International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 260-266 www.ijaem.net ISSN: 2395-5252

Network Packet Sniffing and Monitoring

Prof. Manish Hadap, Chanchal Halwe, Sakshi Wase, Himani Joshi, Sanskruti Kumarley, Rama Patil, Saee Kakade

Department of Information Technology, YCCE, Nagpur, India
Department of Information Technology, YCCE, Nagpur, India
Department of Information Technology, YCCE, Nagpur, India
Department of Information Technology, YCCE, Nagpur, India
Department of Information Technology, YCCE, Nagpur, India
Department of Information Technology, YCCE, Nagpur, India
Department of Information Technology, YCCE, Nagpur, India

Date of Submission: 10-10-2024 Date of Acceptance: 20-10-2024

ABSTRACT-The daily increase in the number of users on the network is causing a surge in network traffic, highlighting the importance of monitoring both user activity and network traffic to ensure smooth network operations. Monitoring network activity is challenging due to the large volume of packets on the network. Packet sniffing is a technique used to observe various network activities and identify vulnerabilities, enabling network administrators to bolster network security. This process involves inspecting data transmitted by other users on the network and is applicable to both switched and non-switched networks. Packet sniffers can function as administrative tools or be misused for malicious intent, depending on the user's goals. Sniffing can reveal passwords used in network connections such as Telnet, login, and FTP, as well as examine and capture packets traversing the network without modifying them. It decodes captured packets, allowing network administrators to interpret, analyze, and extract valuable information from packet content.

Wireshark is an open-source network packet analyzer that can be employed to evaluate traffic, data packets, and their influence on network behavior. With its user-friendly graphical interface and support for numerous protocols, Wireshark is a versatile tool for network troubleshooting, security analysis, and protocol development. It also provides advanced features such as real-time packet capture, deep packet inspection, customizable filters, and precise network behavior analysis.

Keywords-network security, packet sniffer, Wireshark, network monitoring, sniffing, telnet, FTP, security analysis.

I. INTRODUCTION

Network traffic analysis involves examining data packets exchanged between devices within a network. Wireshark streamlines packet analysis by capturing and presenting network packets in a user-friendly format. Packet sniffing tools serve various purposes, including aiding network administrators in detecting weaknesses, threats, and vulnerabilities to enhance overall network security.

These tools are also utilized by network and security engineers for intrusion detection and penetration testing to identify network attacks during performance disruptions. Moreover, sniffers help in understanding different network applications that use protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), including their parameters, payload type, IP addresses, and Media Access Control (MAC) addresses.

Data transmission from one machine to another is facilitated using tcpdump on Open-Source Linux platforms like Ubuntu. By delving into each packet's contents, crucial details such as data origins and destinations, involved protocols, and timing of data exchanges can be revealed. Sniffing enables attackers to capture packets like Syslog, DNS, web, and email traffic. By analyzing these packets, they may uncover sensitive information such as usernames and passwords from protocols like TCP.

Wireshark assists in both live and retrospective network traffic monitoring, helping to identify anomalies, potential security risks, and performance degradation areas. This in-depth understanding of network communications provides administrators and security experts with the insights

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 260-266 www.ijaem.net ISSN: 2395-5252

needed to optimize and protect their network infrastructure, thus boosting overall network efficiency and security.

Packet sniffers log and display collected data according to parameters such as destination address, source address, target port number, and used protocols.

II. LITERATURE REVIEW

[1] The literature review for this study emphasizes the challenges of traditional firewall implementations, which are either software-based and lack high-speed data handling capabilities or hardware-based and face limitations in terms of cost and upgradability. The review notes that FPGA architecture emerges as a balanced solution due to its ability to offer low latency, high throughput, and ease of upgrade. Previous research has demonstrated FPGA's effectiveness in handling network traffic, and this study builds on that work by presenting an FPGA-based packet sniffer capable of analyzing Ethernet frames in real-time at data transfer rates of up to 10 Gbit/s.

[2] Prior research has highlighted the importance of network traffic analysis in maintaining network security and performance. The use of packet capture tools like Wireshark has been recognized as a crucial method for monitoring network activity and detecting anomalies. Studies have shown that Wireshark's capabilities, such as plotting flow graphs and IO graphs, provide valuable insights for investigating captured traffic. Additionally, the software's ability to analyze TCP headers and trace IP addresses, port numbers, and sequence numbers has been noted for its role in identifying suspicious or malicious behavior in real time.

