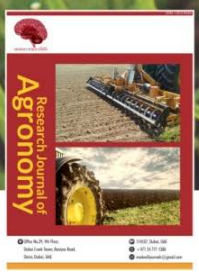
Research Journal of Agronomy

MEDWELL PUBLICATIONS



Local Area Network (LAN) Mock-up and the Prevention of Cybernetics Related Crimes in Niger Mills Company using Firewall Security Device

D.E. Bassey and J.C. Ogbulezie
Electronics and Computer Technology Unit, Department of Physics, University of Calabar, Calabar, Nigeria

Key words: Lan, firewall, wireshark, ethernet, networking

Corresponding Author:
D.E. Bassey
Electronics and Computer Technology Unit, Department of Physics, University of Calabar, Calabar, Nigeria

Page No.: 19-24
Volume: 11, Issue 4, 2017
ISSN: 1815-9354
Research Journal of Agronomy

Abstract: This study was conducted using the Local Area Network (LAN) of the Niger mills, Calabar, Cross River state, Nigeria. It entailed the simulation of LAN with a view to checking its quality, latency and also creating a firewall security device to mitigate the rate of cybercrime. A simulator-software (Packet tracer) was used to design, configure, troubleshoot and visualize network traffics within a controlled simulated program environment. The various components of the network were configured using commands and CISCO 3600 router. The design was also made up of 3 core layer switches with 24 ports each, and 44 computer systems connected to them. Other key items were: hubs, repeaters and two servers that served as system backups. Various computer systems were configured using the Class C IP addressing system. The packets captured on the Niger mills network were analyzed based on the application protocol and the transport protocol. From the study, it was observed that web browsing (HTTP) constituted the highest traffic with 42.9%. This was followed closely by SMPT/POP with 28.9% and the FTP with 16.39%. Others were the DNS with 10.41% and SMB with 1.3%. Further findings indicated that the created firewall into the LAN network was able to prevent intruders and screened unauthorized users from accessing the system. In addition, firewall was able to filter incoming network traffic based on source or destination, filter outgoing network traffic based on source or destination, filter network based on content, detect and filter mal ware, make internal resource available, report on network traffic and firewall activities. This is in line with what Hooke assertions when he conducted a similar simulation using firewall to check the rate of cyber crime in a WAN. Traffic activities of the network were monitored and reported. In order to ensure routine system checkup and to further curb the problem of latency, a qualified

network administrator should be hired to manage the network. Further studies should be carried out using a more sophisticated software application (OPNET) in simulating the different networks (LAN, MAN, WAN).

INTRODUCTION

Computer system networking is a facet of information and communication technology which dealswith the interconnection of cybernetics machines (computers, servers, Personal Digital Assistant (PDAs), etc.) for the purpose of sharing data at a dramatic speed within a given area. Information and communication systems use telecommunication network and other electronic devices for effective and efficient data transfer. The technological ingenuity snow-balled further in to computer networking and multimedia (music, video, pictures and documents or packets). This is against the backdrop that manual transfer of information takes a considerable amount of time to deliver; which more often than not results in information loss. These laudable trend shave resulted to the realization of the "global village" propounded by Mcluhans some years back.

Thus, networking plays a vital role in our everyday life and has reduced the stress and cost involved in the transfer of information (Patterson and Hennessy, 2008). This innovation has become a vital tool in governments, businesses, industries, education, healthcare, etc., to provide a panacea to information glitch hitherto caused by administrative bottle-neck. Conversely, cybernetic crimes has bedeviled the enormous benefits of networking as hackers now pry on closed/open network system to carryout illegitimate activities that are inimical to the underpinning philosophy establishing global networking. Predicated upon this ugly fact, the study deemed it necessary to undertake this simulation with a view to curbing cyber related crimes through firewall security system.

Several switching techniques used to transfer information over the network such as Local Area Network (LAN), Metropolitan Area Network(MAN), Wide Area Network (WAN), Global Area Network(GAN), etc. were considered using firewall security system on LAN simulation. LAN is a simple network that covers a small geographical area with the aim of communicating, exchanging information and sharing resources within the specified area. The small geographical area could be offices, campuses, banks, administrative blocks, etc.

Brief review on computer networking: Computer networking is an interconnection of two or more computers with the view of sharing resources. The resources shared are both hardware and software such as:hardwires devices, CD-ROMs, data files, fax services, printers and backup services. The functions of computer networking include.

Access to shared resources: Since, networking enables sharing of resources, it reduces cost of computer hardware in organizations. Hardware and software devices could be bought in low quantities and shared with all other users on the network.

Ability to communication with others: Computer networking helps in providing the communication infrastructure necessary to communicate with each other. It provides services such as Internet access, E-mail, etc. Computer networking is made possible by the network medium which connects the various devices in the network. There are basically three forms of network media in which data are transmitted. They are:

Copper cable: For copper medium, signals are represented in the pattern of electrical pulses.

