International Journal of Engineering and Management Research
e-ISSN: 2250-0758 | p-ISSN: 2394-6962
https://ijemr.vandanapublications.com

Peer Reviewed & Refereed Journal
Volume-14, Issue-1 (February 2024)
https://doi.org/10.5281/zenodo.10686707

Packet Sniffing

Dr. Paravathi C[1], Roshini D[2] and Shwetha S Nayak[3]
[1]Associate Professor, Department of Computer Science and Engineering, BGS College of Engineering and Technology, Mahalakshmi Layout, Bangalore, INDIA
[2]Student, Department of Computer Science and Design, BGS College of Engineering and Technology, Mahalakshmi Layout, Bangalore, INDIA
[3]Student, Department of Computer Science and Design, Student, BGS College of Engineering and Technology, Mahalakshmi Layout, Bangalore, INDIA

[1]Corresponding Author: pvc311925@gmail.com

Received: 15-01-2024 **Revised:** 03-02-2024 **Accepted:** 18-02-2024

ABSTRACT

Packet sniffing is a technique used to monitor network traffic by intercepting each packet that flows across the network. It can be used as a helpful administrative tool or for malicious purposes. With the advancement of technology, the network is growing rapidly, resulting in an increase in network traffic. Therefore, it is crucial to monitor both the network traffic and the activities of its users in order to maintain a smooth and efficient network. However, monitoring a large network can be a complex task due to the large number of packets involved. This is where packet sniffing comes in handy. Packet sniffing plays a vital role in network monitoring as it allows network administrators to identify any weaknesses in the network. This paper focuses on the use of packet sniffing in various environments, such as cyber attacks and ethical purposes. By utilizing a packet sniffer, we can capture and analyze network traffic. Different protocols, such as TCP, IP, and UDP, are implemented, and filtering based on these protocols is also performed.

Keywords-- Packet Sniffing, Cybersecurity, Network Monitoring, Tools of Packet Sniffing, Attack Techniques

I. INTRODUCTION

When data needs to be transmitted over a computer network, it is broken into smaller units at the sender's node, called data packets, and reassembled at the receiver's node into its original format. It is the smallest communication unit on a computer network. Data packets also known as block, segment, datagram or cell. The act of capturing data packets on a computer network is called packet sniffing. Packet sniffing is done using tools called packet sniffers. It can be filtered or unfiltered. [6]

Filtering is used when only specific packets are collected, and no filtering is used when all packets need to be collected. Wireshark, SmartSniff are examples of packet-sniffing tools. [6]

Organizations like ISP's uses packet sniffing to track all activities such as:

- who is receiver of your email
- what is content of that email
- what you download
- sites you visit
- what you looked on that website
- downloads from a site
- streaming events like video, audio, etc.[6]

To monitor and analyses data traffic, a packet sniffer tool is used. Packet sniffing is a technique of monitoring every packet that crosses the network. The tools commonly used to do packet sniffing techniques are generally Wireshark and Netcut. Packet sniffing is usually done by hackers or malicious intruders to carry out prohibited actions such as stealing passwords, and retrieving other important data. Then for the way the packet sniffing works is divided into three Process, namely collecting, conversion, analysis, and data theft.[2]

II. FUNDAMENTALS OF SNIFFING

When packets transmit from source to destination then it travels through many intermediate devices. A node whose NIC is set in the promiscuous mode receives all information travels in network. Each NIC have physical address which is different and unique from another network. When packet arrives at NIC then hardware address of frame matched with physical address that NIC have, but if we set it in promiscuous mode then all packets will arrive at that interface. When we use switch which already pass filtered data then we perform some method to capture all data of network. When NIC accept packets, packets are copied to driver memory then it passes to kernel and kernel passes it to user application. The process of Sniffing is also based on the devices used in the network. On this basis the Sniffing can be done in two modes Active sniffing and Passive Sniffing. Passive

Peer Reviewed & Refereed Journal
Volume-14, Issue-1 (February 2024)
https://doi.org/10.5281/zenodo.10686707

sniffing is intercepting packages transmitted over a network that uses a hub. It is called passive sniffing because it is difficult to detect. It is also easy to perform as the hub sends broadcast messages to all the computers on the network. Active sniffing is intercepting packages transmitted over a network that uses a switch. There are two main methods used to sniff switch linked networks, ARP Poisoning, and MAC flooding.[3]

Packet sniffers come in many forms. Some packet sniffers used by network engineers are single-purpose hardware solutions. [7]

