Local Area Network (Lan) Mock-Up And The Prevention Of Cybernetics Related Crimes In Nigermills Company Using Firewall Security Device

Authors:

Donatus E. Bassey, Julie C. Ogbulezie, Effiom, E. O.

ABSTRACT

This study was conducted using the Local Area Network (LAN) of 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 traffic within a controlled simulated program environment. Various computer systems were configured using the Class C IP addressing system. The packets captured on the Niger Mills network were analyzed based on application and transport protocol. From the study, it was observed that web browsing (HTTP) constituted the highest traffic with 42.9 per cent. This was followed closely by SMPT/POP with 28.9 per cent and the FTP with 16.39 per cent. Others were the DNS with 10.41per cent and SMB with 1.3per cent. Further findings indicated that creating and activating firewall into the LAN network was able to prevent intruders. It also 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 malware, make internal resource available, report network traffic and firewall activities. Further studies should be carried out using a more sophisticated software application (OPNET) in simulating the networks

Key Words: LAN, Firewall, Wire-shark, Ethernet and Networking

Electronics and Computer Technology Unit,

Department of Physics,

Faculty of Science,

University of Calabar, Calabar

Cross River State,

Nigeria.

1. INTRODUCTION

Computer system networking is a facet of Information and Communication technology that deals with the interconnection of cybernetics machines. It is involved in the process of sharing data at a dramatic speed within a given area. Information and Communication systems use telecommunications network, and other electronic devices for effective and efficient data transfer. This technological break-through led further to computer networking and multimedia (music, video, pictures and documents or packets). As observed by Bassey, D.E. et al., 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 trends have 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, 2008). This innovation has become a vital tool in governments, businesses, industries, education, healthcare, etc. Conversely, cybernetic crimes has bedeviled the enormous benefits of networking, as hackers now pry on closed / open network system to carry out illegitimate activities that are inimical to the philosophy establishing global networking. Predicated by this fact, the study carried out mock-up model of Niger Mills network, by simulating the networking-content of the cooperation, and creating Fire-walls; in order to examine the activities of Fire-walls in monitoring and curbing cyber related crimes.

2.0 Research Methodology.

2.1 LAN Components of Niger-Mills

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 Nigermills network using the star topology.

Network communication was achieved using a Cisco 3600 router. Based on this framework, the design was made using three (3) core layer switches with 24 port Cisco catalyst 2950 switch model. While the distribution and access switches were D-link switches; using link speed of 100Mb/s. The network had a total of 44 systems inter-connections.

With the assistance of the company's profile and ICT staff, various offices were networked in line with the number 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. Figure 2 below shows an illustration of the simulated LAN network. The network has four components to aid in both-way communication flow. The components were: transmission media, hardware devices, rules and standards, or protocols and other software components (network operating systems and applications). The project configured network hardware facility such as router; through the command line interface; while Class-C type IP addresses were assigned to end user devices like

printer, PCs and server.

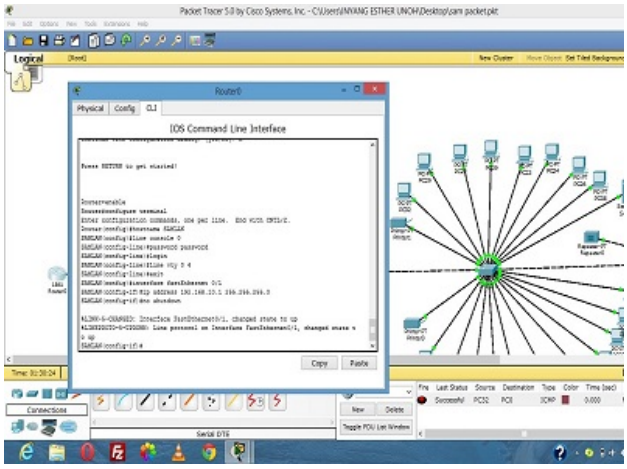

Figure 1: Showing router fully configured to perform its action

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 2 55.255. 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), (Jessica, 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.

Table 1: The seven layers of the OSI models

Layer 7	Application Layer
Layer 6	Presentation Layer
Layer 5	Session Layer
Layer 4	Transport Layer
Layer 3	Network Layer
Layer 2	Data-Link Layer
Layer 1	Physical Layer

2.2 Firewalls Security Device

James (2010) believes that firewall examines traffic as it enters one of its interface. In the course of this, it applies rules to the traffic, and in essence, permits or denies the traffic in line with these rules. The 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.

a. Filter incoming network traffic based on source or destination.

b. Filter outgoing network traffic based on source or destination

c. Filter network based on content

d. Detect and filter malware

e. Make internal resource available

f. Report on network traffic and firewall activities.

