

INTRANET SECURITY USING A LAN PACKET SNIFFER TO MONITOR TRAFFIC

Ogbu N. Henry¹ and Moses Adah Agana²

¹Department of Computer Science, Ebonyi State University, Abakaliki, Nigeria

² Department of Computer Science, University of Calabar, Nigeria

ABSTRACT

This paper was designed to provide Intranet traffic monitoring by sniffing the packets at the local Area Network (LAN) server end to provide security and control. It was implemented using five computer systems configured with static Internet Protocol (IP) addresses used in monitoring the IP traffic on the network by capturing and analyzing live packets from various sources and destinations in the network. The LAN was deployed on windows 8 with a D-link 16-port switch, category 6 Ethernet cable and other LAN devices. The IP traffics were captured and analyzed using Wireshark Version 2.0.3. Four network instructions were used in the analysis of the IP traffic and the results displayed the IP and Media Access Control (MAC) address sources and destinations of the frames, Ethernet, IP addresses, User Datagram Protocol (UDP) and Hypertext Transfer Protocol (HTTP). The outcome can aid network administrators to control Intranet access and provide security.

KEYWORDS

Packet, Sniffer, Protocol, Address, Network, Frame

1. INTRODUCTION

In every network, security is needed by the users. Hence, a reliable and secure connection from every computer in a network must be ensured as users communicate with each other. One of the methods to realize this is by using a packet sniffer to capture and analyze packets that run through the network.

Packet sniffing is tool used for monitoring and analyzing the network to troubleshoot and log activities. It assists in capturing all the packets on networks irrespective of the final destination of the packet. It is important to manage, maintain and monitor networks to avoid contemporary network problems such as abuse of privacy and propagation of malicious connections. By so doing, the network can operate smoothly and efficiently. For this purpose, a packet sniffer, sometimes called a network analyzer (formerly known as ethereal) is used. The essence is to curb malicious attacks.

With a packet sniffer, one can watch all the non-encrypted data that travel from one's computer onto the internet; this includes data that is not secured by encryption [1]. All the data traffic travelling across the network can be viewed by the network administrator if a packet sniffer is placed on a network in promiscuous mode, and once the raw packet data is captured, the packet sniffer analyzes it and presents it in human readable form so that the person using the software can decipher it.

There are two variants of sniffers: either hardware or software. The basic task of any sniffer is to intercept and collect the local traffic, and then provide the function to decode and analyze the content of the packets in human readable format. A packet sniffer has many uses, both positive and negative. It is principally used to monitor network activities. For example, when a network monitoring tool is located at one of the servers of one's Internet Service Provider (ISP), it would be potentially possible to monitor all of the network activities, such as which website is visited, what is looked at on the site, who is sent an email, what is being downloaded from a site and also what streaming events are used. When used positively, a packet sniffer helps to maintain a network to enable it work normally. It captures packets, records and analyzes traffic, decrypting and displaying the packets in clear text. It further converts the captured data to a readable format, showing relevant information such as the IP address, protocol, host and the server name. Though having a sniffer installed can benefit a lot in terms of network troubleshooting and network usage, it is however unable to read the encrypted packets [2].

A virtual private network (VPN) linking offices to their headquarters' internal network using shared infrastructure and dedicated connections is what is termed an Intranet. Intranet VPNs allow access only an organization's employee or agent using authentication and encryption techniques. Intranet web servers therefore differ from public web servers. The public web servers do not have access to an organization's Intranet without passwords and permissions, except via hacking. Cyber criminals can go to any length to breach network securities.

A packet sniffer is used as a tool to capture all the packets flowing through a network irrespective of the final destination of the packet. If it is installed in any of the nodes of the network (either as source or destination), it can be used to analyze the performance of the network or to find bottlenecks in it. Packet sniffers are of two types: active sniffers which can send data in the network and can be detected by other systems through different techniques and the passive sniffers which only collect data, but cannot be detected (e.g. Wireshark). Also, the structure of a packet sniffer consists of two parts: packet analyzer which works on the application layer protocol and the packet capture (pcap) which captures packets from all other layers [2].