In contrast, other packet sniffers are software applications that run on standard consumer computers and use network hardware provided on the host device to perform packet capture and insertion tasks. [7]

Packet sniffers work by intercepting and logging network traffic through wired or wireless network interfaces on a host computer.In a wired network, the information that can be collected differs depending on the network structure.Packet sniffers may be able to detect traffic throughout the network or only on specific segments.This depends on your network switch configuration.In wireless networks, a packet sniffer typically captures his one channel at a time, unless the host computer has multiple wireless interfaces capable of multichannel capture. [7]

Packet sniffer is also known as packet analyzer, protocol analyzer or network. [8] Packet sniffing is the process of capturing, collecting, and logging some or all packets that pass through a computer network, regardless of how the packets are addressed. [8]

In this way, each packet or a defined subset of packets can be collected for further analysis. Network administrators can use the collected data for a variety of purposes, including monitoring bandwidth and data traffic. [8]

Packet sniffer is made up of two main parts. First, a network card connects the sniffer to the existing network. Second, the software allows you to analyze the data collected by the device. A network is a collection of nodes, such as personal computers, servers, and network hardware that are connected. [8]

A network connection allows data to be transferred between these devices. [8]

The connection can be physical using a cable, a wire or wireless using a radio signal. Networks can also be a combination of both types.[8]

There are two main types of packet sniffers:

- Hardware packet sniffers
- Software packet sniffers[8]

Hardware packet sniffers are especially useful when trying to view traffic for a specific network segment. [8]

By connecting directly to the physical network at the appropriate location, a hardware packet sniffer can ensure that no packets are lost due to filtering, routing, or other intentional or unintentional causes. [8]

The hardware packet collector stores the collected packets or forwards them to a collector that records the data collected by the hardware packet collector for further Hardware packet sniffers are designed to plug into a network and analysis.[8]

Software Packet Sniffer Most modern packet sniffers are software-based. [8]

Network interfaces connected to a network can receive network traffic passing through them, but most are configured to not. [8]

A software packet sniffer changes this configuration so that the network interface routes all network traffic to the stack. [8]

This configuration is known as promiscuous mode on most network adapters. [8]

In promiscuous mode, the packet sniffer's function is to isolate, reconstruct, and log all software packages that pass through the interface, regardless of the destination address.

Software packet sniffers collect all traffic flowing on physical network interfaces. [8]

This traffic is logged and used according to the software's packet sniffing requirements. [8]

III. SNIFFERS FUNCTIONALITY

During sniffing, The Attacker connects to the target network to sniff packets. Using a sniffer, which switches the attacker's system's network interface card (NIC) to promiscuous mode, the attacker captures the packet.[3]

Once the attacker captures the packets, he can decrypt these packets to extract information. Sniffers can be used to hack a system or network.[3]

a) The steps an attacker takes to use a sniffer to hack a network are listed below and illustrated in Figure 1: An attacker who decides to hack a network will first discover the appropriate switch to access the network and connect the system to one of the port switches.[3]
b) After successfully connecting to the switch, the attacker tries to determine network information such as network topology using network discovery tools.[3]
c) By analyzing the network topology, the attacker identifies the victim's machine to target for attack.[3]
d) After identifying the target, the attacker uses ARP spoofing techniques to send spoofed (spoofed) ARP messages.

Peer Reviewed & Refereed Journal
Volume-14, Issue-1 (February 2024)
https://doi.org/10.5281/zenodo.10686707

e) The previous step helps the attacker redirect all traffic from the victim computer to the attacker's computer.[3] This is a man-in-the-middle attack (MITM).

f) Now the attacker can view all data packets sent and received by the victim and extract confidential information such as usernames, passwords, credit card details, PIN codes, etc.[3]

IV. ETHICAL NETWORK MONITORING USING PACKET SNIFFING TOOLS

A Comparative Study II

Vulnerabilities and Network Attacks

Vulnerabilities are weaknesses in protocols, applications, and data transmitted in computer networks. [3]

Therefore, threats exploit these weaknesses to damage resources, systems, and applications. The first thing attackers do is scout the victim's network by gathering vulnerability information using tools like dig, whois, traceroute and nslookup along with packet sniffing tools. [3]

Network scanning is used to detect vulnerabilities in the network system. Port scanning is the process of searching for active ports when a client requests a server. There are two types of cyber attacks: active or passive.

