Developing a Good Cybersecurity Awareness in Tertiary Institutions - A Prerequisite to Robust Cyberspace in COVID-19 Pandemic Epoch

Etim Emmanuel Okon & Ogbonna, Akobundu I.
Department of Computer Science,
Abia State Polytechnic, Aba, Nigeria

Etuk Enefiok A.
Department of Computer Science,
Michael Okpara University of Agriculture,
Umudike, Nigeria

Abstract
The corona virus has made online solutions inevitable and will remain so for a long time due to convenience and personal safety especially in institutions of higher learning. This work was motivated by the need to create awareness on privacy, data protection and security where these tools are pooled together to help school management maintain robust networks in our tertiary institutions. Staff, students, applicants, contractors, government agencies and others are constantly bombarding institutions networks, thereby continually creating a pool of data and information within the network. The aim of this paper therefore is to provide a clear understanding of these tools for a robust network with enhanced data protection, privacy of information maintenance and most importantly a secured network environment. This paper discuses some of the cybersecurity techniques/tool, their applications in tracking and stopping the nefarious activities of attackers to our networks - countermeasures and impacts. It will be pertinent to note that a sound knowledge of cybersecurity techniques by staff and students in our tertiary institutions will be sine qua non for safeguarding our cyber space against theft, hacking and damages of data, information, software, hardware and disruption or misdirection of system services, fighting cybercriminals and keeping the necessary confidentiality on our data and information.

Key words: *Cybersecurity, Awareness, Tertiary Institutions, Robust, Cyberspace, COVID_19*

I. INTRODUCTION

Cybersecurity and Infrastructure Agency (2019) adduced that the 2019 NCSAM (National Cybersecurity Awareness Month) theme captioned "Own IT. Secure IT. Protect IT." was a campaign designed to encourage all citizens to be safer and more personally accountable for using security best practices online. The campaign provides material on a wide variety of security topics including: Social media safety, Updating privacy settings, Awareness of device application security, Keeping software up-to-date, Safe online shopping, Wi-Fi safety and Protecting customer data.

In Nigerian Tertiary Institutions, the absence of a national cyber security policy for students, staff, vendors and others to institution's network is done based on the financial, technological, skills and necessity of individual schools. In April, 2020 many realized that schools may be close for a longer period and the need for alternatives. Despite the industrial action of the Academic Staff Union of University (ASUU) many tertiary institutions both private and public decided to embark on online lectures and provision of other services to

staff and students using the cyber space. Compared with western countries, the Federal Ministry of Education's school-closure directive did not produce guiding principle on how to ease learning disruptions for students and how to handle the digital means of learning which may be alternative method to physical teaching learning process in the dynamic society together with the enormous traffic on the school's network and the attendance security implications.

The index case of Covid-19 in February, 2020 was the advent of spread of this deadly disease in Nigeria. According to Ajisegiri, Odusanya & Joshi (2020) Nigeria is one of the 210 countries affected globally. The first case was confirmed in Lagos State on 27 February 2020. This index case was a 44-year-old man, an Italian citizen who returned from Milan, Italy, on 24 February and presented at a health facility on 26 February 2020. It did not take the Federal Government long to realize the challenges that our dear country is into. The setting up of the Presidential Task Force (PTF) on Covid-19 culminated to several initial decisions to be taken by the government. One of these painful but necessary decisions was the shutting down of all tertiary institutions in the country to check the spread of this pandemic. March 19th, 2020 was the turning point when a circular from Federal Ministry of Education granted an approval for the shutting of all school for a period of one (1) month beginning from Monday 23rd March 2020 to prevent the spread of the Corona virus (COVID-19). Many thought the shutdown will last for about a month. Adelakun (2020) observed that the severe short-term disruption is felt by many families around the world: home schooling is not only a massive shock to parents' productivity, but also to children's social life and learning. Teaching is moving online, on an untested and unprecedented scale. Student assessments are also moving online, with a lot of trial and error and uncertainty for everyone. Many assessments have simply been cancelled. Importantly, these interruptions will not just be a short-term issue, but can also have long-term consequences for the affected cohorts and are likely to increase inequality.