Packet sniffers are software tools used in monitoring network activities, akin to law enforcement investigations into criminal behaviours, monitoring the communications to and from people of interest to gather evidence about crimes that the suspects will commit [3]. Packet sniffers are installed on computers in a network, and once activated, they make copies of all network traffic packets that are sent and received by the host computer. They are used for a variety of reasons, including: as a problem solving tool to fix network problems, as a performance tool to identify bottlenecks in the network and areas where efficiency can be improved, and as a technique in security management. A network administrator can grab those packets that are passing through the network to trace any access to the network. A packet sniffer is used for detecting messages being sent and received from a network interface, detecting an error implementation in network software and collecting statistics and the network traffic.

A network interface card (NIC) of a system in promiscuous mode has the ability to take over all packets and frames it receives on a network [4]. The security threat presented by sniffers is their ability to capture all incoming and outgoing traffic, and it may seem difficult to detect these sniffing tools because they are passive in nature. The detection of such sniffing tools is however only difficult when the capturing and analyses of data is done in a SHARED environment not on a SWITCHED environment. With the information captured by the packet sniffer, administrators can identify erroneous packets, using them to pinpoint bottlenecks and help to maintain efficient network data. Some organizations see packet sniffers as internal threats. Some however see packet sniffers as just being a hacker's tool, though it can also be used for network traffic

monitoring, traffic analysis and troubleshooting to avoid misuse of network by both internal and external users [5].

Slowdown in the network performance can cause some serious concern to network analysts, leading to loss in resources. It is often difficult to deal with such cases due to want of time. Most problems in a network most times could be due to attacks by unknown third parties making attempts to put the web server out of service by means of Denial of Service (DOS) attack. This is achieved by sending some malicious traffic in in order to discover hosts to infect or simply by infecting ports with malwares. In all these cases, knowing the sources of the attacks is the first step towards taking appropriate action in achieving correct protection. A good way of achieving correct protection is by using a trusted packet sniffer such as Wireshark, formerly known as Ethereal, whose prime objective is networking troubleshooting, analysis, and networking research [6].

Packet sniffing is a technique used in tapping each packet that flows through a network. It is used in sniffing data belonging to other users of the same network. Packet sniffers can also be used for malicious purposes, or can be operated as an administrative tool. It is dependent on the user's intentions. Network administrators use packet sniffers as utilities for efficient network administration. The conclusions drawn from the working behaviour of Wireshark, a packet sniffing software according to [7] include:

- i) It only gives the log of data that the network administrator needs to analyze to find the error or attack on the network adapter.
- ii) Only the packets of the current systems on the network can be captured.
- iii) Packet sniffing is extremely time-consuming because the administrator has to examine and disassemble every packet and manually take an action based on the interpretation from the analysis.

Packet sniffers are a useful tool for cyber crime investigators and law enforcement agencies when monitoring emails during investigations [7]. There is a proportional increase in the number of network users as the network sizes keep increasing on daily basis. This equally increases crime rates as well as traffic flows in the networks. It thus becomes pertinent to monitor network traffic as well as its user's activities to keep the network smooth and efficient [4]. For a complex network, it is a very tough task to maintain and monitor the traffic because of the large amounts of data available. For this purpose, packet sniffing becomes a compendium for network management, monitoring, and ethical hacking.

When packets are transferred from source to destination, they pass through many intermediate devices. All information travelling in the network is received by a node whose NIC is set in the promiscuous mode. A method to capture all data of the network is utilized whenever a switch that is already passing filtered data is used [4]. Figure 1 illustrates the physical structure of a packet sniffer.

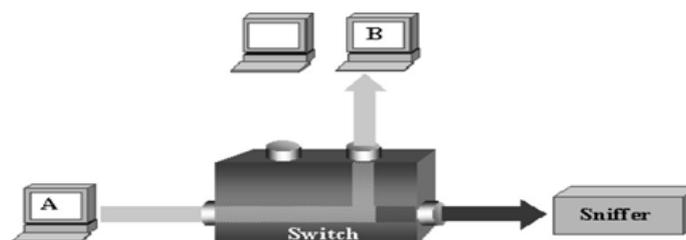


Figure 1: The physical structure of a packet sniffer [4].

