Packet Sniffer

Indrajit Bhattacharya[1], P.Snithik Reddy[2]
[1,2]*Sree Nidhi Institute of Science and Technology, Hyderabad, India*

***Abstract*: Protocol analysis and security rely heavily on packet sniffing and packet capture software. An analysis, debugging, and testing tool for novel protocol implementations is a necessity in protocol design research. Like any technology, in security it can be used both to identify intrusions or attacks on a system and to hack into other people's personal and financial information. These technologies, even though they make it impossible to obtain data directly, are essential in learning about current sessions and collecting encrypted data to launch offline attacks to generate the encryption key, and any such attack limited only by one's imagination. Because of this, packet sniffer software is one of the most crucial instruments needed for the above-mentioned tasks to get started. Ultimately, the goal of our research is to create a lightweight, universal packet sniffer that can be used in any system to monitor the packets that are being transmitted and received across both wired and wireless networks.Sniffer is a packet analyzer.**

1.INTRODUCTION

Packet sniffing is a technique that records the contents of packets as they travel over a network. It's a tool that monitors all the network traffic. Furthermore, it has the ability to intercept and log all network communication, both incoming and outgoing. "Packets" are the means by which information is conveyed over a network. Packets can be delivered from one computer to another on a network by breaking them into smaller segments, each of which has a destination and source address, and other important information. It is possible, however, to examine the performance of a network or identify a bottleneck if a packet sniffer is deployed at any of its nodes (either the source or the destination). Sniffer packets are mostly utilized by network administrators since they aid in troubleshooting, monitoring, and identifying potential network vulnerabilities, as well as providing a human-readable representation of binary network data, such as a clear username and password for a VoIP call. If you don't have authority to use a packet sniffer on a specific network in your organization, these are possible unlawful uses. Protocol and network analyzers can also be used interchangeably with packet sniffers. There are two kinds of packet sniffers: active and passive. Passive packet sniffers don't send or receive any responses; they simply collect data and can't be seen. For example, telecommunications, radar systems, and medical equipment all benefit from passive sniffers. Passive packet sniffers include Colasoft Capsa, TCPDUMP, and Wireshark. Active packet sniffers are capable of sending data over the network, and as a result, other systems may be able to detect them. A packet sniffer, for example, can respond to a broadcast with a phony response or forward it to a valid host. As far as active packet sniffers go: Scapy, SmartRF, and the Network ACTIV Protocol Packet Sniffer

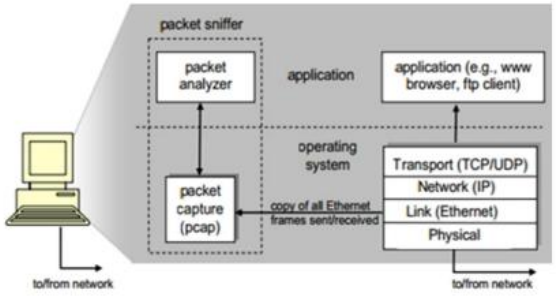


Fig.1: Structure of packet sniffer

Both the packet analyzer and the packet capture are components of the packet sniffer (pcap). Packet analyzers work at the application layer, whereas pcap captures packets at every other layer, including the physical layer, the link layer, the IP layer, and even the transport layer. pcapAn program operating on the network can send and receive packets using the packet analyzer. The basic structure of a packet sniffer is shown in Figure 1 [1]. Programs or devices that may eavesdrop on network communication are known as sniffer programs or devices. "Data Interception" technology[1] is what sniffers really are. They work because the Ethernet standard was based on the idea of sharing data and resources.

Messages sent to one computer can be received by another computer on the same network using broadcast technology. This message will be ignored by all computers save the one to which it is addressed. Even if a message is not intended for a computer, it can nonetheless be accepted. [1] A sniffer[1] is used to do this task. Syslog, DNS, web, email, and other data traffic can be snooped on by an attacker via sniffing. Data, usernames, and passwords from protocols like HTTP, POP3, IMAP4, FTP, and Telnet can be obtained by capturing these packets. Using Promiscuous ports, sniffing is carried out. This paper explains how a packet sniffer works, the protocols that are vulnerable to sniffing, the many types of tools used for sniffing, and how to fight against sniffing attacks[2].