Optical fibre cable: This cable usually comes in two modes, the single mode optical fibre and the multi-mode fibre. However, the Single Mode (SM) optical fibre cable is usually preferable because it carries signals over a longer distance compared to the multi-mode type. The optical fibre cable carries signals represented as patterns of light pulses.

Wireless: This is a standard given by the Institute of Electrical and Electronic Engineering (IEEE-802.11). This medium represents signals using radio transmission or microwave technology.

LAN fundamentals: The term Local Area Network (LAN) refers "to a computer network covering a small physical area like a home, office or a small group of buildings. LAN has the basic featureof higher data transfer rates, small geographical coverage and requires minimal telecommunication facility.LAN has three different connectivity approaches: ethernet, token ring and Fibre Distributed Data Interface (FDDI). However, to ensure effective connectivity, ethernet technology was used in this work. Ethernet works on all network operating systems and provides services in the physical and data link layer of the Open System Interconnection (OSI) model. Ethernet uses a technique access called the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to control the flow of information over transmitted data. In the course of this, checks are conducted if there is on-going transmission on the network and when none is discovered,

the Ethernet network interface card transmits the available data. However, any transmission was detected, the NIC does not transmit to avoid collision. When the NIC senses a collision, it transmits a collision signal to alert other NICs to stop transmission. Such interrupted transmission resumes after a period of time. Ethernet supports data transfer rate of 10 to 100 Mbps using any of the prescribed cables (Wood, 2010).

MATERIALS AND METHODS

Network components of LAN: All networks require four components to enable the nodes within it to communicate with each other in order to inter-change information. These componentsare: transmission media, hardware devices, rules and standards or protocols and software components in form of network operating systems and applications. In this work, network hardwaresuch as router was configured using the command line interface, while Class-C type IP addresses were assigned to end user devices like printer, PCs and server as shown (Fig. 1).

Router configuration:

- Router; enable
- Router; configure terminal
- Router (configure); Hostname DEB-LAN
- DEB-LAN (configure); line console O
- DEB-LAN (configure-line); password password
- DEB-LAN (configure-line); login
- DEB-LAN (configure-line); line Vty 0 4
- DEB-LAN (configure-line);password password
- DEB-LAN (configure-line); login
- DEB-LAN (configure-line); exit
- DEB-LAN (config-line); interface fastEthernet 0/1
- DEB-LAN (config-line); ip address 192.168.10.1 255.255.255.0
- DEB-LAN (config); no shutdown
- DEB-LAN (config); interface se 0/0/0
- DEB-LAN (config); ip address 192.15210.1 255.255.255.0
- DEB-LAN (config-if); # exit

Open System Interconnection Model (OSI): The Open System Interconnection mode is a set of guidelines which enables manufacturers to design and implement network equipments so that they can reliably communicate with each other. The International Standards Organization (ISO) developed a network architecture standard called the Open System Interconnection model (OSI), (Wood, 2010).

The OSI reference model is a seven-layer structure. All signals that originate from any node begin from the topmost layer and ends at the layer 1 where all the transfer of data occurs. Table 1 below shows the 7 layers of the OSI models.

Firewalls security device: James and Keith (2010a, b) believes that firewall examines traffic as it enters one of its interface and applies rules to the traffic-in essence, permitting or denying the traffic based on these rules. The

Fig. 1: Router fully configured to perform its action

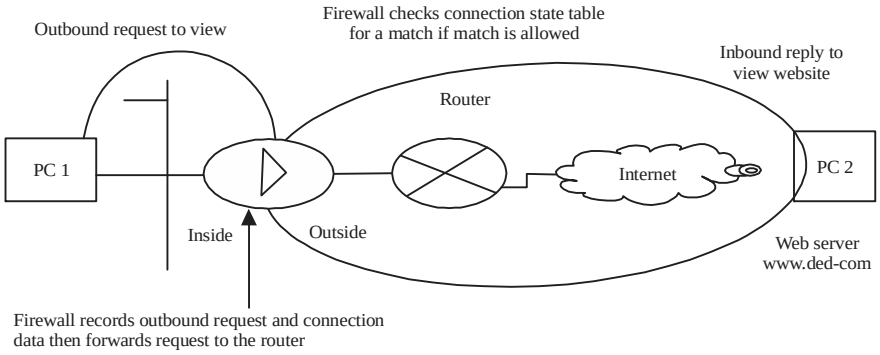


Fig. 2: Firewall in operation in LAN

Table 1: The seven layers of the OSI models

Layers	OSI models (layer)
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data-Link
1	Physical

critical dual purpose of packet inspection and filtering of packets is one of the most fundamental responsibilities of a firewall. The following list includes the most common rules and features of firewalls:

- Filter incoming network traffic based on source or destination
- Filter outgoing network traffic based on source or destination
- Filter network based on content
- Detect and filter malware
- Make internal resource available
- Report on network traffic and firewall activities

Figure 2 shows an illustration of firewall operation in the simulated LAN.