2. PACKET SNIFFER ARCHITECTURE

Any sniffer can be divided into:

- Hardware
- Drive program
- Buffer
- Packet Analysis

Packet sniffers can be operated in both switched and non-switched environment. All transaction hosts are connected to a hub in the switched environment; however, there are periodic updates of network infrastructure by enterprises, replacing aging hubs with new switches. The essence of replacing the hubs with new switches in the switched environment is to increase security. Packet sniffing is thus not impossible in switched environment [8]. The positive side of packet switching is its network traffic analysis capability. The network analyzer can be used for;

- Providing detailed information of activities that are going on in the network
- Testing anti-malware programs and pin-point potential vulnerabilities
- Detecting unusual packet characteristics
- Identifying packet sources and destinations

Figure 2 shows how packets from various sources and destinations are sniffed at the server end.



Figure 2: The Internal process of packet sniffing at server end [8].

A typical packet sniffer is designed to capture all the packets of data passing through a given network interface. Typically, the sniffer will capture packets that were intended for the machine in question. The packet sniffer is however also capable of capturing all packets traversing the network regardless of the destination if placed in a promiscuous mode [9].

Three sniffing methods can be identified, some of which work in switched environments while others work in non-switched environments. The methods include:

1. **IP-based sniffing:** This is the traditional packet sniffing method that works by putting the network card into promiscuous mode and sniffing all packets matching the IP address filter. This method works only in non-switched networks.
2. **MAC-based sniffing:** This method is achieved by putting the network card into promiscuous mode and sniffing all packets matching the MAC address filter.

3. **ARP-based sniffing:** This method does not put the network card into promiscuous mode. It is made possible because the ARP protocol is stateless, as a result of this, sniffing can be done on a switched network [10].

Network sniffing encompasses the process of monitoring, capturing and interpreting all incoming and outgoing traffic that flow through a network. A Packet sniffer shows all sorts of transactions going on in a network, including unknown communications between network nodes and devices, the detailed error codes provided by layer-specific protocols, including even poorly designed programs that run abnormally [10].

2.1 THE WORKING PROCESS OF A PACKET SNIFFER

Three major steps are involved in the packet sniffing process, namely: collection, conversion and analysis [10].

Collection: The packet sniffer first turns on the selected network interface into promotion mode in which the network card can listen to all network traffics on network segment in question, capturing the raw binary data from the wire.

Conversion: This involves converting the captured binary data into a readable form. Most of the advanced command-line-driven packet sniffers terminate at this point. The interpretation of the network data at this point is in a very basic level, leaving the majority of the analysis to the end user.

Analysis: The captured network data is taken at this point and its protocol is verified based on the information extracted, the analysis of the protocol's specific features is then made. One of the most popular open-source packet analyzers is Wireshark, which was originally named Ethereal. The name Wireshark was given in May 2006 due to trademark issues.

3. RELATED WORKS

Few researches have been conducted on the application areas of packet sniffing, especially in network security. A packet sniffer application for network security in Java was designed by [11]. In the study the C language application was rewritten in Java such that it could consume lesser memory, while performing the packet sniffing in a more efficient manner, providing information for the network administrator to enforce network security standards.

In a related development, an ethical network surveillance system using packet sniffing tools was developed [12]. The research findings showed that packet sniffers can be ethically used to monitor packets in a network and provide feedbacks for administrators to use in enforcing network security.

Similarly, a research on ethical network monitoring using Wireshark and Colasoft Capsa as sniffing tools was conducted [13]. The study showed that these tools could be useful in monitoring the activities of employees in a network and report captured packets to network administrators to enable them take proactive security measures against network security breaches by unscrupulous employees.