2.LITERATURE REVIEW

2.1 Packet Sniffing : Network Wiretapping Packet Sniffing : Network Wiretapping

Using a technique called packet sniffing, you can listen in on every packet that makes its way across the network. Sniffering is a technique in which a user eavesdrops on other network users' communications. Switched and non-switched networks can benefit from it. It is possible to use a packet sniffer for both administrative and malevolent objectives. It all depends on what the user intends to do. AntiSniff's methods for detecting these sniffing programs are also addressed in this document, as are the various methods for sniffing packets in hub and switched networks.

Analysis of Different Packet Scanning Tools 2.2

Sniffing packets is a method for keeping tabs on every data transfer over a network. As network technology advances and becomes more widely used, it is becoming increasingly important to protect against cyberattacks. Security measures must be taken to prevent unwanted access as well as hacker attacks. For troubleshooting and logging purposes, packet sniffing is essential. For wired and wireless network analysis, Packet Sniffers are essential tools. A comparative study of several packet sniffing technologies is the topic of this paper.

In order to maximize the network value, use ColasoftMaximize

The widespread use of current information technology, including e-commerce, e-government, and network offices, provides businesses with the ability to grow more quickly. People may benefit from the network's convenience and profitability, but they must also bear the low efficiency, problems, and even breakdowns that come with it, which can harm the functioning of businesses and organizations and result in unfathomable losses for them. Network engineers and administrators have challenges in improving network speed and efficiency as security management and performance maintenance become increasingly critical. However, due to the complexity of the network infrastructure and the rapid development of network technology, it is more difficult than ever before to perform network maintenance and network configuration. An effective network solution such as Colasoft Capsa can assist administrators in becoming network troubleshooting experts and in identifying and resolving network issues as they arise.

When packets are too large, network performance suffers.

Transmission Control Protocol is the most often used Internet protocol. It does this by breaking up a huge piece of data into smaller pieces, which are referred to as segments. Improved network performance is made possible via segmentation. It has a severe flaw in that its congestion control algorithm does not allow long-distance networks to use all of the available bandwidth. Network Simulator-2 is a useful tool for testing TCP performance in various network settings (NS-2). TCP methods can be tested and evaluated using this application. As packet size increases, so does TCP's performance in a rapidly moving network. As packet size increased, so did the network's throughput. This is because after exceeding the dedicated packet size, it will allocate double the required packet size and fill unallocated packet space, reducing throughput.

The fundamentals of performance testing

If you're like most organizations, you're not aware of the enormous benefits that can be gained from performing performance testing earlier in the development process than is absolutely necessary. • To fulfill arbitrary deadlines, skip all performance testing. To the extent where the outcomes are useless,

over-engineer it. This is because there is a belief that it is difficult to do, which is obviously false. While many people believe outsourcing is the greatest and most cost-effective method for performance testing, this is simply not the case. It's a common misconception that only highly compensated consultants can perform in-house testing, but this is simply not true. As previously stated, it takes a lot of time to build and implement, which means that the delivery timescales would be affected, which is false. As long as you get an application that runs well under heavy demand, even if any of above is true, a minor delay in delivery should be acceptable. In this white paper, we are going to illustrate that any firm can undertake performance testing regardless of the complexity of the application under test, with a little thought and common sense.

List of Top 5 Packet Sniffer Appreciation

This awareness of diverse sorts of traffic traversing networks and providing enough methods for decision-making is becoming increasingly critical as networks continue to grow. Traffic monitoring and analysis is vital for troubleshooting and solving network issues so that they don't take down network services for long periods of time. Network traffic can be monitored and analyzed with the help of a plethora of technologies. This paper compares the performance of five different packet sniffers, comparing them to each other.