Packet sniffing is considered a type of passive attack where the attacker monitors and collects network information to obtain vulnerabilities such as cleartext passwords, routing information, financial transactions, emails, MAC (Media Access Control) address, Internet Protocol (IP)., unencrypted addresses, important and sensitive information can be obtained through packet detection tools without the user's knowledge.

Another type of cyber attack is an active attack, in which an attacker compromises a network by impersonating another entity within the network.

Examples of active attacks include IP spoofing, Address Resolution Protocol (ARP) spoofing, and MAC spoofing. [3]

V. SIGNIFICANCE OF PACKET SNIFFING IN NETWORK MONITORING

Network Monitoring Active network monitoring can provide network administrators with information to proactively manage the network and communicate network usage statistics to others. [2]

Link activity, error rate, and link health are some of the factors that help network administrators determine network health and usage.

Collecting and reviewing this information over time allows network administrators to see and predict developments, and can enable them to detect and replace a faulty component before it fails completely. [2]

SNMP is commonly used to collect information about devices. Simple Network Management Protocol (SNMP) was developed to allow administrators to manage nodes such as servers, workstations, routers, switches, and security devices on IP networks. [3]

It allows network administrators to monitor and manage network performance, find and resolve network problems, and plan for network growth. [3]

SNMP is an application layer protocol that provides a message format for communication between managers and agents. [3]

The SNMP system consists of three components: SNMP Manager, SNMP Agents (Managed Node) and Management Information Base (MIB). [3]

Packet Sniffing Packet sniffing is a tool used to monitor data packets when packets pass through a network. [3]

There is packet detection software, but there are also hardware devices that are installed directly on the network. Sniffer can manage data sent specifically to them. [3]

System administrators can legally use Sniffer on their networks to monitor and troubleshoot traffic on their own networks. For example, if one computer has trouble communicating with another computer, an administrator can view packets from one computer to another and determine the cause of the problem.[2]

The packet sniffer includes the following components:

1. Hardware: standard network adapters.
2. Capture Filter: This is the most important part. It collects network traffic from the cable, filters the specific traffic desired, and then caches the data.
3. Buffer: used to store images captured by Capture Filter.
4. Real-time analyzer: a packet sniffer module used to analyze traffic and move traffic for intrusion detection.
5. Decoder: Protocol Analysis Some examples of packet detection tools are Wireshark Kismet, Tcpdump, Cain and Abel, Ettercap, Dsniff, Netstumbler, Ntop, Ngrep, Etherape, and KisMAc.Wireshark is a network packet analysis tool. [2]

Network packet scanning attempts to capture network packets and display data packets in as much detail as possible. [2]

Users can think of a network packet analyzer as a measuring device used to check what is happening inside a network cable, such as a voltmeter used by an electrician

Peer Reviewed & Refereed Journal
Volume-14, Issue-1 (February 2024)
https://doi.org/10.5281/zenodo.10686707

to check what is happening inside an electrical cable. In the past, both tools and goods were either very expensive, exclusive, or both. However, with the arrival of WireShark, that all changed. Wireshark is one of the best opensource data analytics packages available today.

There are several parameters to classify packet sniffing as shown below.

IP-based sniffing: This is a basic and commonly used packet sniffing method.

This puts the network card into promiscuous mode and captures all packets passing through the network.

Using

IP-based filtering only packets matching the specified IP address are captured. Typically, there are no IP-based filters configured, so IP sniffing captures all packets.

IP-based Sniffing filters work on networks without switches.

MAC Sniffing: Similar to IP-based filters, MAC sniffing filters allow hosts to capture all packets on the network according to their corresponding MAC addresses.

ARP Sniffing: This method is effectively used in switched networks. It works slightly differently and does not require the network card to be in promiscuous mode when an ARP packet is sent. This is because the ARP protocol is stateless. [5]

VI. ART OF NETWORK INTERCEPTION

When computers on a network send data in the form of packets. These packets are actually blocks of data that are transferred to a particular system. All data sent has a predefined destination point. Therefore, all data is transferred directly to a specific computer. Typically, systems on a network are designed to receive packets and read only the data destined for them. The sniffing process requires cooperation between the software and his hardware. Process id given in 3 steps.