Academic records for thousands of students are generated on daily bases and students are also permitted to access their records online, staff records are moved from one department to another for emoluments, promotions and trainings, outsiders such as admission applicants and contractors are granted certain privileges to information on the school websites, and finally academic staff utilize the network for intellectual articles. The ability to provide adequate privacy, data protection and security to our networks becomes an important issue due to type of persons who access the network, the volume of data generated and limitations to unauthorize information. According to Cisco (2020) the first dimension of the cybersecurity cube identifies the goals to protect cyberspace. These goals identified in the first dimension are the foundational principles. These three principles are confidentiality, integrity and availability. The principles provide focus and enable the cybersecurity expert to prioritize actions when protecting any networked system. Confidentiality prevents the disclosure of information to unauthorized people, resources, or processes. Integrity refers to the accuracy, consistency, and trustworthiness of data. Finally, availability ensures that information is accessible by authorized users when needed. Use the acronym CIA to remember these three principles.

A network security system combines numerous layers to address network security across an institution. The first layer enforces network security through a username/password mechanism allowing only authenticated users with customized privileges to access the network. A user who has been granted access into the network system requires the network policies that are enforced by the network's configured firewall which restricts a user to particular services. The configuration software, however, cannot detect or prevent viruses and

malware which is harmful to the network leading to loss of data. Antivirus software or an intrusion prevention system (IPS) is therefore integrated into the network security as the second layer to prevent viruses and other harmful malware from attacking the network.

The state of data in our institution's network requires substantial knowledge in order to safeguard them. These network systems domains consist of a considerable amount of critically important data which must be protected for confidentiality, integrity and availability. Data in a network system is possible in these three states, data in transit, data at rest or storage and data in process.

Types of skills and disciplines used to provide privacy, data protection and security cannot be over emphasis. The first skill includes the technologies, devices, and products available to protect information systems and fend off cyber criminals. There are numerous challenges confronting online platform in Nigeria ranging from unstable and poor supply of electricity to power computers and it peripheral, smartphones, network equipment, etc. Inadequate knowledge of the cyber space by most students and staff, and high cost of data services to Internet access is another challenge confronting services in Nigeria. The knowledge and understanding of the cyber space by staff and students especially, the safeguard against various malicious activities therein due to high internet traffic is what we will be discussing on this paper.

II. RELATED LITERATURE

Before the advent of corona virus, a report from an online chronicle, institutions websites were hacked and the servers hosting both websites and emails put out of control. Other incidents, with motives ranging from fraud to political or protest action and ransom, have been reported at universities in Algeria, Egypt, Morocco, Kenya, Nigeria, Botswana, Uganda, Ghana and South Africa (Ajisegiri et al, 2020)

From the above, one sees the embarrassing posture of vulnerability of cyberspace in most African Universities; hence the position of the Nigerian Agencies and individual higher institutions trying to implement various solutions to safeguard their cyberspace and the call by many for a collaborative action for enhanced national cybersecurity framework in Nigeria.

The Concept of Cybersecurity

Cisco (2020) defined Cybersecurity as the practice of protecting systems, networks, and programs from digital attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cyber security measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

Cybersecurity also known as information technology security or electronic information security and applicable in diverse contexts including business, mobile computing implies that computers, mobile devices, networks, servers, electronic devices and most important data must be protected from malicious attacks. This concept can further be characterized into network security, application security, information security, operational security, disaster and business continuity, and End-user education.

Cavelty (2012) said Cyber-security is both about the insecurity created by and through this new place/space and about the practices or processes to make it (more) secure. It refers to a set of activities and measures, both technical and non-technical, intended to protect the bioelectrical environment and the data it contains and transports from all possible threats.

The Australian Cyber Security Center (ACSC) according to Oladimeji et al (2019) recommends that multi-factor authentication be implemented for users using remote access

solutions, users performing privileged actions and users accessing important (sensitive or high availability) data repositories.

University information systems have become ideal targets for hackers; this is because the systems contain sensitive personal data as well as abundance of intellectual property from researchers. In many ways, colleges and universities experience the same data security breaches major corporations do (Cavelty, 2012).

Personnel handling data need to how data are collected, stored, and protected. Beaudin (2015) stated that responsible personnel need to know their role in incident response in case of data vulnerability. All people on the campus handling data need to know their role in data safety, including administrators, faculty, staff, researchers, and students (Mello, 2020). Practices include password, authentication, access, and portable issues; bring your own device (BYOD) which is common in tertiary institutions. Communication is a crucial element of a successful plan – everyone needs to know his or her particular role in preventing a breach and reacting to a breach. Adequate knowledge in cyber security is the antidote and necessary approach to securing the cyber space in our institutions.