3.IMPLEMENTATION

Using the term "packet" in the context of computer communications, we can refer to a specific amount of data. All traffic on the Internet is transmitted in the form of packets, including file downloads, web page retrievals, and email. It is a unit of data that is transmitted in packet mode on the internet. A All data link layer frames travelling via the device's network adapter are intercepted by a packet sniffer application. The packet sniffer saves the data that is sent to other devices for further investigation. For legitimate network and system administration purposes, this can be used to observe and debug traffic. Network administrators often employ packet capture to troubleshoot problems, but it may also be used to look for security concerns in network traffic. Packet captures could be used by a hacker to acquire passwords and other sensitive information.

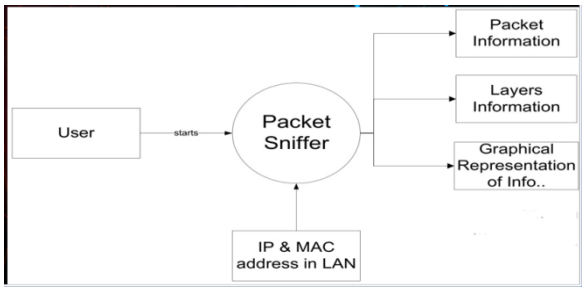


Fig.2: Flow diagram

The raw data packets are intercepted and stored when a packet sniffer is placed in the network. This data packet is then processed by packet sniffing software before being provided to the system administrator or technician. Packet Sniffer devices are used to monitor network activity, discover faults, or even detect loopholes, and can be a useful tool for network administrators. It happened while I was working as a system administrator at Reliance Mumbai Metro One that a malware attack occurred. Certain Windows XP and Windows Server 2003 computers were experiencing erratic behavior, while Windows 7 systems were experiencing a Blue Screen of Death. There was an initial impact on CCTV systems, but it expanded to other systems. SMB vulnerabilities in earlier Windows systems allowed the malware to spread by injecting code into the svchost.exe process, causing Firewalls to cycle on and off, preventing critical data from being transferred between stations. A packet sniffing tool like Wireshark or TCPDump was used to catch this behavior, but it required different versions to be loaded on different operating systems.

Network sniffer and parser Tcpdump can be used on a wide range of platforms. Because the installation file for TcpDump is so small (484 KB), it uses relatively little RAM. There is no graphical user interface for TcpDump (GUI). These commands require study and familiarity with command prompts like screen. There are numerous extensive sorting and filtering options in Wireshark that are not available in TCPdump, but its installation file size is just 18MB and after installation it will take up an incredible 449MB on Linux and Windows, respectively. As a result, it is quite expensive in terms of memory requirements.

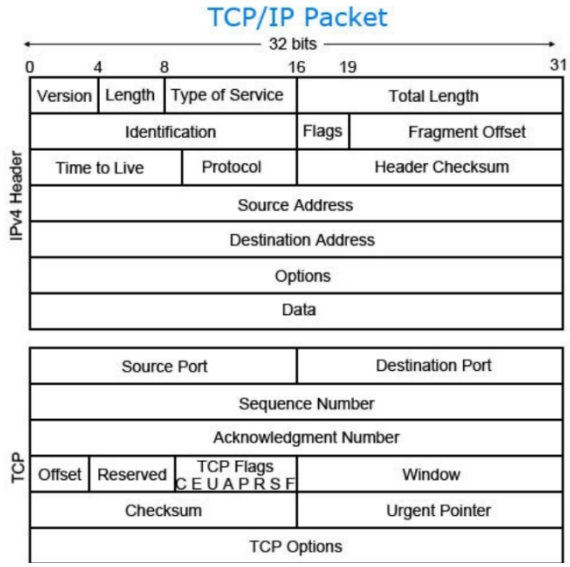


Fig.3: TCP/IPV4 packet

Most of the features of other packet sniffers are included in our application, which has a simple user interface. A Python executable file of 8 MB in size is available for Windows users, and it simply requires the PCAP Drivers that are required by other solutions like TcpDump and Wireshark to be installed. Linux doesn't need a driver for this; all you need is a recent version of python, which comes pre-installed on nearly all distributions.