Sequence of operation of Firewall in the simulated LAN: PC 1 is a computer system (deb-pc) that opens a web browser and wants to view a web page from the www.deb.com web server. This action causes PC1 to send the request for "view this web page" out through the firewall across the internet and to the web server. The firewall sees the request originated from PC1 and is destined for www.deb.com. The firewall records the outbound request and expects that the reply will come only from the www.deb.com web server. The session marker placed in the firewalls session, start table that tracks the communication process from start to finish. Connection metrics such as time opened and so forth, are displaced with the marker in the session start-table-record maintained by the firewall. The www.deb.com web server replies to the web page request from PC1 which is transmitted back through the terminal to the firewall. The firewall checks its session state-table to see whether the metrics being maintained for this session match the outbound connection.

Niger mills LAN network design: This method involved the use of a packet application called Wire-shark. The application was used on the Niger mills network to capture packets on the Network Interface Card (NIC) of some users on the network to be able to monitor their activities on the network based on the protocols they were using at that given time. The software (WIRE-SHARK) decoded packets contents of the interface for readability. Its output was analyzed and the user behavior on the network was characterized based on the WIRE-SHARK output.

The design of this network described briefly the physical connection of the systems used at the Niger Mills LAN network. It represented the physical layout of the device on the network. The study reviewed and re-designed the Niger mills network using the star topology.

Network communication among the VLANS was made possible using a Cisco 3600 router. Based on this framework, the design was made using three core layer switches with 24 port Cisco catalyst 2950 switch model. While the distribution and access switches were D-link switches with the link speed being 100 Mb/s. The network had a total of 44 systems inter-connections.

With the assistance of the company's profile and ICT staff, the various offices were networked in line with the numbers of users and number of computers needed. The Information Technology office was chosen as the suitable location where the server was kept for safety purposes. Fig. 2 shows an illustration of the simulated LAN network.

RESULTS AND DISCUSSION

The packets captured on the Niger mills network was analyzed based on the application protocol, the transport

Fig. 3: Showing simulated LAN using Cisco Packet Tracer

Table 2: Analysis of packets based on application protocol

Protocol	No of packets (bits)	Percentage of packets (%)
HTTP	31,542	42.90
FTP	12,055	16.39
SMB	960	1.39
SMTP/POP	21,300	28.90
DNS	7,653	10.41

Total number of application packets: 73,510 bits

Table 3: Analysis of packets based on transport protocol

Protocol	No of packets (Bits)	Percentage of packets (%)
TCP	114,130	69.30
UDP	23,220	14.10
ARP	10,960	6.66
STP	15,603	9.48
CDP	710	6.43

Total number of packets: 164623 bits

protocol and also protocols used to determine the path to the destination of the packets. The application protocols was used to determine the user behavior and the type of application the packet was holding. Examples of application protocols used were the Hypertext Transfer Protocol (HTTP) used for identifying web pages, File Transfer Protocol (FTP) used in file sharing between two systems, Simple Mail Transfer Protocol (SMTP) which was used for the transfer of e-mails, Post Office Protocol (POP), which was used for receiving e-mails and Server Message Block (SMB) also used for file sharing.

On the other side, the transport protocol defined how the packets were transmitted across the network. Examples of these protocols used were Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Transmission of packets can be done by either using a reliable protocols or an unreliable protocol. Reliable protocols ensured that packets were safely delivered to their destinations by creating a connection-oriented session which gives feedback on whether a message is received by a destination and also allowed for retransmission of host packets.

From the study conducted, it was noted that unreliable protocols do not guarantee safe delivery of packets to their destinations and also do not give account of host packets or packets with error. TCP is therefore considered very reliable while UDP is unreliable.

Table 2 and 3 show the analyses of the packets captured based on the WIRESHARK output for the application and transport protocol used to locate the best path to the destination. Table 2 shows the various application protocols associated with the packets captured and the number of application packets relative to the total number of application packets captured.

In Table 3 gives the transport protocols and other protocols used in determining the best path a packet can take to its destination, the number of packets associated with each protocol and the percentage of packets relative to the total number of packets captured.

Packets usually contain more than one protocol, for example, a TCP packet can be a web page which also makes it an HTTP (this explains why there were more packets. The other packets seen in the captured output define the protocols such as Address Resolution Protocol (ARP) which ensured that there was only one logical path for all destinations on the network. All these protocols worked together to define the best path a packet took to its destination.