Recent Cyber Security Issues

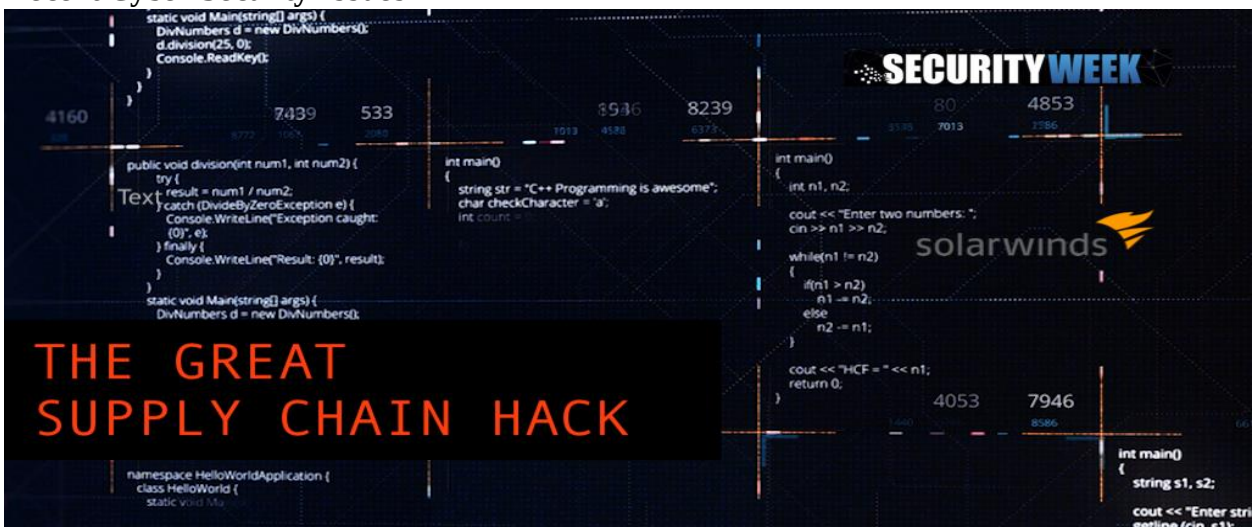

Figure 1 The Great Supply Chain Hack. Source: Security Week (2020)

According to Security Week (2020) A global cyber espionage campaign has resulted in the networks of many organizations around the world becoming compromised after the attackers managed to breach the systems of Texas-based IT management and monitoring solutions provider SolarWinds. Specifically, the attackers compromised the build system for the company's Orion monitoring product, which enabled them to deliver trojanized updates to the company's customers for at least three months.

Mello (2020) stated that an outlaw online network that's been used to infect millions of computers with ransomware has been disrupted by Microsoft. The company announced that, together with telecommunications providers around the world, it was able to cut off the infrastructure used by the Trickbot botnet so it could no longer be used to initiate new infections or activate ransomware already planted on computer systems.

Microsoft Corporate Vice President for Customer Security & Trust Tom Burt noted in a company blog that the United States government and independent experts have cautioned that ransomware is one of the largest threats to the upcoming elections.

Techpoint (2020) explained that it's the year of the pandemic, and besides the ensuing economic effects, it appears companies around the globe are dealing with increased rates of cyberattacks. Unfortunately, African countries seem to be major targets. As businesses

embrace emerging technology solutions like Internet-of-Things (IoT), Artificial Intelligence, and cloud computing, their exposure to cyberattacks has increased. In a recent survey, Sophos Group plc, a British security software and hardware company, revealed that 86% of Nigerian companies fell prey to cyberattacks within the past year. This is the second highest percentage recorded globally after India and much higher than in South Africa with 64%. This survey made use of data from 65 Nigerian companies that host data on public cloud-based services like Azure, Oracle, AWS, Alibaba cloud, and others.