4. ASSUMPTIONS AND LIMITATIONS OF THE STUDY

a) Assumptions of the Study

This study assumes that an Intranet can be more secured if the network administrator has detailed information on the activities of the users and nodes in the network. The study also assumes that

packet sniffers can be used to provide the network administrator with information on the activities of the network to enable him take proactive measures to secure the Intranet.

b) Limitations of the Study

The study is limited in scope to packet sniffing using only one packet analyzer (Wireshark). A comparative use of other packet analyzers would have made it possible to determine which one is more efficient. In addition, the study was limited to just Intranets due to want of time and resources. An extension of the work to cover both Extranets and the Internet could have made it more worthwhile. However, the results obtained from the study can be generalized to other larger networks.

5. METHODOLOGY

The system was designed using five computer systems configured with static Internet Protocol (IP) addresses used in monitoring the IP traffic on the network by capturing and analyzing live packets from various sources and destinations in the network. The LAN was deployed on windows 8 with a D-link 16-port switch, category 6 Ethernet cable and other LAN devices. The Ebonyi State University Abakaliki Intranet was used in testing the system. The IP traffics were captured and analyzed using Wireshark Version 2.0.3. Four network instructions were used in the analysis of the IP traffic. It was intended to display the IP and MAC address sources and destinations of the frames, Ethernet, IP addresses, User Datagram Protocol (UDP) and Hypertext Transfer Protocol (HTTP).

a) System Design

Figure 3 shows the physical design of the system. Cables and other devices were linked to establish communication between five offices using an access point.

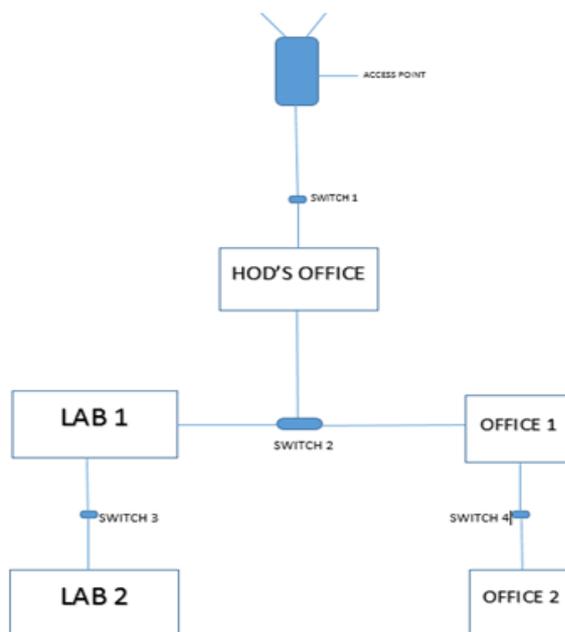


Figure 3: Physical Design of System LAN

Figure 4 shows the physical design of the Wireshark to sniff packets from five network nodes connected to a switch.

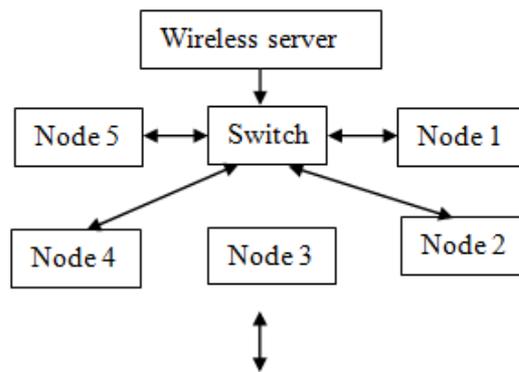


Figure 4: Physical Design of Wireshark

Before the implementation of wireshark, there must be an existing LAN. This is to ensure that different devices/systems are connected and are communicating with or without the internet. To ensure that connected devices are communicating with each other and to enable the network administrator to view and analyze activities in the network, the following steps were carried out:

- Crimping of cable
- Pinging
- File sharing

After launching the packet sniffer at the administrator's work station, it begins to capture packets on different applications such as web browsers and the File Transfer Protocol (FTP) client.

