Unveiling Cyber Threats: A Comprehensive Analysis of Wireshark as a Vital Cybersecurity Tool

K.Bala Chowdappa[1*], S. Zahoor Ul Huq[2], S.Shabana Begum[1] and K.Kedharnath Reddy[3]

[1]Assistant Professor, Department of CSE, G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India
[2]Professor,Department of CSE, G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India
[3]Research Scholar, Department of CSE, G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India
bala@gprec.ac.in

Abstract. Information technology is developing very quickly, which is good for an organization's chances of success in a variety of commercial domains.This paper provides an example of how to use Wireshark as a network sniffing tool. An experimental setup that illustrates the productiveness of dangerous packet detection in any network has demonstrated this. Experimentation on a live network that Wireshark is analyzing has allowed for testing. Conclusions have been open that unequivocally view off Wireshark's capacities and position it as top contender for further development into a reliable intrusion detection solution. This paper describes how Wireshark functions as a network protocol analyzer and emphasizes how flexible it is as an open source tool that lets developers incorporate potential intrusion detection device features.Currently, the most comprehensive Graphical User Interface (GUI) display may be found in network analyzer software called Wireshark.

Keywords: Wireshark, Data, Network, Sniffing, Packets

1 Introduction

The One of the tools used in network analysis is the Wireshark application, which is also known as a full network protocol analyzer. Network administrators frequently utilize these for software analysis, network problem solving, communication protocol development, and training. In addition to selecting and displaying the data in as much detail as it can, this programme can record any packages that pass. An intrusion detection system is some data logging that also has the ability to identify malicious entries in a network (IDS).

B. S. Babu et al. (eds.), *Proceedings of International Conference on Advanced Materials, Manufacturing and Sustainable Development (ICAMMSD-2024)*, Advances in Engineering Research 257,
https://doi.org/10.2991/978-94-6463-662-8_29

Additionally, an intrusion detection system (IDS) maintains a warehouse of known identity,mark and can detect instances of close matches between signatures and recent or ongoing behavior by comparing activity, traffic, or behavioral patterns it observes in the logs it monitors against those signatures. The IDS will detect sound triggers or notifications simultaneously. A way that communicates to a known virus is denoted as a signature. This paper develops a testing challenge and draws relevant conclusions regarding the capabilities of Wireshark as a good IDS from the experiment results.

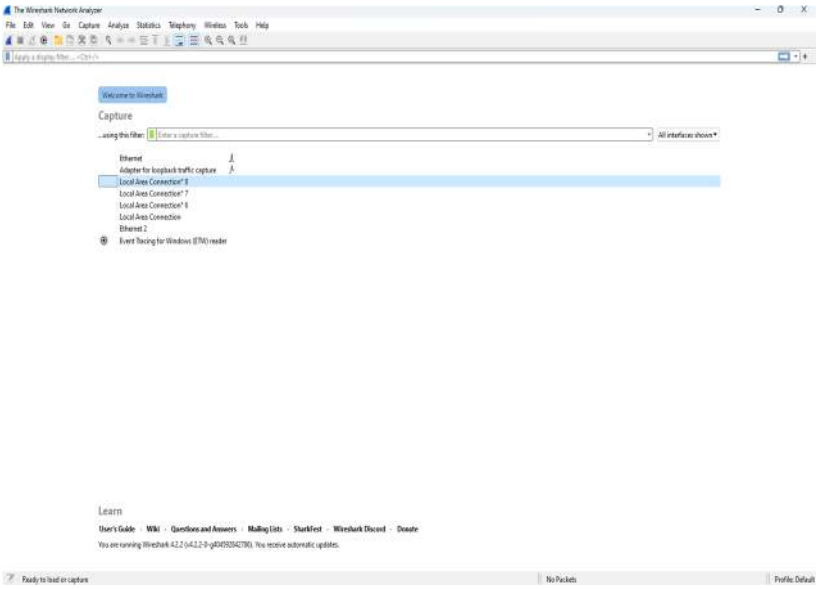

Fig 1. Interface of Wireshark.

2 About Wireshark

There are numerous primary Wireshark application functions.Strangely enough, though, this program's primary reputation comes from the fact that novice hackers frequently employ it for hacking endeavors.Wireshark isn't really made for hackers or hacking. Hacking is not the primary purpose of the Wireshark application.The primary purpose of the Wireshark application is to enable network administrators to monitor events on their network and ensure that no malicious activity is occurring there.

3 Wireshark Functions

1. Network administrators use the Wireshark tool primarily to analyze network performance. Wireshark can record information or data packets moving via the visible network. Any kind of data can be readily examined, mostly through the use of sniffing, which involves detecting critical data like passwords for other accounts.

