BOOK CHAPTER | *"Cutting Through the Fence"*

Analysing Network Information and Protocol Using Wireshark

Theophilus Botchway
Digital Forensics & Cyber Security Graduate Programme
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: tbotway@yahoo.com
Phone: +233204001025

ABSTRACT

The volume and variety of threats and attacks against computer systems has increased the value of computer network security. There is growing need for a network manager to have the ability to inspect and analyse network data in order to understand what is going on and to respond quickly if an attack is detected. During a network investigation, protocol analysis is the evaluation of some fields in a protocol's data structure. Understanding the components of a network protocol may be quite beneficial during an inquiry. Wireshark is a useful tool for analysing network packets and their dynamics and may be used to identify and categorize many sorts of attack in this regard. This paper examines network protocols that are often utilized by applications using Wireshark. Wireshark can decode the stream of data traveling across a network and display those bits in the protocol's structured representation. The purpose of this paper is to show how Wireshark may be used to analyse network information and protocol.

Keywords: Packet Sniffer, Wireshark, Protocol Analyser, Network Packet Analysis

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Theophilus Botcway (2022): Analysing Network Information and Protocol Using Wireshark Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 203-208
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P33

1. INTRODUCTION

A packet sniffer according to Qadeer et al.,(2010) is a software that runs on a network linked device and passively receives all data link layer packets that travel through the adapter which is also called a Network or Protocol Analyser. It records data sent to other devices and stores it for further examination. A network or system administrator can properly utilize it to monitor and troubleshoot network traffic (Qadeer et al., 2010). An administrator can identify inaccurate packets and utilize the data to spot problems and assist maintain effective network data transfer using the information acquired by the packet sniffer. Sniffers provide a security risk because they may record all incoming and outgoing data, including clear-text passwords and usernames, as well as other sensitive information.

A packet sniffer tool is used to monitor and analyse data transmission that examines every packet that passes across it. Wireshark is a tool that is frequently used for packet sniffing programs (Orebaugh et al., 2006).

According to Vanparia et al., (2015), initially branded as Ethereal, Wireshark is an open source protocol analyser that works on Windows and Unix systems. Additionally the primary goal of Wireshark is to analyse traffic while serving as a user friendly tool for communication analysis and addressing network issues. It is also equipped with a number of filters which alternatively makes it easier to define a search criteria. Breaking down of recorded packets by layers is made easier with the use of wireshark, with a simple and spontaneous front – end. Wireshark is the most widely used network protocol analyser and a standard for many organisations. It is able to recognize the structure of several networking protocols, allowing you to inspect the fields of the packets being watched. This offers the network managers a variety of alternatives for doing traffic analysis jobs(Vanparia et al., 2015).

During a network inquiry, protocol analysis is the inspection of one or more fields inside a protocol's data structure and knowing the bits and pieces of a network protocol may be quite useful. This paper examines network protocols that are often utilized by applications specifically, Wireshark can be used to do protocol analysis. Wireshark can decode the stream of bits traveling across a network and display those bits in the protocol's structured format.

1.1 Background To The Study

In order to comprehend what travels over networks, packet sniffing is used. Malicious traffic transiting our networks may have a significant and sometimes irreversible effect on network devices. Sniffing allows a network analyst to ensure that the network and network security equipment, such as the router, firewall and other devices are configured and functioning as intended, such that data is being transmitted through secure channels. In the event of a security breach, security analysts employ sniffing to gather information about the source of the attack, the time and length of the assault, the data transferred among other things. It may also be used to demonstrate the use of any insecure protocols used to send delicate data (Verma, 2015). Packet analysis can also assist a network administrator in monitoring and reporting network activity, distinguishing between normal and unusual traffic, performing network diagnostics, conducting deep packet inspection and investigating security breaches. That piece of proof can be collected by using a packet sniffer. As a result, packet analysis or network analysis is the skill of understanding and analysing packets passing over a network using a packet sniffer or protocol analyser such as the Wireshark (CompTIA, 2022).

Gerald Combs founded Wireshark, in 1998, which is a packet analyser that is both free and open-source. It's used for analysing network issues as well as troubleshooting and protocol development. Due to trademark difficulties, the project was renamed was renamed from Ethereal to Wireshark in May 2006.Wireshark is a cross-platform packet capture tool that operates on a variety of Unix-like and Microsoft Windows operating systems (Verma, 2015). Wireshark is totally secure to use and it is normally used by NGOs, government agencies, enterprises and academic institutions for troubleshooting and training. Looking at traffic via the Wireshark microscope is the best method to learn about networking. It can however be used wrongly because Wireshark is a sophisticated packet sniffer, there are concerns regarding its legality. Using Wireshark on networks without authorization to inspect network packets is done by hackers (Saxena et al., 2017.).