[3] Packet sniffing is a technique that intercepts and monitors network traffic, allowing network administrators to capture and analyze packets for various purposes, both ethical and malicious. In an era of rapidly expanding networks and increasing traffic, packet sniffing plays a critical role in ensuring network efficiency and security. By leveraging sniffing tools, administrators can identify vulnerabilities, troubleshoot issues, and maintain smooth network operations. Packet sniffing also enables filtering based on different protocols like TCP, IP, and UDP for focused monitoring and analysis in a range of environments, including detecting cyber-attacks and assessing network health.

[4] This paper emphasizes the growing importance of network traffic analysis in keeping pace with evolving cyber threats to detect and counteract attacks. Tools such as Wireshark are essential for identifying indicators of compromise (IoCs) and supporting security professionals in incident response and network forensics. The paper highlights the role of packet analysis in understanding network patterns, uncovering malicious activities, and implementing network security protocols, while showcasing Wireshark's abilities to gather IoCs for effective threat detection and response.

[5] The paper underscores the essential role of traffic analysis in enhancing both network performance and security, noting its dual function as a key diagnostic tool and a potential vulnerability for attackers. Wireshark is presented as a robust and adaptable tool for traffic analysis, with applications including diagnosing performance issues, exploring integrated system problems, conducting network forensics, shaping policies through traffic analysis, performing penetration testing, and serving educational purposes. The thorough review highlights Wireshark's importance in network management, security, and academic settings.

[6] Research has demonstrated Wireshark's effectiveness in network forensics, enabling the identification of attack signatures and improving cybersecurity through detailed packet analysis. Despite its strengths, Wireshark has limitations in intrusion detection, highlighting the need for additional security measures. Flow sampling at Internet Exchange Points offers insights into industrial protocol usage but may lack real-time threat detection capabilities. Wireshark's use in forensic analysis allows for detailed examination of network attacks, but solely relying on it for website security classification may oversimplify vulnerability assessment.

[7] This paper offers an in-depth analysis of packet sniffers, discussing their functionality, development on the Linux platform, and application in intrusion detection. It examines techniques for identifying and managing these tools efficiently, particularly in analyzing network bottlenecks. By using existing tools such as Wireshark, tcpdump, and Snort, the creation of a custom packet sniffer can introduce new features not present in current solutions, utilizing libraries like libpcap for capturing packets.

[8] This paper examined three packet sniffer protocols: Wireshark, Ethereal, and TCP Dump, showcasing the results obtained from these tools. These packet sniffers play a vital role in research and the development of new applications in communication technology. They provide deep insights into network traffic, enabling the analysis and diagnosis of network issues. The paper highlights the importance of these tools for

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 260-266 www.ijaem.net ISSN: 2395-5252

understanding network behavior, troubleshooting problems, and enhancing network performance. Utilizing packet sniffers contributes to the ongoing advancement of communication technology and aids in the creation of innovative solutions.

[9] In recent years, digital interactions have become an integral part of daily life, offering unparalleled convenience and connectivity. However, as individuals engage in online activities such as shopping, communication, and financial transactions, they face the risk of unauthorized data interception, known as sniffing. This literature review explores the network transmission process, examining how data packets travel across networks, and the various types of sniffing that can compromise data privacy and security. It also delves into defense mechanisms designed to protect against sniffing and ensure safe, secure online experiences.

[10] The literature review contextualizes the study's focus on analyzing internet traffic at Telkom Vocational School by emphasizing the critical role of network analysis in optimizing bandwidth management. Highlighting the use of Wireshark for packet sniffing, it underscores its significance in capturing and filtering HTTP packet data, essential for understanding user behavior and network utilization. Previous research in network traffic analysis, particularly utilizing tools like Wireshark, establishes a foundation for the study's methodology and objectives. This review sets the stage for understanding how internet usage data can inform network design decisions and resource allocation strategies in educational settings.