The sniffing process is as follows:

- Start
- Select capture interface
- Capture packets
- Set filter
- Stop capturing if no more streaming frames
- Save captured frames
- Analyze captured packets
- Generate report
- End.

Figure 5 shows the data flow model of the packet sniffing process. The user of the sniffed packets is the network administrator. The packet sniffer gets the IP address information from the user's system, generates reports to the network traffic system and analyzes the report, giving the user a feedback for appropriate action.



Figure 5: Data flow model of the packet sniffing process

Figure 6 shows the data flow model of the packet sniffer in the LAN. The packet sniffer generates the packet information, layers information, graphical representation of the information and presents the analysis.

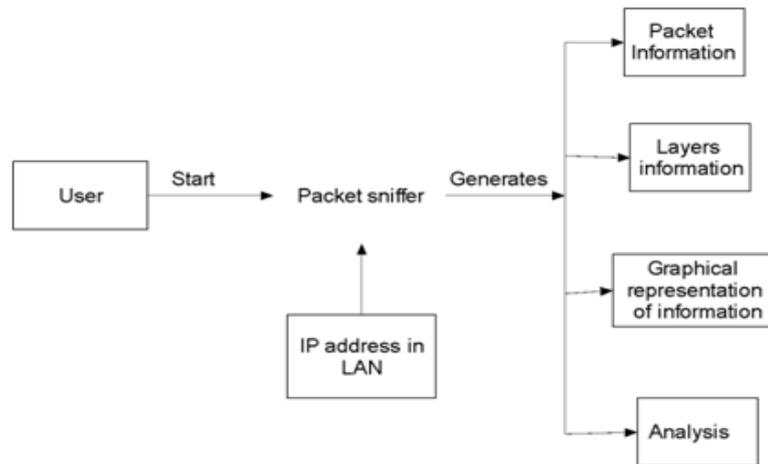


Figure 6: Data flow model of the packet sniffer in the LAN

The administrator must issue a pinging command to ascertain if there is communication between two or more systems after being connected through a bridge (switch). This is illustrated in Figure 7.

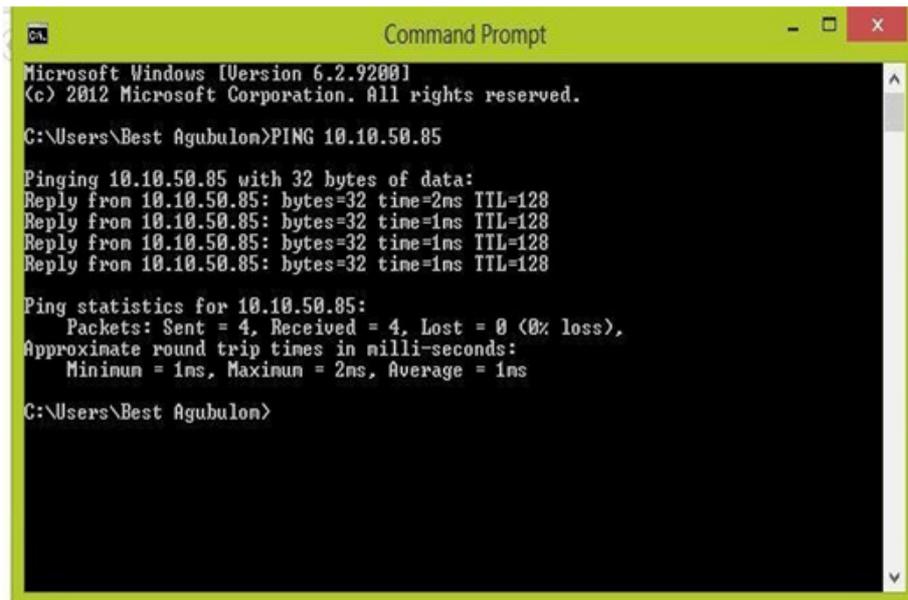
```

Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Best Agubalon>PING 10.10.50.85
  
```

Figure 7: Pinging command issued by an administrator

The outcome of the pinging is shown in Figure 8. All the pinged IP addresses are displayed.