2.3 Sequence of operation of Firewall in the simulated Niger-mills LAN

1. 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.

2. The firewall sees the request originated from PC1 and is destined for www.deb.com

a. The firewall records the outbound request and expects that the reply will come only from the www.deb.com web server.

b. The session marker placed in the firewalls session, start table that tracks the communication process from start to finish

c. Connection metrics such as time opened are displaced with the marker, through the session start-table-record maintained by the firewall.

3. The www.deb.com web server replies to the web page request from PC1, which is transmitted back through the terminal to the firewall.

4. The firewall checks its session start-table to see whether the metrics being maintained for this session match the out-bound connection.

2.4 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). Those NIC, were those users already on the network; in order to monitor their activities in accordance with existing protocols at that given time. The software (WIRE-SHARK) decoded packet-contents of the interface for readability. Its output was analyzed and the user behavior on the network was characterized by the WIRE-SHARK output.

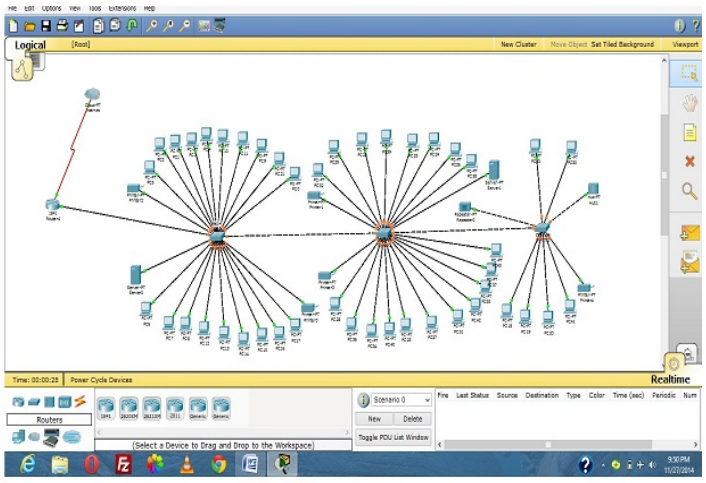

Figure .2: Niger-mills simulated LAN using Cisco Packet Tracer

3.0 RESULTS AND DISCUSSION

3.1 Interpretation of Results

The packets captured on the simulated Niger-mills network, was analyzed using the application protocol and the transport protocol. In addition, the protocols used to determine the path to the destination of the packets was also applied. The application protocol 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 the 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 re-transmission 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. TCP was therefore applied.

Tables 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: Analysis of packets based on application protocol

Total number of application packets: 73,510 bits

Protocol	No of Pkts(Bits)	Percentage of Packets (%)
HTTP	31,542	42.9
FTP	12,055	16.39
SMB	960	1.39
SMTP/POP	21,300	28.9
DNS	7,653	10.41

TABLE 3: Analysis of packets based on transport protocol

Total number of packets: 164623 bits.

Protocol	No of Pkts (Bits)	Percentage Of Packets (%)
TCP	114,130	69.3
UDP	23,220	14.10
ARP	10,960	6.66
STP	15,603	9.48
CDP	710	6.43

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.

Table 3 gives the transport protocols and other protocols used in determining the best path a packet can take to its destination. Also determined were 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 in Table 3 than Table 2). 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.

3.2 Discussion of Findings

Figures 3 and 4 give a comparative graphical representation of the analysis carried out from the results obtained by this study.

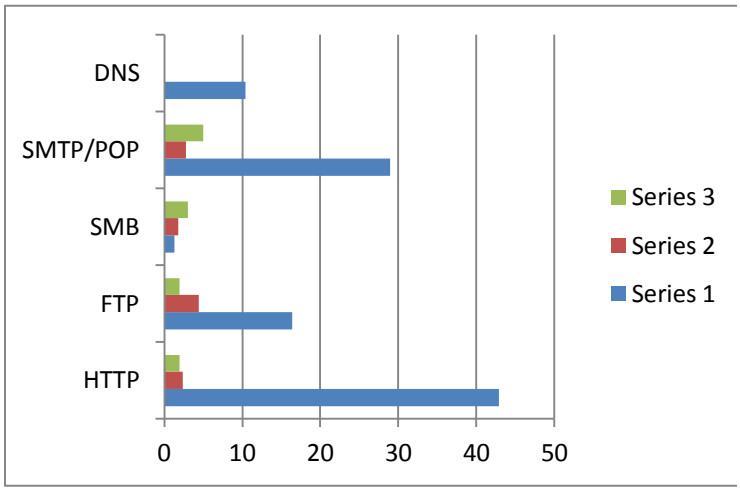

Figure 3: Bar chart showing analysis of packets based on user application protocol