III. METHODOLOGY

The research methodology involves a structured process to conduct a network packet sniffing analysis using various software tools and network configurations. The approach is outlined as follows:

A. Project Overview

The project methodology involved creating a virtual networking environment using VirtualBox and deploying an Ubuntu virtual machine with Wireshark for packet analysis. The experiment examined the security of data transmission on insecure and secure websites (including a localhost site and Udemy) by capturing and analyzing network traffic during login attempts, assessing whether sensitive information was transmitted in plaintext or encrypted form.

B. Network Setting Up the Environment

A virtual networking environment was established using VirtualBox, deploying an Ubuntu virtual machine as the network node for conducting packet sniffing experiments. Wireshark was installed on the Ubuntu VM to capture and analyze network traffic.

C. Designing the Experiment

The experiment aimed to assess data transmission security by examining login attempts on two websites: a localhost site for insecure transmission and Udemy for encrypted transmission.

D. File Packet Sniffing

Wireshark was used to capture network traffic on the Ubuntu virtual machine during login attempts on both insecure and secure websites, monitoring the security of data transmission.

E. Data Website Creation

An insecure localhost website was created to simulate an environment without encryption protocols, while a secure website similar to Udemy was designed with strong security measures.

F. Testing Packet Analysis

Captured packets were analyzed using Wireshark to determine whether sensitive information was transmitted in plaintext or encrypted form, evaluating the security measures in place on the websites.

IV. TECHNOLOGY

A. Wireshark

Wireshark is a popular open-source network protocol analyzer used for capturing and analyzing network traffic. It provides tools for live traffic monitoring, filtering, and protocol analysis, helping in the detection of anomalies and potential security threats. In this project, Wireshark is utilized to analyze the network packets captured during data transmission, providing insights into network behavior, traffic patterns, and potential security vulnerabilities.

B. Ubuntu

Ubuntu is a widely used open-source Linux distribution known for its ease of use and broad compatibility. It serves as the operating system for the project, hosting the necessary software tools and creating a stable environment for network monitoring and analysis. In this project, Ubuntu is used as the primary platform for running Wireshark and VirtualBox, providing a consistent and secure base for capturing and analyzing network traffic.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 260-266 www.ijaem.net ISSN: 2395-5252

C. Linux

Linux is a versatile open-source operating system that forms the backbone of many modern computing environments. It offers high performance, stability, and security features that make it suitable for network monitoring and analysis projects. In this project, the Linux environment supports packet sniffing tools like Wireshark, and it facilitates the execution of network tasks such as traffic capturing and analysis.

D. VirtualBox Machine

VirtualBox is a virtual machine software that allows the creation of virtualized network environments within a physical machine. It enables the simulation of different network scenarios and configurations without the need for physical hardware. In this project, VirtualBox is used to create virtual network topologies, simulate various network conditions, and capture data packets for analysis using Wireshark, thereby providing valuable insights into network performance and behavior.

V. IMPLEMENTATION

The implementation of a network packet sniffing and analysis process begins with setting up a peer-to-peer (P2P) network connection between devices. This direct communication link between connected peers is established without intermediaries, promoting efficient data transfer. To ensure stable connectivity, a crossover Ethernet cable is used to directly connect the devices in the network. This setup allows for seamless file sharing and resource transfers.

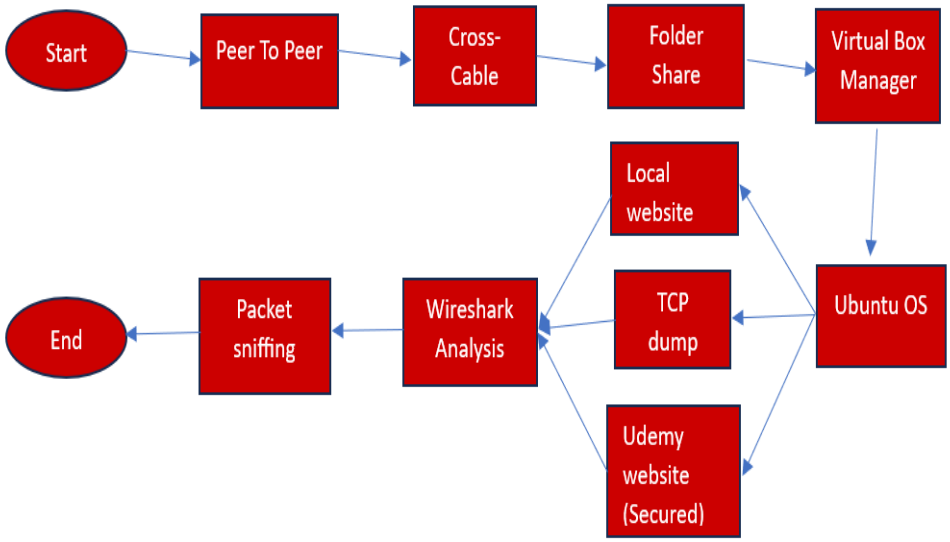
Once the network is established, file-sharing capabilities are set up across connected devices. Shared folders are created to facilitate smooth file transfers and resource sharing among peers. An Ubuntu PC is utilized as the central machine for network monitoring and analysis. This PC serves as a hub for capturing and analyzing network traffic.