Figure 3 and 4 give a comparative graphical representation of the analysis carried out from the results obtained by this study. From Fig. 3, it showed that web browsing (HTTP) constituted the highest traffic with 42.9%. This was followed closely by (SMPT/POP) with 28.9% and the FTP with 16.39%. Others were the DNS with 10.41% and SMB with 1.3%. It was observed from the result that most of the users of the network were interested in viewing web pages, sending and viewing messages while less downloading and uploading of files were done.

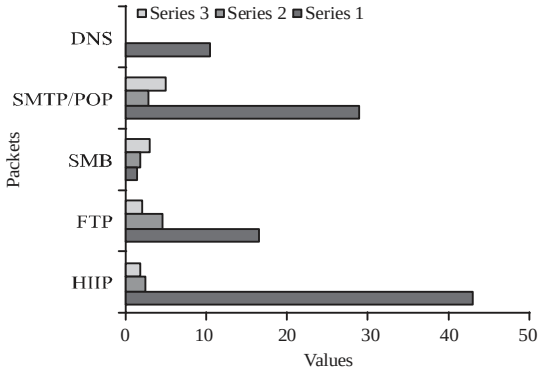


Fig. 4: Bar chart showing analysis of packets based on user application protocol

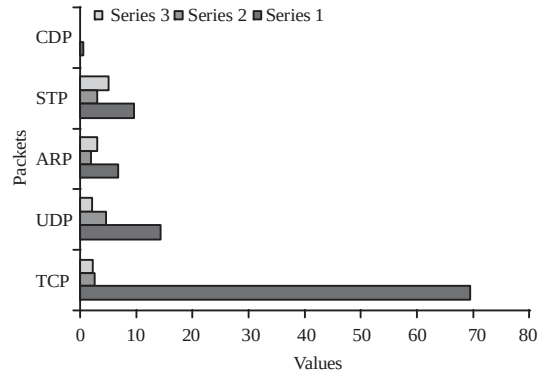


Fig. 5: Bar chart showing analysis of packets based on transport protocol

In Fig. 4, it was observed that the TCP dominated the traffic with 69.3% which means more of web browsing, sending and receiving of mails and more uploads and downloads of files were done in the network than in other applications. UDP constituted 14.10% of the network traffic. Thus, there were little or no video streaming and music sharing on the network. The remaining 6.62% was generated from ARP, STP and CDP. These protocols defined the best path in which the packets could get to its destination.

It was also observed that the network was designed in such a way that all the links connecting the core distribution and layer switches were operating on the same bandwidth of 100 Mbp. Another factor that affected the network performance was the fact that Niger mills was making use of a remote domain name server which was referred to as DNS (meaning that the name server is not situated at Niger mills Calabar). Hence, for name resolution to be performed, packets have to be transferred to the remote server. Querying it to examine and resolve issues took time and space; thereby adding delay to the network and slowing the network. It was also noted that viruses could be one major factor that consumed the available bandwidth, thereby resulting to a lower network performance which was one major hindrance encountered by the study. In order to resolve most of these unpleasant operational issues regular scan of all the relevant system parameters on the network was performed.

CONCLUSION

The process of planning and designing a Local Area Network must be based on visibility study of a workable topology, cabling media, speed, etc. All these factors must be considered in order to create a suitable network design. From the results of the findings, it was observed that firewall was able to prevent intruders and to screen unauthorized users from accessing the system without the the authorization of the administrator. Further to this, firewall was able to filter incoming network traffic based on source or destination, filter outgoing network traffic based on source or destination, filter network based on content, detect and filter mal ware, make internal resource available, report on network traffic and firewall activities. This was in line with what Hooke (2000) asserted when he conducted similar simulation using firewall to check the rate of cyber crime in a WAN. The study noted that firewall performed these functions without any glitch. Similarly, the study recommended VLAN and Firewall as a tool for cyber crime prevention. The study further recommended the practice of effective maintenance as an antidote for reliable and efficient network by network administrators.

REFERENCES

Hooke, A., 2000. Interplanetary internet. InterPlanetary Networking Special Interest Group (IPNSIG), USA.

James F.K. and W.R. Keith, 2000a. High Speed Networking: A Systematic Approach to High Bandwidth Low-Latency Communication. Kluwer Academic Publishers, Amsterdam, Netherlands,.

James, F.K. and W.R. Keith, 2010b. Computer Networking: A Top-Down Approach Featuring the Internet. 5th Edn., Pearson Education, London, UK., Pages: 864.

Patterson, D.A. and J.L. Hennessy, 2008. Computer Organization and Design: The Hardware/Software Interface. 4th Edn., Morgan Kaufmann Publishers Inc., San Francisco, CA., USA., ISBN-13: 978-0123744937, Pages: 912.

Wood, J.A., 2010. The darknet: A digital copyright revolution. Richmond J. Law Technol., Vol. 16, No. 4.