III. CYBER ATTACKER TECHNIQUES/TOOLS

Threat Actor's Tools

Attackers are constantly sniffing networks to have unauthorized access to our assets such as intellectual properties and personal data, including smart phones, servers, computers, IOTs, tablets, etc. In order to have a successful exploitation of vulnerability, a threat actor must have a technique or tool. The attacking tools have become more sophisticated in recent years, and highly automated. The new tools require less technical knowledge and requirement to implement. This treat actor's tools and techniques are summarized in the table below.

TYPE OF TOOLS	DESCRIPTION
Password crackers	Passwords are the most vulnerable security threat. Password cracking tools are mostly referred to as password recovery tools and can be used to crack or recover the password. This is achieved in two ways, either by removing the original password, after bypassing the data encryption, or by outright discovery of the password. Password crackers continually make guesses in order to crack the password and access the system. Examples of password cracking tools include John the Ripper which is an open source and free software that is used for password testing. It can run on many different platforms like Unix, Dos, etc., Ophcrack – a free open-source program used in cracking windows password based on rainbow tables, etc.
Wireless hacking tools	Network security threats are more prevalent in wireless networks. Wireless hacking tools are used to intentionally hack into a wireless network to detect security vulnerabilities. Examples of wireless hacking tools include Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and NetStumbler.
Network scanning and hacking tools	Network scanning tools are used to probe network devices, servers, and hosts for open TCP or UDP ports. Examples of scanning tools include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
Packet crafting tools	Packet crafting tools are used to probe and test a firewall's robustness using specially crafted forged packets. Examples of such tools include Hping, Scapy, Socat, Yersinia, Netcat, Nping, and Nemesis.
Forensic tools	White hat hackers use forensic tools to sniff out any trace of evidence existing in a particular computer system. Example of tools include Sleuth Kit, Helix, Maltego, and Encase.
Rootkit detectors	A rootkit detector is a directory and file integrity checker used by white hats to detect installed root kits. Example tools include AIDE, Netfilter, and PF: OpenBSD Packet Filter.
	Hacking operating systems are specially designed operating

Hacking operating systems	systems preloaded with tools and technologies optimized for hacking. Examples of specially designed hacking operating systems include Kali Linux, SELinux, Knoppix, Parrot OS, and BackBox Linux.
Vulnerability exploitation tools	These tools identify whether a remote host is vulnerable to a security attack. Examples of vulnerability exploitation tools include Metasploit, Core Impact, Sqlmap, Social Engineer Tool Kit, and Netsparker.
Fuzzers to search vulnerabilities	Fuzzers are tools used by threat actors when attempting to discover a computer system's security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af.
Encryption tools	These tools safeguard the contents of an organization's data when it is stored or transmitted. Encryption tools use algorithm schemes to encode the data to prevent unauthorized access to the data. Examples of these tools include VeraCrypt, CipherShed, Open SSH, OpenSSL, OpenVPN, and Stunnel.

Table 1: Threat Actors Tools

Threat actors deploy various tools/techniques in carrying the criminal activities. Table 1 shows in a tabular form some of the tools/techniques, brief description of how and what the attackers used them.

Types of Attacks

Cyber criminals are constantly developing and exploring various forms of attack on our networks. Clear understanding of some of these attacking methods by staff and students in tertiary institution will help in guarding against these attacks. It is also important to note that the list is however inexhaustible.

Eavesdropping

Jake (2020) describe eavesdropping attack, also known as a sniffing or snooping attack, as a theft of information as it is transmitted over a network by a computer, smartphone or another connected device. The attack takes advantage of unsecured network communications to access data as it is being sent or received by its user. An eavesdropping attack can be difficult to detect because the network transmissions will appear to be operating normally. To be successful, an eavesdropping attack requires a weakened connection between a client and a server that the attacker can exploit to reroute network traffic. The attacker installs network monitoring software, the "sniffer," on a computer or a server to intercept data as it is transmitted.

This attack occurs when a threat actor snoop, captures and listen to network traffic. The attacker's interest in most cases is sensitive data and information on intellectual work, personal data, finance and business that can be sold for criminal purposes.

The initial strategies against this type of attack is to avoid free and public wi-fi networks (in schools, airport, cinema eateries, etc, in most cases are actually provided by the attackers.), use operating systems that are still supported by the manufacturers, keep your antivirus updated and use and maintained a strong password.