Within the Ubuntu PC, VirtualBox is installed and configured to create virtualized network environments, simulating different network scenarios. Network traffic is captured and saved in a TCP dump file format using VirtualBox, recording real-time data packets as they traverse the network.

The TCP dump files are then imported into Wireshark for analysis. Wireshark, a powerful network packet analyzer, decodes captured packets and provides detailed information about network traffic, such as source and destination Ips, protocols, and packet sizes. Appropriate filters can be applied in Wireshark to focus on specific types of network packets or protocols of interest.

The implementation concludes after analyzing the captured data using Wireshark. Findings and insights from the analysis are compiled to generate recommendations for network optimization and security improvement. This process enables efficient network monitoring and troubleshooting, helping to maintain a secure and well-functioning network.

Flowchart:

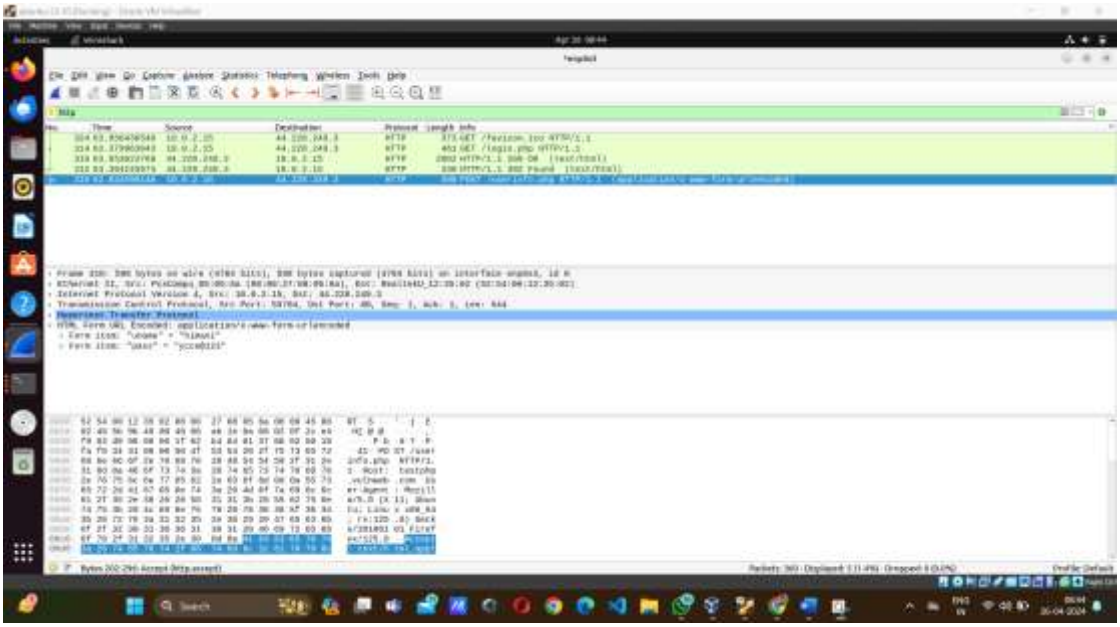


International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 260-266 www.ijaem.net ISSN: 2395-5252