- Packet sniffer collects packets from the network in raw binary format. This typically occurs in switched networks when the selected network interface is in promiscuous mode .
- Captured binary data is converted to a readable format.
- Analysis of captured and transformed data. After the captures the network data, the packet sniffer checks the protocol based on the extracted information and starts analyzing certain characteristics this of protocol [13],[23]

VII. PACKET SNIFFING AND USING PACKET SNIFFING PROGRAMS

Packet sniffing involves capturing data packets as they flow over a computer network. Packet sniffing is to computer networks what wiretapping is to telephone networks. This is done through the use of packet sniffers, devices that are connected to the network and used to listen to network traffic. Administrators can use the information collected by packet sniffers to identify bad packets and use that data to identify bottlenecks and maintain efficient network data transmission. However, it is also often used by hackers and crackers to illegally collect information about networks they want to penetrate. Packet sniffers can be used to capture data such as passwords, IP addresses, protocols used on your network, and other information that can help attackers penetrate your network. Packet sniffing is primarily used for intrusion detection, network management, eavesdropping, and packet sniffing. Password sniffing programs are the most common packet sniffing programs. [1]

VIII. SNIFFING AROUND THE HUB AND SNIFFING IN A SWITCHED NETWORK

Sniffing on a Hub Sniffing on a network where a hub is installed is a packet analyst's dream.

Traffic sent through a hub is sent to all ports connected to that hub. To analyze computers on a hub, simply connect a packet sniffer to an empty port on the hub and see all communication to and from all computers connected to that hub. when the sniffer is connected to a hub network, the visibility window is unlimited. Sniffing in Switched Networks Switched environments are the most common type of network. Switches provide an efficient way to forward data on broadcast, unicast, and multicast traffic. [1]

A port monitor is a program that runs in the background while other programs are running. Port mirroring, or port spanning as it is often called, is probably the easiest way to capture traffic from target devices on a switched network.

Hubbing out Another very easy way to capture traffic through target devices on a switched network is to use hubs. Hubbing out is a technique that places target devices and analysis systems on the same network segment by connecting them directly to a hub. [1]

IX. BEYOND INVALID ADDRESSES: A COMPREHENSIVE GUIDE TO PACKET SNIFFER DETECTION

There are many ways to detect sniffers on your network. • Users can generate packets containing invalid addresses. If a machine (on the network) accepts the packet, you can conclude that it is running a sniffer. Here's how to do it: User can temporarily change her MAC address on her computer. If you send a package to your computer's old address, the package will not be accepted. When the machine actually accepts the packet, a sniffer is executed. • You can detect sniffers using software programs such as AntiSniff. According to a review by Dave Kearns (Network World on NT), "AntiSniff provides the ability to remotely detect computers that are intercepting packets." By running a series of non-penetrative tests in a variety of ways. , network administrators and information security professionals can determine: Is a remote computer eavesdropping on all your network communications?" [1] Anti Sniff is a tool from his L0pht Heavy Industries designed to detect hosts on Ethernet/IP network segments that are collecting data uncontrollably . Tests are divided into three classes: DNS tests, operating system-specific tests, and network and machine latency tests. [21], [1]

X. CONCLUSION

In This Paper, Packet sniffing helps analyze data traveling on a network. Sniffing tools can help you accomplish this. Among its many practical uses are troubleshooting, traffic analysis, and network traffic monitoring. Learn about important packet sniffing tools that monitor and capture traffic between authorized users. This makes packet sniffing a serious network security issue. Sniffers can be used in any environment. Therefore, we recommend that you send your data encrypted. Packet sniffers are not hacking tools. It is used to troubleshoot, monitor, analyze, and audit network traffic to make your network more secure, reliable, and perform better. There are a variety of tools known as packet sniffing tools for capturing, monitoring, inspecting, and analyzing wired and wireless computer network traffic.

REFERENCES

[1] Patel, Nimisha. Patel, Rajan & Patel. Dhiren. (2009). Packet sniffing: Network wiretapping. *IEEE International Advance Computing Conference (IACC 2009) Patiala, India,* pp. 2691-2696. Available: https://www.researchgate.net/publication/267908713_Packet_Sniffing_Network_Wiretapping.

[2] Siswanto, Apri & Syukur, Abdul & Abdul Kadir, Evizal & Suratin,. (2019). *Network traffic monitoring and analysis using packet sniffer.* 10.1109/COMMNET.2019.8742369. Available at: https://www.researchgate.net/publication/333965857_Network_Traffic_Monitoring_and_Analysis_Using_Packet_Sniffer.