Wireshark is a free network or protocol analyser (sometimes known as a network sniffer) that may be downloaded from the Wireshark website. Protocol analysers are tools for analysing network traffic entering and exiting a given host machine. The analyser runs on various systems such as the UNIX, Linux, and Microsoft Windows operating systems and captures packets with the GTK+ gadget toolkit and pcap. The analyser works on UNIX, Linux, and Microsoft Windows operating frameworks, and uses the GTK+ gadget toolbox and pcap for packet capturing and allows the operator to see all the traffic being passed over the network. Some capabilities of wireshark includes allowing many protocols to be thoroughly investigated, and more added from time to time. It also allows live capture and offline investigations (Dabir & Matrawy, 2007). Additionally, Wireshark is the most widely used packet analyser, and there is a reason for this. It has a lot of functionality, a large list of popular and rare protocols, and an easy-to-use interface(Nath, 2015).

2. LITERATURE REVIEW

Previous research works, such as (Bhandari et al., 2018),which investigated packet analysis and network traffic monitoring via TCP protocol using the wireshark packet sniffer. TCP throughput graph, TCP time sequence graph and TCP round trip time graph was the data studied. Based on data analysis of network traffic. Several ideas for network traffic control were offered by the researchers. Similarly, Rosa & Kadir (2018),suggested a novel system monitoring strategy. The research suggested that based on traffic behaviour methodologies and a history of linked traffic, it may give extensive information whereas complete data on internet traffic is being tracked for analysis. Additionally, for intrusion detection, Qadeer et al., (2010), created a packet sniffer on the Linux platform. The goal of the study was to look at the bottleneck scenario that might occur in a network. The next step was to identify the software's presence on the network and deal with it effectively. Furthermore, using the Simple Network Management Protocol, (Lizarti et al., 2015) describe traffic analysis in VPNs . In this study, network traffic apps create real-time traffic statistics based on TCP ports and UDP and was accessed discreetly using VPN technology to assist network managers in monitoring and analysing network problems.

Protocol Analyser

Research by Orebaugh et al., (2006), identified Protocol analysers as the tools for analysing network traffic entering and exiting a given host machine also called network analysers or network traffic analysers. This study suggested that there two separate pieces of protocol analysers. The sniffer is a piece of software that goes by the names Pcap (packet capture), Npcap, or Win10Pcap. And these are the tools that capture all of the data that flows in a certain interface and it either saves it into a file or make a live feed straight into the protocol analyser. Subsequently it reads the pcap data and analyses it in a way we can understand. Furthermore, in the article by Infosec resources, it discussed some high level network protocols such as the wireshark which is able to decode streams of bits across a network and show those bits in a structured format of the protocol.

Packet Sniffing

Asrodia & Patel, (2012) demonstrates that the following components make up the packet sniffer: Network adapters are standard hardware, Capture Filter is the most crucial component which takes network traffic from the wire, filters it for the specific activity and then buffers the data, Buffers are utilized to save the frames recorded by the Capture Filter, Real-time analyser is a module in the packet sniffer application that analyses traffic and shifts it to identify

intrusions and the Decoder such as the Wireshark kismet, tcpdump, ntop, ngrep, etherape, and kisMAc are a few examples of packet sniffing tools.

Wireshark tool

Wireshark is a packet analyser for networks. A network packet analysis will attempt to collect network packets and present them as precisely as possible. Users might think of network packet analysis as a measuring equipment for checking what happens within a network cable. Wireshark is one of the most powerful open source data packet analysis tools available today (Chappell & Combs, 2010). According to Saxena & Technol, (2017), this tool is used by network administrators to investigate network issues and also assess network security. CompTIA, (2022)is also of the view that Wireshark performs three functions namely Packet Capturing, Filtering and Visualization.

3. RESEARCH GAPS/FINDINGS

In the research it was discovered that Wireshark is not a system for detecting intrusions and will not tell you if someone does anything weird on your network that is not allowed. If weird things happen, Wireshark might be able to help the user find out what's going on. Wireshark does not transfer packets across the network or do any other unnecessary tasks. Wireshark is a manual tool that does not provide long-term monitoring.

However, because network packet analysis allows partial access to personal and geographical information, Wireshark may be used not just to provide security but also to break into a network. Furthermore, the Wireshark application enables you to detect security problems in the system at the level of user authentication. You can identify the likelihood of utilizing backdoor by easily capturing unprotected packets that are sent between network cameras and servers (Dabir & Matrawy, 2007).