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Best Agubulon>PING 10.10.50.85

Pinging 10.10.50.85 with 32 bytes of data:
Reply from 10.10.50.85: bytes=32 time=2ms TTL=128
Reply from 10.10.50.85: bytes=32 time=1ms TTL=128
Reply from 10.10.50.85: bytes=32 time=1ms TTL=128
Reply from 10.10.50.85: bytes=32 time=1ms TTL=128

Ping statistics for 10.10.50.85:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Best Agubulon>
```

Figure 8: Result showing pinged devices and feedbacks

This window in Figure 8 confirms the connectivity of the command “ping 10.10.50.85” that was issued, which simply means there is communication between the two devices and a reply from the recipient IP address 10.10.50.85.

b) System Requirements

The hardware required for the system include: personal computers, switches, Ethernet cables, interface cards, wireless access points, crimpers, trunks, a LAN tester, and an RJ-45 connector. The software components required for the system include Wireshark (packet sniffer), Wincap (to allow the network interface card to operate in ‘promiscuous mode’) and Windows 8 operating system.

c) Results and Discussion

The results obtained under testing the system are presented and discussed in this section. Figure 9 shows the user interface where the administrator initiates the packet sniffing process. The most common medium frequently used by network administrators to analyze network is ETHERNET.

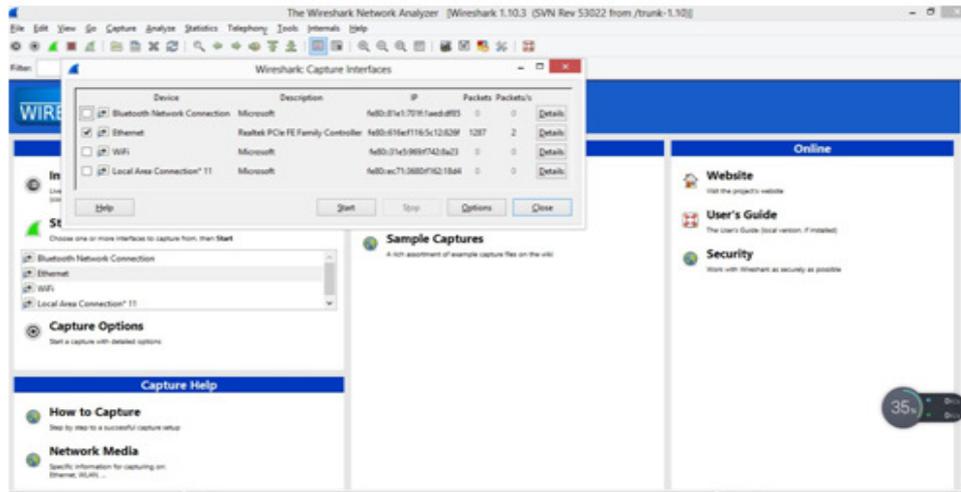


Figure 9: Wireshark user interface

The live data captured by the network sniffer showing random movements of different IP addresses of users on the network, from their sources to destination, the time, protocol, length and information on the network is illustrated in Figure 10

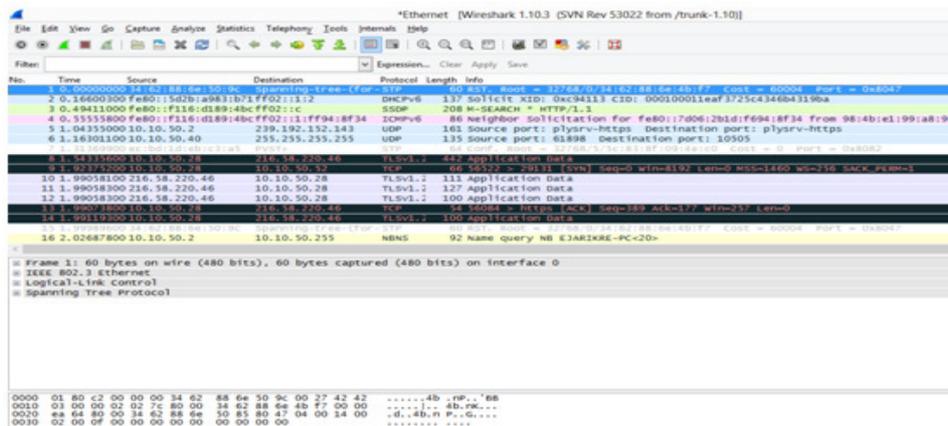


Figure 10: Captured packets

The interface in Figure 10 above shows packets running from different source IPs to destination IPs, their protocols, the time each went in, the length of data and the type of activities carried out by each user.