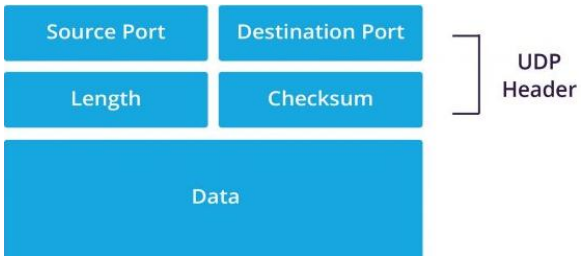


Fig.4: UDP packet

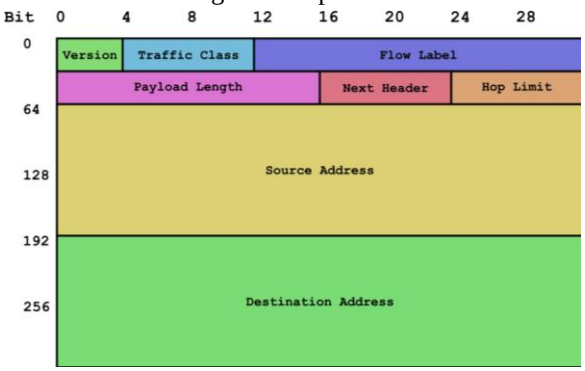


Fig.5: TCP/IPV6 packet

4. WORKING OF SNIFFERS

Sniffing occurs when an attacker connects to the target network in order to collect packets for analysis. The packet is intercepted by the attacker using sniffers, which put the NIC on the attacker's system into promiscuous mode. It is possible for an attacker to decrypt these encrypted packets once they have been captured. It is possible to hack a system or a network using sniffers. An attacker that wants to utilize sniffers to breach a network follows these steps:

To get access to a network, an attacker must first locate the proper switch and attach a machine to one of its available ports.

b) After successfully connecting to the switch, the attacker uses network discovery tools to gather network information such as topology.

When the attacker uses the network topology to identify the victim's computer, he or she can then direct their attacks there.

d) The attacker utilizes ARP spoofing techniques to transmit a phony (spoofed) ARP message after identifying the victim.

Step e helps the attacker redirect all traffic away from the victim's computer and towards the attacker's. It's a "man in the middle" assault (MITM).

A hacker now has access to the victim's entire traffic, including all data packets sent and received, and can use that knowledge to get access to the victim's account or credit card information.