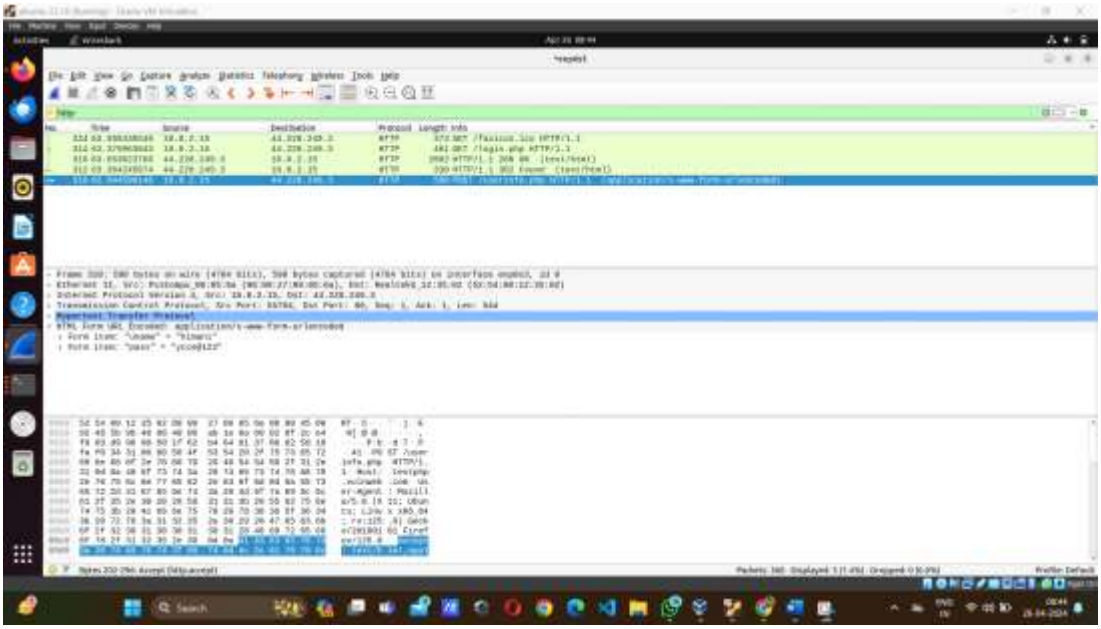
VI. RESULTS

A. Localhost Website Packet Sniffing

An unsecured localhost website was tested, revealing vulnerabilities in data transmission through packet sniffing using Wireshark. Wireshark, a network protocol analyzer, captured sensitive data such as usernames and passwords transmitted in plaintext over the network when a user logged in. This occurred because the website used HTTP without encryption, leaving the data open to interception and potential exploitation by malicious actors. This observation underscores the crucial need to adopt secure communication protocols like HTTPS to protect sensitive information during transmission. When login credentials (username and password) were entered on the localhost website, Wireshark recorded packets containing plaintext data.



The captured packets showed that usernames and passwords were sent over the network in plaintext, highlighting insecure data transmission practices.