The captured traffic showing the frames involved, time in nanoseconds, source IP addresses and respective destination IP addresses, protocols involved, and the information depending on the activity of different hosts and length of data when the system was tested is illustrated in Figure 11. These aid the administrator to determine the system security and take necessary actions.

No.	Time	Source	Destination	Protocol	Length	Info
482	49.241309	10.10.50.92	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
483	49.418376	HewlettP_5478:58	Broadcast	ARP	60	who has 10.10.50.42? Tell 10.10.50.39
484	49.437384	Fe80::c599:2c62:ac9ff02::1:3		LLMNR	86	Standard query 0x37fe A isatap
485	49.736304	10.10.50.103	10.10.50.255	NBNS	92	Name query NB ISATAP<00>
486	50.242254	10.10.50.92	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
487	50.488799	10.10.50.103	10.10.50.255	NBNS	92	Name query NB ISATAP<00>
488	51.242471	10.10.50.92	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
489	51.715566	De117c:e7:51	Broadcast	ARP	60	who has 10.10.50.42? Tell 10.10.50.43
490	51.760748	pegatron_3f:e2:76	Broadcast	ARP	42	who has 10.10.50.42? Tell 10.10.50.47
491	51.761368	HewlettP_ed:a9:c9	Pegatron_3f:e2:76	ARP	60	10.10.50.42 is at a0:48:1c:ed:a9:c9
492	51.761793	10.10.50.47	10.10.50.42	TCP	66	56440 -> 80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
493	52.071097	10.10.50.43	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
494	52.243142	10.10.50.92	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
495	52.779891	10.10.50.43	10.10.50.255	NBNS	92	Name query NB ISATAP<00>
496	52.779409	Fe80::d9a3:e137:c8dff02::1:3		LLMNR	86	Standard query 0x37fe A isatap
497	52.779860	10.10.50.43	224.0.0.252	LLMNR	66	Standard query 0x37fe A isatap
498	53.001306	Fe80::d9a3:e137:c8dff02::1:3		LLMNR	86	Standard query 0x37fe A isatap
499	53.001925	10.10.50.43	224.0.0.252	LLMNR	66	Standard query 0x37fe A isatap

Frame 482: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
 Ethernet II, Src: AsustekC_2f:05:91 (38:2c:4a:2f:05:91), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
 Internet Protocol Version 4, Src: 10.10.50.92, Dst: 239.255.255.250
 User Datagram Protocol, Src Port: 65318 (65318), Dst Port: 1900 (1900)
 Hypertext Transfer Protocol