2. Due to network loops, loopback networks can produce an abnormally high number of packets in a WireShark analysis; for instance, thousands of packets may appear out of nowhere in a matter of seconds.
3. Recognise unwelcome DHCPS servers. It turns out that there is an active DHCP server even if the network in the office is configured to be static. Wireshark will display the broadcast data from the dhcp server.
4. Additionally, WireShark is able to observe actions like sharing files among computers; the SMB2 protocol is used by the data package.

4 Best Features of Wireshark

1. Able to fully display network protocol data from data packets.
2. Data packages can be stored as files and then viewed again for additional examination at a later time.
3. Sniffing packets of network data.
4. Packets completely able to fully display network protocol data from data packets.
5. Data packages can be stored as files and then viewed again for additional examination at a later time.

Maintaining a system is not always easy, challenges must be met. There are various typical roadblocks that arise frequently when operating an accounting information system, including:

- Businesses require computer hardware and accounting software that ensure complete security and privacy of financial data.
- The new finance system and standardization are not yet ready to be implemented by human resources. Therefore, training and application take longer.
- Incomplete information and data generated about finances. Thus, the verification procedure is still ongoing. Even more time is required than should be the case.

5 Methods

In this study, the descriptive approach was used by gathering prior research on Wireshark Packet Capture. This paper attempts to illustrate how Wireshark Packet Capture is perceived from the standpoint of accounting information technology systems based on the literature review that is given. This study aims to explain to readers the nature of Wireshark Packet Capture from the standpoint of accounting information systems.

6 Results

As The advancement of technology has made it easier for information to move across all spheres of life, including business. It is thought that the information network can lower obstacles and boost commerce since it shortens and closes the gap between producers and customers. The usage of information networks has many advantages, but it also has drawbacks, such as the potential for data leakage and a lack of consistent benefits.

One tool that is employed in the accounting industry is information technology. This allows management to more easily oversee the system's operations and enable the accounting process to be completed automatically, precisely, and quickly.

Actually, hackers and hacking are not the intended uses for Wireshark. Hacking is not the primary purpose of the Wireshark application. The primary purpose of the Wireshark software is as a network administrator to be able to monitor what goes on within his network or to ensure that it is operating correctly and that no malicious activity is occurring there.The primary purpose of the Wireshark software is to facilitate network investigation and troubleshooting.

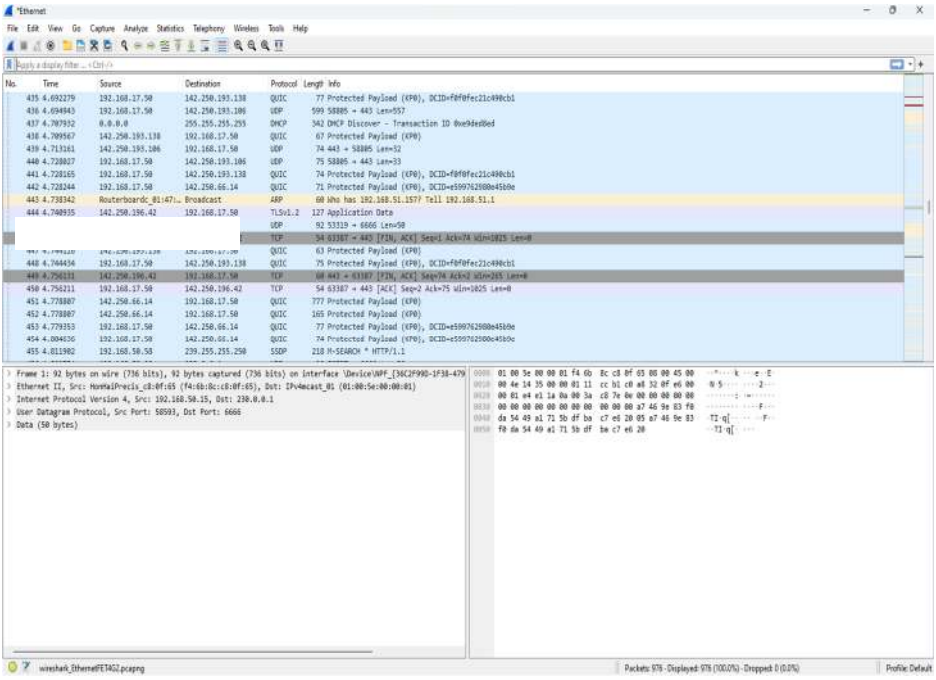

Fig 2. Capturing Network Data Packets using Wireshark.