Man-in-the-middle

This is a transparent method a cyber-criminal adopts when hijacking a legitimate conversation between two end devices. It happens when a threat actor positions himself in between two legitimately communicating host and makes each of the host to believe that the conversation is delivered. The source and the destination are unaware that the threat actor has position himself and is able to actively monitor, capture and control their communication clearly. Dobran (2019) maintained that a Man-in-the-Middle (MITM) attack happens when a hacker inserts themselves between a user and a website. This kind of attack comes in several forms. For example, a fake banking website may be used to capture financial login information. The fake site is "in the middle" between the user and the actual bank website. Some of the man-in-the-middle attack include, Rogue access point, Address resolution protocol (ARP) spoofing, Multicast Domain Name System (mDNS) spoofing, DNS spoofing, etc.

Man-in-the-middle attacks can be prevented using a VPN (virtual private network) to encrypt the web traffic. Encryption reduces the threat actor's capability to read, understand and modify the web traffic. Securing the network with IDS (Intrusion Detection System), strong firewalls and third-party penetration testing tools by the network administrators can mitigate attacks. Also, a two-factor authentication method of applying password and short message system (SMS) combination can limit the rate of attacks. For instance, if you intend to withdraw cash from an ATM, you need your bankcard (something you have) and you need to know the PIN. This is also an example of multifactor authentication. Multifactor authentication requires more than one type of authentication. The most popular form of authentication is the use of passwords.

Denial-of-service (DoS) attack

Cisco defined denial-of-service (DoS) attack as prevention of normal use of a computer or network by valid users. After gaining access to a network, a DoS attack can crash applications or network services. A DoS attack can also flood a computer or the entire network with traffic until a shutdown occurs because of the overload. A DoS attack can also block traffic, which results in a loss of access to network resources by authorized users.

According to Cybersecurity & Infrastructure Agency (2019) a denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible. Denial-of-service attacks don't just affect websites—individual home users can be victims too. Denial-of-service attacks can be difficult to distinguish from common network activity, but there are some indications that an attack is in progress.

Common types of DoS attacks include Smurf attack, which forward Internet Control Message Protocol broadcast packets to many hosts with a spoofed source Internet Protocol (IP) address that belongs to the targeted device. The recipients of these spoofed packets will then respond, and the targeted host will be flooded with those responses. Another type is the SYN flood. Here, an attacker sends a request to connect to the target server but does not complete the connection through what is known as a three-way handshake—a method used in a Transmission Control Protocol (TCP)/IP network to create a connection between a local host/client and server. The incomplete handshake leaves the connected port in an occupied status and unavailable for further requests. An attacker will continue to send requests, saturating all open ports, so that legitimate users cannot connect.

Denial of Service attack can be avoided through the installation and maintenance of strong antivirus software, making your firewall configuration to restrict network traffic entering and leaving your computer, and adopting good security approaches in order to minimize information access.

Other types of attacks easily adapted by students and staff include, Sniffer, IP address spoofing, pass word-based, compromised key, and data modification attacks. Threat actors greatly employ malwares in carrying out their nefarious activities, Malware is a means to get a payload delivered. When it is delivered and installed, the payload can be used to cause a variety of network-related attacks from the inside. Threat actors can also attack the network from outside. Some of these malwares are very important to ignore. They include: ***Viruses***-a type of malware that spreads by inserting a copy of itself into another program. After the program is run, viruses then spread from one computer to another, infecting the computers. Most viruses require human help to spread. For example, when someone connects an infected USB drive to their PC, the virus will enter the PC. The virus may then infect a new USB drive, and spread to new PCs. Viruses can lay dormant for an extended period and then activate at a specific time and date.

Trojan horse malware-is a software that appears to be legitimate, but it contains malicious code which exploits the privileges of the user that runs it. Often, Trojans are found attached to online games. Users are commonly tricked into loading and executing the Trojan horse on their systems. While playing the game, the user will not notice a problem. In the background, the Trojan horse has been installed on the user's system. The malicious code from the Trojan horse continues operating even after the game has been closed.