```

0000  01 00 5e 7f ff fa 38 2c 4a 2f 05 91 08 00 45 00  ..P...B.3/...E.
0010  00 0a 28 7b 00 00 01 11 64 48 0a 0a 32 5c e7 ff  ..(....8B..P..
0020  ff fa ff 26 07 6c 00 b6 d6 dc 4d 2d 53 45 41 52  ...&!....M-SEAR
0030  43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH * HTTP/1.1..H
0040  ef 54 3a 20 32 33 39 2e 32 35 35 0e 32 35 35  OSTS: 239.255.255
0050  2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20  _250:190 0..MAN:
  
```

Figure 11: Captured frames

6. CONCLUSIONS

Network security is a sine qua non for any organizational success, considering the value of data and information transmitted via networks. The Intranet though secured and restricted to authorized members of an enterprise that owns it is still prone to cyber attacks most times.

Certain activities in a network need to be critically watched to avoid security breaches. Such activities among others are: new user accounts, increased activity on a previously low usage account, new files with novel or strange file names, accounting discrepancies, changes in file lengths or dates, attempts to write to system, data modification or deletion, denial of service, unexplained, poor system performance, anomalies, suspicious probes, suspicious browsing, inability of a user to log in due to modifications of his/her account, etc.

This necessitates the use of some sniffing software to monitor the packets and activities in an Intranet.

The results obtained from the study showed the IP and MAC address sources and destinations of the frames, Ethernet, UDP and HTTP successfully captured. These can assist network administrators to make informed decisions on possible threats that the network can be exposed to.

ACKNOWLEDGEMENTS

The authors are grateful to the authorities of the Ebonyi State University Information and Communication Technology (ICT) Directorate for allowing us access to use the Intranet to test this work.

REFERENCES

- [1] Vikrant N., Ankush H. (2015). A Protocol Based Packet Sniffer. International Journal of Computer Science and Mobile Computing, 4(3), pp 406-410.

- [2] Gandh.C., Gaurav.S., Rishi.P.,Pupal.S., and Bhavya.K. (2014). Packet sniffer- A comparative study'. *International Journal of Computer Networks and Communications Security*, 2(5), 179- 187.
- [3] Fuentes, F., Kar, D. (2005). *Ethereal vs. TCP Dump: A Comparative Study on Packet Sniffing Tools for Educational Purposes*. *Computer Journal of Computing Science in Colleges*, 4(20), 169-176.
- [4] Pallavi A., Vishal S. (2013). *Network Monitoring and Analysis by Packet Sniffing Method*. *International journal of Engineering Trends and Technology (IJETT)*, 4(5), 2133-2135.
- [5] Mohammed, Q., Arshad, I., Mohammad, Z., and Misbahur, R. (2010). *Network Traffic Analysis and Intrusion Detection using Packet Sniffer*. *ICCSN Second international Conference, Ethiopia, 6-8 March*, 313-317.
- [6] Biswas, J. (2014). *An Insight into Network Traffic Analysis using Packet Sniffer*. *International Journal Of Computer Applications*, 94 (11), 39-44.
- [7] Mahesh, K, and Rakhi, Y. (2015). *TCP and UDP Packets analysis using Wireshark*. *International Journal of Science, Engineering and Technology Research (IJSETR)*, 4(7), 470- 474.
- [8] Rupam S. , Atul V., and Ankita, S. (2013). *An Approach to Detect Packet using Packet Sniffer*. 4(3), 21-33
- [9] Nagalakshmi, S. (2017). *Network Monitoring and Detecting Packets using Sniffing Method*. *International journal of Scientific and Engineering Research* 8(4), 41-44.
- [10] Pallavi A., and Hemlata P. (2012). *Network Traffic Analysis using Packet Sniffer*. *International Journal of Engineering Research And Applications*, 2(3), 854-856.
- [11] Otusile, O., Awodele, O., Ogbonna, A.C., Ajeagbu, C. and Anyeahie, A. (2013). *A Packet Sniffer (PSniffer) Application for Network Security in Java*. *Issues in Informing Science and Information Technology* 10, 389-400.
- [12] Ibrahim, D., Anwar, S. and Nagi, A.A. (2018). *Ethical Network Surveillance using Packet Sniffing Tools: A Comparative Study*. *International Journal of Computer Network and Information Security* 10(7), 12-22.
- [13] Nedhal, A.B. (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.

AUTHORS

Dr. Ogbu N. Henry is a Lecturer at the Ebonyi State University Abakaliki. He has a Ph.D. in Computer Science (Digital Emergency Response)



Dr. Moses Adah Agana is a Senior Lecturer and Head of Department of Computer Science in the University of Calabar, Nigeria. He has a Ph.D. in Cyber Security.