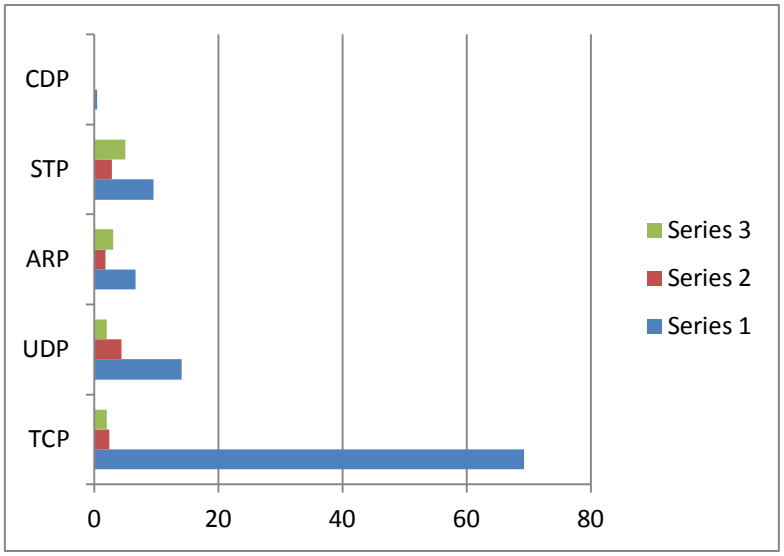

Figure 4: Bar chart showing analysis of packets based on transport protocol

Figure 3 shows that web browsing (HTTP) constitute the highest traffic with 42.9 per cent. This was followed closely by (SMPT/POP) with 28.9per cent, and FTP with 16.39 per cent. Others were DNS with 10.41 per cent and SMB with 1.3 per cent. 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 down loading and up loading of files were carried out.

In Figure 4, it was observed that TCP dominated the traffic with 69.3 per cent. This means more web browsing, sending and receiving of mails, and more up-loads and down-loads of files were carried out in the network than in other applications. UDP constituted 14.10 per cent of the network traffic. Thus, there were little or no video streaming and music sharing on the network. The

remaining 6.62 per cent was generated from ARP, STP and CDP. These protocols defined the best path in which the packets could get to its destination.

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 (100Mbp). Another factor that affected the network performance was the fact that Niger-mills was making use of a remote domain-named 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 were 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 unveiled that viruses contributed to lower bandwidth availability; which resulted to lower network performance. This issue 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.

4.0 CONCLUSION

The process of planning and designing a Local Area Network must be based on visibility study of a workable topology, distribution cables, 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 also screen unauthorized users from accessing the system. This property was demonstrated as the configured firewall filtered all incoming network traffic in line with their sources or destinations. It also filtered network elements, detect and filter malware, make internal resource available, remit reports 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 cybercrime in a WAN environment. The study noted that firewall performed these functions without any glitch. Similarly, the study recommended VLAN and Firewall as a tool for cybercrime prevention. The study further recommended the practice of effective maintenance as an antidote for reliable and efficient network by network administrators.

REFERENCES

[1.] Bassey, D. E., Ogbulejie, J.C., Okon, B. E (2016). Modelling a Low Latency IP Network in Nigeria. IJSETR, Vol.15, Issue 3, 830-834.

[2]. David A. Patterson (2008). Computer Organization: Hardware/Software Interface, 4th Edition.

[3] Geoffrey M. Voelker (2009): Characterizing user behavior and network performance in a public wireless LAN. Proceedings of the 2009 IEEE international conference on communication, 1287-1291.

[4]. Hooke, A. (2000), Interplanetary Internet, Third Annual International Symposium on Advanced Radio Technologies, retrieved 2011-11-12.

[5]. James F.K, Keith W.R. (2010): Computer Networking: A Top-Down Approach featuring the internet (5th Edition).

[6]. James F.K, and Keith W.R. (2000). High Speed Networking: A systematic Approach to High Bandwidth low-latency communication.

[7]. Wood, Jessica (2010). “The Darknet: A Digital Copyright Revolution”. Richmond Journal of Law and Technology 16 (4). Retrieved 25 October 2011.