[3] Tuli, Ruchi. (2020). Packet sniffing and sniffing detection. *International Journal of Innovations in Engineering and Technology, 16,* 22. DOI: 10.21172/ijiet.161.04. Available at: https://www.researchgate.net/publication/356284567_Packet_Sniffing_and_Sniffing_Detection

[4] Sarve, Miss & Mahadik, Shubhangi. (2022). Comparative study on packet sniffing tools. *International Journal of Advanced Research in Science, Communication and Technology*. 403-407. DOI: 10.48175/IJARSCT-5697. Available at: https://www.researchgate.net/publication/361874814_Comparative_Study_on_Packet_Sniffing_Tools.

[5] Thiyeb, Ibrahim & Saif, Anwar & Al-Shaibany, Nagi. (2018). Ethical network surveillance using packet sniffing tools: A comparative study. *International Journal of Computer Network and Information Security, 10,* 12-22. DOI: 10.5815/ijcnis.2018.07.02. Available at: https://www.researchgate.net/publication/326419957_Ethical_Network_Surveillance_using_Packet_Sniffing_Tools_A_Comparative_Study.

[6] Packet Sniffing?. GeeksforGeeks[online]. Available at: https://www.geeksforgeeks.org/what-is-packet-sniffing/.

[7] Packet Sniffers and How Do They Work lifewire [online]. Available at: https://www.lifewire.com/what-is-a-packet-sniffer-2487312.

[8] Packet sniffing-Definition and details, paessler [online]. Available at: https://www.paessler.com/it-explained/packetsniffing#:~:text=Packet%20sniffing%20is%20the%20practice,be%20gathered%20for%20further%20analysis.

[9] I. Kaur, H. Kaur & E. G. Singh. (2014). Analysing various packet sniffing tools. *Int. J. Electr. Electron. Comput. Sci. Eng, 1*(5), 65–69.

[10] Tom King. (2002). *Packet sniffing in a switched environment*. SANS Institute, GESC Practical

Peer Reviewed & Refereed Journal
Volume-14, Issue-1 (February 2024)
https://doi.org/10.5281/zenodo.10686707

V1.4, Option 1, Aug 4th 2002, Updated June/July 2006.

[11] Nabanita Mandal & Sonali Jadhav. (2016). A survey on network security tools for open source. *IEEE*.

[12] Savita Kamalakarrao Kulkarn. (2015). A survey of password attacks, countermeasures and comparative analysis of secure authentication methods. *IJARCSMS, 3*(11), 319-331.

[13] Dr. Aruna Varanasi & P. Swathi (2016). Comparative study of packet sniffing tools for http network monitoring and analyzing. *IJCSET, 6*(12), 406-409.

[14] Nedhal A. Ben-Eid. (2015). Ethical network monitoring using wireshark and colasoft capsa as sniffing tools. *International Journal of Advanced Research in Computer and Communication Engineering, 4*(3), 471-478.

[15] Palak Girdhar & Vikas Malik. (2016) A study on detecting packet using sniffing method. *Journal of Network Communications and Emerging Technologies (JNCET), 6*(7).

[16] Greg Barnett, Daniel Lopez, Shana Sult & Michael Vanderford. (2002). *Packet sniffing: Network wiretapping.* Group Project, INFO 3229-001.

[17] A. Meehan, G. Manes, L. Davis, J. Hale & S. Shenoi. (2001). Packet sniffing for automated chat room monitoring and evidence preservation. *Proceedings of the Second annual IEEE Systems, Man and Cybernetics Information Assurance Workshop, New York*, pp. 285-288.

[18] Chris Senders. (2007). *Practical packet analysis, using wireshark to solve real-world network problems.* San Francisco: No Starch Press Inc.

[19] Dick Hazeleger. (2001). *Packet sniffing: A crash course*. Netherlands.

[20] Sabeel Ansari, Rajeev S.G. & Chandrashekar H.S. (2002). Packet sniffing: A brief introduction. *IEEE, 21*, pp. 17-19.

[21] Raed Alomoudi, Long Trinh & Darleen Spivey. (2004). *Protecting vulnerabilities or online intrusion: The efficacy of packet sniffing in the workplace.* Florida Atlantic University ISM 4320.

[22] H. AbdelallahElhadj, H. M. Khelalfa & H. M. Kortebi. (2002.) *An Experimental sniffer detector: Sniffer wall.* S´Ecurit´e des Communications sur Internet (SECI02).

[23] BoYu. (2010). Based on the network sniffer implement network monitoring computer application and system modeling (ICCASM), *International Conference on Volume*: *7* pp. V7-1-V7-3.