7 Conclusion

From the above study, it can be stated that the advancement of actual information technology is highly advantageous for all spheres of life, particularly business, and this includes accountants' preparation of financial reports.
These days, having knowledge of information technology systems will help accountants in their work, thus it's important to comprehend how computer networks are used and assessed. As a result, accountants need to be well-versed in information technology (IT), including both its advantages and disadvantages.
Gaining a deeper comprehension will enhance the organization's proficiency in utilizing information technology to accomplish supervision objectives. The primary goal for management should be to preserve and oversee information sources.

References

1. Fidele, K. A., Suryono, S., & Syafei, W. A. Denial of Service (DoS) attack identification and analyse using sniffing technique in the network environment. E3S Web of Conferences, 202, 15003, (2020)
2. Bressoud, T., & White, D. The HyperText Transfer Protocol. In Introduction to Data Systems, (2020)
3. Panjaitan, Lidia & Sinukaban, Fransisca & Muda, Iskandar & Kumar, Ayush. Wireshark Packet Capture: The technology accounting information system perspective. International Journal of Multidisciplinary Research and Growth Evaluation. 02. 79-82, (2022)
4. Ariyanus. Intrusion Detection System, Andi: Yogyakarta, (2007).
5. Kumar, A., & Yadav, J. B. Comparison: Wireshark on different parameters. International Journal of Engineering and Computer Science, (2016)
6. Tuli, R. Analyzing Network performance parameters using wireshark. International Journal of Network Security & Its Applications (IJNSA), 5(1), 1–2, (2013)
7. Lyu, M., Gharakheili, H. H., Russell, C., & Sivaraman, V. Hierarchical Anomaly-Based detection of distributed DNS attacks on enterprise networks. IEEE Transactions on Network and Service Management, 18(1), 1031–1048, (2021)
8. Bebortta, S., Gupta, M., & Haseena, M. Advanced methods for network traffic analysis using Wireshark: A comprehensive approach to packet capture and security monitoring. International Journal of Research Publication and Reviews, 4(11), 1960-1965, (2023)
9. Musa, A., Abubakar, A., Gimba, U. A., & Rasheed, R. A. An investigation into peer-to-peer network security using Wireshark. In 2019 15th International Conference on Electronics, Computer and Computation (ICECCO) (pp. 150-155). IEEE, (2019)
10. Harirul Kamal, M. F. A., & Kamis, K. A. Real-time Android botnet detection via network traffic analysis using Wireshark and SSL capture. IEEE Access, 10, 45927-45935, (2022)
11. Siddiqui, A., Jain, P., & Verma, R. Forensic analysis of network security attacks using Wireshark. Journal of Computer Networks and Communications, Article ID 891234, (2020).
12. Ahmad, F., & Sohail, S. Utilization of Wireshark for enhanced industrial traffic analysis and cybersecurity. IEEE Transactions on Industrial Informatics, 19(7), 4893-4900, (2023).
13. Mala, B., Agrawal, S., Sharma, A., & Kaur, R. Exploring Wireshark for network traffic analysis. International Journal of Future Management Research, 5(6), 112-120, (2023).

14. Rahman, M., & Singh, P. Packet sniffing and analysis using Wireshark for IoT network security. Journal of Computer and Cyber Security, 18(2), 145-152, (2022).
15. Li, H., & Feng, T. Comparative study on the use of Wireshark for monitoring network performance and security breaches. Cybersecurity Journal, 29(3), 234-241, (2021).
16. Patel, J., & Gupta, R. Wireshark-based intrusion detection systems: Methods and effectiveness. Network Security and Performance Analysis, 12(1), 58-64, (2020)
17. Zhang, Y., & Lee, S. Application of Wireshark in educational settings for practical cybersecurity training. Educational Technology and Cybersecurity, 8(4), 332-340, (2019)
18. Chen, L., & Wang, Z. Analysis of Wireshark's capabilities in identifying network threats: A case study. International Journal of Advanced Network Security, 7(5), 390-395, (2021)
19. Reddy, P., & Mitra, A. Enhancing network security through packet analysis with Wireshark in enterprise environments. Journal of Network and Security, 13(3), 225-232, (2021)
20. Singh, N., & Roy, M.Wireshark applications in detecting DDoS attacks in cloud infrastructures. Cloud Computing and Security Journal, 15(2), 58-66, (2022).
21. Brown, K., & Allen, R. Using Wireshark to monitor and troubleshoot wireless networks in small businesses. Wireless Networking Review, 6(4), 75-83, (2018)
22. Torres, J. M., & Lopez, F. Real-time network performance monitoring with Wireshark and custom filters. International Journal of Data Systems Analysis, 9(1), 90-97, (2018).