5. EXPERIMENTAL RESULTS

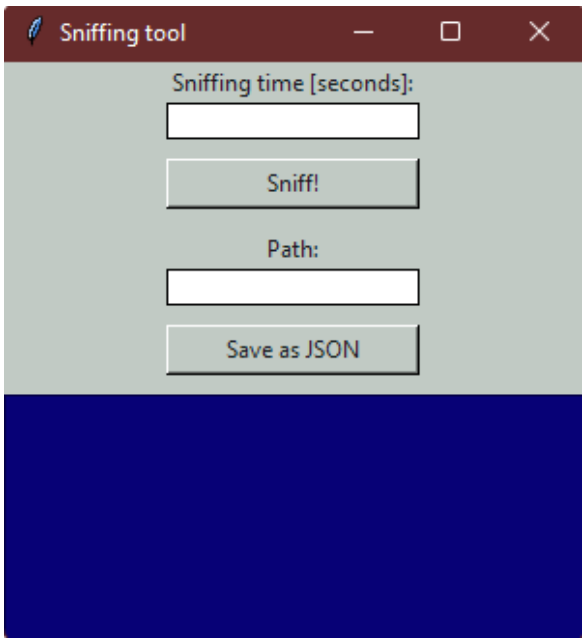


Fig.6: Output-1

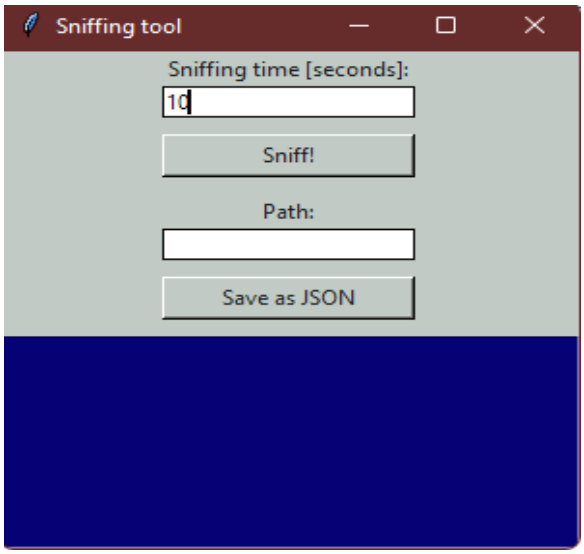


Fig.7: Entering time

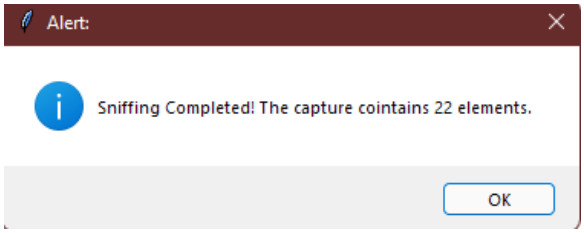


Fig.8: Sniffing complete

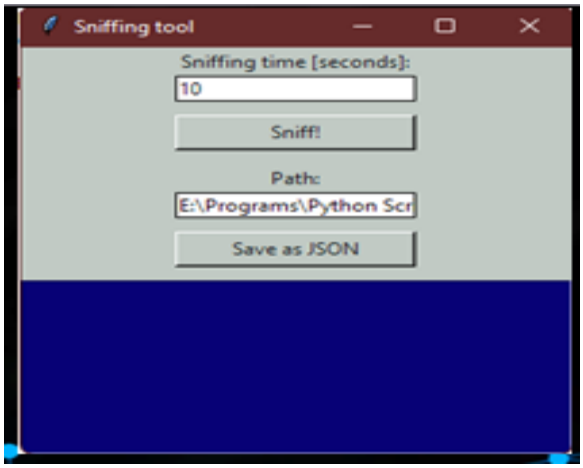


Fig.9: Enterering path

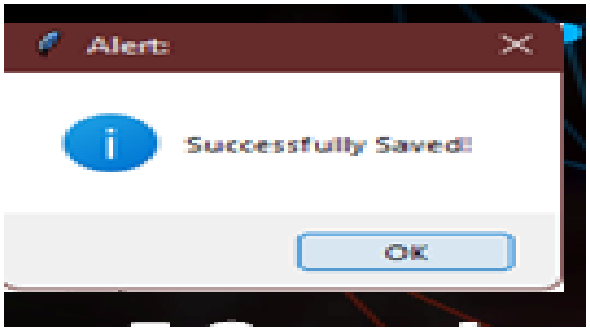
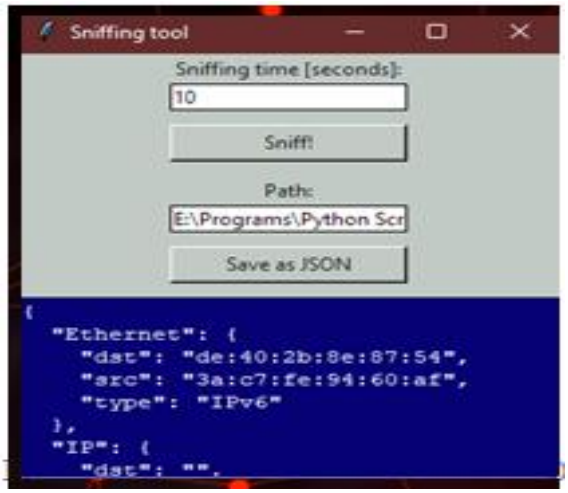