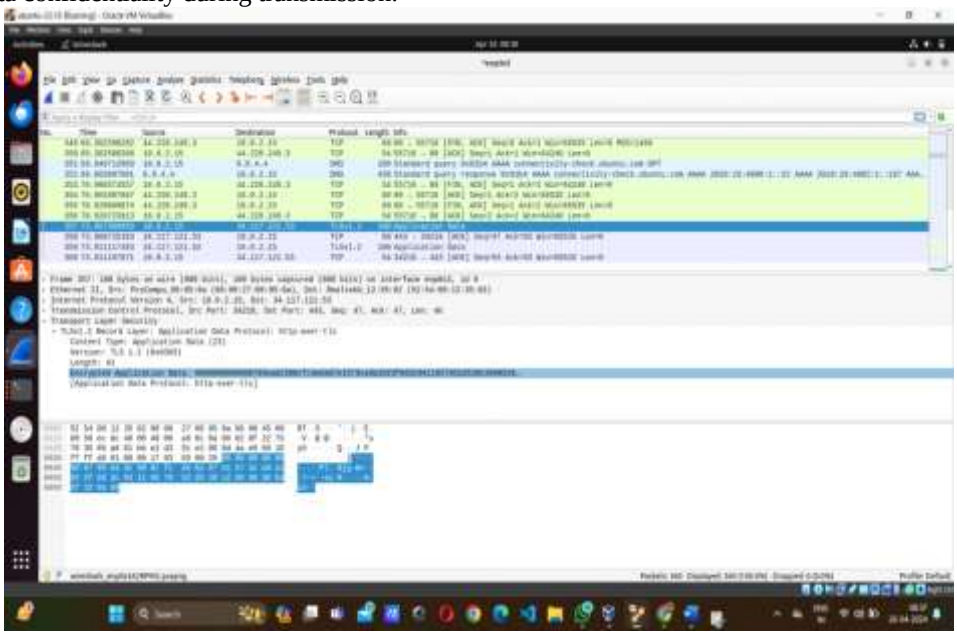


International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 260-266 www.ijaem.net ISSN: 2395-5252

B. Secure Website (Udemy) Packet Sniffing

Even though Udemy is a secure website, Wireshark intercepted packets containing sensitive data during packet sniffing. Fortunately, the password was encrypted, showcasing the website's robust security measures to protect user information. This implies the use of advanced encryption algorithms and secure communication protocols to safeguard user data during transmission. The intercepted data remains secure because it can't be decrypted without the public key. The packets captured by Wireshark contained an encrypted password, signifying secure data transmission.

Analysis of the intercepted packets demonstrated that the password was protected with advanced encryption, ensuring data confidentiality during transmission.



International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 260-266 www.ijaem.net ISSN: 2395-5252

VII. CONCLUSION

Network packet sniffing is a valuable practice for network administrators as it provides detailed insights into network traffic and performance. By capturing and analyzing packets using tools like Wireshark, network admins can monitor network activity in real-time, identify and resolve issues such as bottlenecks or interruptions, and optimize overall network efficiency. Packet sniffing enables proactive troubleshooting, allowing administrators to detect potential security threats and take timely actions. This process also aids in capacity planning and resource allocation, supporting network scalability and growth. Ultimately, packet sniffing is an essential component of effective network management, ensuring secure and well-performing networks.

REFERENCES

[1]. Marco Grossi, Fabrizio Alfonsi, Marco Prandini and Alessandro Gabrielli, A Highly Configurable Packet Sniffer Based on Field-Programmable Gate Arrays for Network Security Applications, MDPI Electronics, Volume 12, Issue 21, 2023.

[2]. Brij Mala, Sanskar Agrawal, Aditya Sharma, Rupinder Kaur, Exploring Wireshark for Network Traffic Analysis, IJFMR Volume 5, Issue 6, November-December 2023.

[3]. Dr. Paravathi C, Roshini D, Shwetha S Nayak, Packet Sniffing, International Journal of Engineering and Management Research Vol. 14 No. 1, February 2024.

[4]. Bindu Dodiya, Umesh Kumar Singh, Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise, International Journal of Computer Applications (0975 – 8887) Volume 183 – No. 53, February 2022.

[5]. Muhammed Alfawareh, A Deeper Look into Network Traffic Analysis using Wireshark, Academia, 2021.

[6]. Dr. B. Kalaiselvi, Aruna. K, Network Traffic Analysis Using Wireshark, International Journal of Research Publication and Reviews 4(12):1960-1965, December 2023.

[7]. Mohammed Abdul Qadeer, Arshad Iqbal, Mohammad Zahid, Misbahur Rahman Siddiqui, Network Traffic Analysis and Intrusion Detection using Packet Sniffer, Communication Software and Networks, International Conference on. 313-317. 10.1109/ICCSN.2010.104, Jan 2010.

[8]. Pooja Pandit, A Study of Packet Sniffer Tools, Mumbai University, September 2021.

[9]. Md Liakat Ali, Sadia Ismat, Kutub Thakur, Abu Kamruzzaman, Zijie Lue, Hasnain Nizam Thakur, Network Packet Sniffing and Defense, IEEE 13th Annual Computing and Communication Workshop and Conference, Las Vegas, NV, USA, 2023, pp. 0499-0503.

[10]. A. Bhandari, S. Gautam, T. K. Koirala, and M. R. Islam, Packet Sniffing and Network Traffic Analysis Using TCP—A New Approach. Advances in Electronics, Communication and Computing. Lecture Notes in Electrical Engineering, vol 443. Springer, Singapore, 2018.