4. IMPLICATIONS FOR AFRICAN ONLINE USERS

According to research, technological advancement is at a slow pace in most African countries, hence the security awareness of internet users is poor. Consequently, the African online users are easily targeted for network sniffing such as capturing sensitive data (login credentials), eavesdropping on chat messages and capturing files that have been transmitted over the network by hackers with the help of a sniffer (wireshark). In order to avoid such intrusion, online active users must ensure the use of latest and updated version of software and hardware as well as ensuring security by encrypting messages sent while online.

5. CONCLUSION

Packet sniffing is a technique for analysing data during network transmission. To put it into practice, sniffing tools are useful. It's helpful for network traffic monitoring, analysis, and troubleshooting, among other things. Wireshark is the most widely used network protocol analyser in the world. This tool is frequently used by network administrators to debug network issues. We may conclude from the aforementioned facts that wireshark is a great tool for analysing network data and protocol.

6. RECOMMENDATION FOR POLICY AND PRACTICES

It is important to keep current with the newest Wireshark version since flaws are often addressed. Wireshark should not be executed as root or administrator. Users must also examine collected files in a non-critical setting. Make a special user account for this purpose, or perhaps employ a dedicated computer. Use a modest capture tool that is less vulnerable to security flaws. When utilizing tools like wireshark, always make sure you have authorization.

This paper suggests that a traceback mechanism be added to the network to secure it. For most hacking attempts, attackers utilized a faked IP address. Wireshark's trackback method is likely to determine the address of the real source packets, resulting in Dos attacks.

7. DIRECTION FOR FUTURE WORKS

Wireshark, on the other hand, is unable to notify users in advance that an attack is imminent. If a bug is recognized ahead of time that it will harm the network, it will be a huge benefit to the IT sector and a big preventative measure against resource loss. Wireshark's ability to forecast the flow of data streams requires network analysts to explore and build methodologies.

REFERENCE

1. Asrodia, P., & Patel, H. (2012). Analysis of various packet sniffing tools for network monitoring and analysis. *International Journal of Electrical, Electronics and Computer Engineering, 1(1), 55-58.*
2. Bhandari, A., Gautam, S., Koirala, T. K., & Ruhul Islam, M. (2018). Packet sniffing and network traffic analysis using TCP—A new approach. *Lecture Notes in Electrical Engineering*, *443*, 273–280. https://doi.org/10.1007/978-981-10-4765-7_28
3. Chappell, L., & Combs, G. (2010). *Wireshark network analysis: the official Wireshark certified network analyst study guide*. Protocol Analysis Institute, Chappell University.
4. CompTIA. (2022). *What Is Wireshark and How to Use It | Cybersecurity | CompTIA*. https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it
5. Dabir, A., & Matrawy, A. (2007). Bottleneck analysis of traffic monitoring using wireshark. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/4430446/
6. Lizarti, N., Teknologi, W. A.-S.-S. dan, & 2015, U. (2015). Aplikasi Network Traffic Monitoring Menggunakan Simple Network Management Protocol (SNMP) pada Jaringan Virtual Private Network (VPN). *Jurnal.Stmik-Amik-Riau.Ac.Id*. http://jurnal.stmik-amik-riau.ac.id/index.php/satin/article/view/17
7. Nath, A. (2015). *Packet Analysis with Wireshark*. www.packtpub.com
8. Orebaugh, A., Ramirez, G., Burke, J., Pesce, L., Wright, J., & Morris, G. (2006). Introducing Wireshark: Network Protocol Analyzer. *Wireshark & Ethereal Network Protocol Analyzer Toolkit*, 51–99. https://doi.org/10.1016/B978-159749073-3/50007-5
9. Qadeer, M. A., Iqbal, A., Zahid, M., System, A., & Siddiqui, M. (2010). *Network Traffic Analysis and Intrusion Detection using Packet Sniffer*. https://doi.org/10.1109/ICCSN.2010.104
10. Rosa, S. L., & Kadir, E. A. (2018). Abnormal internet usage detection in LAN islamic university of Riau Indonesia. *ACM International Conference Proceeding Series*, 17–22. https://doi.org/10.1145/3233740.3233746

11. Saxena, P., & Technol, S. S.-I. J. A. R. I. (2017). Analysis of network traffic by using packet sniffing tool: Wireshark. *Academia.Edu*. https://www.academia.edu/download/55420664/Analysis_of_Network_Traffic_by_Using_Packet_Sniffing_Tool_Wireshark.pdf
12. Vanparia Pradip G., Ghodasara Yogesh, & Donga Hitendra N. (2015). *(1) (PDF) Network Protocol Analyzer with Wireshark*. https://www.researchgate.net/publication/282385189_Network_Protocol_Analyzer_with_Wireshark/citations
13. Verma, P. (2015). *Wireshark Network Security A succinct guide to securely administer your network using Wireshark*. www.packtpub.com