in a large package management area is usually based on live recognition of real-time network traffic. The diversity of development seen in this sector is made even confirmed only when such real time is considered included. Privacy is permanent given the competitive level of importance especially in these days when the whole social media platform.

it has become an integral part of our daily lives, and most academic researchers are inclined to look at how you can get into their research to reduce privacy. This is usually the case accomplished by discarding various technical jargons and creating a vague and indistinct line.

they stand like this

. "It's my network, so I can do whatever I want."
. "Cord rules are guilty of academic research."
. "Sniffing packets is legal for filtering data after 48 bytes (or 96 or 128)."
. "Capturing content may be illegal, but non-video capture is fine."
. "We are not breaking the law because we did not disclose the details."

- "The network wiretapping laws have an exception for academic research."
- "Packet sniffing is legal so long as you filter out data after the 48th (or 96th or 128th) byte."
- "Capturing content may be illegal, but capturing non- content is fine."
- "We're not breaking the law because we've anonymized the data."

II. CONCLUSION AND FUTURE WORK

This is the main driving force for this project to provide a highly recommended tool that can be used by people just to monitor their home network of tasks included in the process. Many are unusual you do not have network monitoring technology with tools like wireshark and TCP dump. So yes a market niche or foundation of people found where they really want to know what's going on with their home network project called, "NETWORK TRAFFIC MONITORING AND ANALYSIS USING PACKET SNIFFER" will turn to it be very helpful and guided. Also, from recent research it turns out that this project is not only useful for network monitoring but can also be used effectively in the field of education too.

Potential future activities that can be undertaken in the project are based on test responses
and my critical assessment is listed as follows (See appendix for research results.):

1. Live View (e.g. without creating a script) resulting in an animated GUI that completely cuts user access to the backend completely cuts back user access.
2. Visual filtering provided in relation to domain names.
3. Notice of Access to Suspicious Websites.
4. Sorting function on the basis of each session.
5. Availability of the Windows App because it fits well in the market.

REFERENCES:

[1]. Miller, R. (2019). The OSI Model: An Overview. SANS Institute, Page(s):5-12
[2]. Nimisha P, R. G. (2014). Packet Sniffing: Network Wiretapping. IEEE International Advance Computing Conference.
[3]. Magers Daniel.(2002). Packet Sniffing: An Integral Part of Network Defense , SANS Institute.
[4]. Qadeer M.A., Zahid M., Iqbal A., Siddiqui M.R "Network Traffic Analysis and Intrusion Detection Using Packet Sniffer" ICCSN '10 Second International Conference, 2010, Page(s): 313 - 317
[5]. A. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov. 2007, Page(s):158 – 162
[6]. Nucci A & Papagianaaki, K (2009). Design, Measurement and Management of Large-Scale IP Network.
[7]. Protocol Layers and the OSI Model [2018] , Online Available at https://docs.oracle.com/cd/E19455-01/806-0916/ipov-7/index.html Accessed on [2019.04.28].