Fig.10: Saved



"Raw": {
"load": "'GET / HTTP/1.1\\r\\nUser-Agent: Mozilla/5.0 EA Download Manager
PCWIN\\r\\nlocaleInfo: en_US\\r\\nAccept-Language: en-US\\r\\nConnection:
heartbeat.dm.origin.com\\r\\n\\r\\n'"
}
}

Fig.12: Unencrypted data in packet

6. CONCLUSION

In this paper, we'll take a look at some of the most useful packet sniffing techniques for keeping tabs on legal user activity. It's important to remember that every tool has its own unique set of capabilities and working methods. "Prevention is better than cure," as the adage goes. Some countermeasures against sniffing, then, are also being considered in this paper Packet sniffing is a severe issue for network security because the primary goal of using sniffers is to gather sensitive data, such as passwords. Encryption is the greatest way to protect your data from being intercepted by sniffers. Detecting and protecting data from network sniffers can be done in a variety of ways, as has been covered in the latter half of this study. As a network administrator's worst nightmare, sniffers can be difficult to detect in some cases.

On both qualitative and quantitative metrics, no one packet sniffer outperforms all the others. TCPdump offers the lowest overhead, but Colasoft Capsa provides the highest level of network security. The following table lists the most common scenarios and the most appropriate tool for each one. The goal of this research is to make recommendations for the best packet sniffing tools based on the needs of actual

users. Each of these factors can be used to create a new packet sniffer that avoids the limitations of existing ones while outperforming them in terms of both quantitative and qualitative metrics.

REFERENCES

[1] "Tutorial on Wireshark". Internet: http://webhost.bridgew.edu/sattar/CS430/HW/ LABS/wireshark.htm [Oct. 10,2013].

[2] L. Garcia,"programming with libpcap," in Hacking- Practical protection hard core IT magazine, Vol 3, 2008, pp. 38-46.

[3] K. zhou, "Top 5 Most Welcomed Packet Sniffers," [online], 2009, http://snifferclub. Blog spot.in/2009/05/top-5- most-welcomed-packet-sniffers.html.

[4] All about TCPdump [Online] Available http://www.TCPdump.org/.

[5] H. styn, "TCPdump fu," Linux journal,. [online], 2011, http://www.linuxjournal.com/content/ TCPdump-fu?page=0,1 .

[6] TCPdump Command, Command Reference, [online], http://publib.boulder.ibm.com/info center/pserie s/v5r3/index.jsp?topic=/com.ibm. aix.cmds/doc/ aixcmds5/TCPdump.htm

[7] All about Xplot [Online] Available http:// www.xplot.org/

[8] All about Gnuplot [Online] Available http:// www.gnuplot.info/

[9] All about Wireshark [Online] Available http:// www.Wireshark.org/.

[10] How to Use GeoIP With Wireshark, "Wireshark", [online], http://wiki.Wireshark.org/HowToUseGeoIP

[11] All about Colasoft Capsa [Online] Available www.colasoft.com

[12] Colasoft Capsa- Compare Editions, "ColasoftMaximize network value" [online], http://www.colasoft.com/Colasoft Capsa/editions.php

[13] A. Shah, D. Bhatt, P. Agarwal, and P. Agarwal, "Effect of Packet-Size over Network Performance", International Journal of Electronics and Computer Science Engineering, Vol. 1, pp. 762-766, 2012.

[14] J.Colantonio,"Performance testing basics", http://www.joecolantonio.com/2011/07/05/perf ormance-testing-what-is-throughput, 2011.

[15] .Stating Response Time Requirements, RPM solutions, [online], 2004, http://www.loadtest.com.au/Terminology/Resp onseTime.htm