According to Punch Newspaper October 23, 2021, Sadiq Oyeleke posits thus; The Nigerian Communication Commission (NCC) on Friday alerted Nigerians of the existence of a new high-risk and extremely damaging, malware called Flubot. The publication listed things to know about this new virus that steals banking details from Android devices. This malware impersonates android mobile baking applications to draw fake web view on targeted applications and is circulated through Short Messages Services (SMS) and can snoop on incoming notifications, initiate calls, read or write SMSes and transmit the victim's contact list to its control center. There is urgent need to create effective awareness, considering the damage this and other malware will create on our networks especially in the Tertiary Institutions where one of the polices on networks is "Bring Your Own Device" (BYOD) which are mostly android devices.

Computer ***worms***-are similar to viruses because they replicate and can cause the same type of damage. Specifically, worms replicate themselves by independently exploiting vulnerabilities in networks. Worms can slow down networks as they spread from system to system. Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, they no longer require user participation. After a host is infected, the worm is able to spread very quickly over the network. Malware can be prevented by using strong antivirus software, constant updating of the operating in our devices and adhering the cybersecurity rules and guidelines.

IV. NETWORK SECURITY MONITORING TECHNIQUES/TOOLS

Most tertiary institutions in keeping with Federal Government directives for non-pharmaceutical means of preventing the spread of COVID-19 decided to provide many of their services online. In doing this, many networks in our campuses are experiencing tremendous increase in network traffic thereby exposing our networks to cyber criminals who used students and staff to create and have access to the networks. "All networks are targets" is a common adage used to describe the current landscape of network security. Therefore, to

mitigate threats, all networks must be secured and protected. These monitoring techniques and tools are what we intend to create the necessary awareness and their implementation will save as a guide for the protection of our networks. In order to clearly understand network security monitoring techniques, it is pertinent to explore common security architecture.

Common Security Architecture

Firewall design is primarily about device interfaces permitting or denying traffic based on the source, the destination, and the type of traffic. Some designs are as simple as designating an outside network and inside network, which are determined by two interfaces on a firewall. The three common designs include:

Public and Private: The public network also known as outside network is untrusted, and the private network or inside network is trusted. Typically, a firewall with two interfaces is configured as follows:

- Traffic originating from the private network is permitted and inspected as it travels toward the public network. Inspected traffic returning from the public network and associated with traffic that originated from the private network is permitted.
- Traffic originating from the public network and traveling to the private network is generally blocked.

Demilitarized zone (DMZ): Is a firewall design where there is typically one inside interface connected to the private network, one outside interface connected to the public network, and one DMZ interface with these configurations:

- Traffic originating from the private network is inspected as it travels toward the public or DMZ network. This traffic is permitted with little or no restriction. Inspected traffic returning from the DMZ or public network to the private network is permitted.
- Traffic originating from the DMZ network and traveling to the private network is usually blocked.
- Traffic originating from the DMZ network and traveling to the public network is selectively permitted based on service requirements.
- Traffic originating from the public network and traveling toward the DMZ is selectively permitted and inspected. This type of traffic is typically email, DNS, HTTP, or HTTPS traffic. Return traffic from the DMZ to the public network is dynamically permitted.
- Traffic originating from the public network and traveling to the private network is blocked.

Zone-based policy firewalls (ZPFs): use the concept of zones to provide additional flexibility. A zone is a group of one or more interfaces that have similar functions or features. Zones help you specify where a firewall rule or policy should be applied. For instance, a network with multiple LANs can have security policies for LAN 1 and LAN 2 similar and can be grouped into a zone for firewall configurations. By default, the traffic between interfaces in the same zone is not subject to any policy and passes freely. However, all zone-to-zone traffic is blocked. In order to permit traffic between zones, a policy allowing or inspecting traffic must be configured.

Intrusion Prevention and Detection Devices

Tunggal (2021) describe network intrusion as any unauthorized activity on a computer network. Detecting an intrusion depends on having a clear understanding of network activity and common security threats. A properly designed and deployed network intrusion detection system and network intrusion prevention system can help block intruders who aim to steal sensitive data, cause data breaches, and install malware.

A networking architecture paradigm shift is required to defend against fast-moving and evolving attacks. This must include cost-effective detection and prevention systems, such as intrusion detection systems (IDS) or the more scalable intrusion prevention systems (IPS). The network architecture integrates these solutions into the entry and exit points of the network.

When implementing IDS or IPS, it is important to be familiar with the types of systems available, host-based and network-based approaches, the placement of these systems, the role of signature categories, and possible actions that a router (example Cisco IOS) can take when an attack is detected.

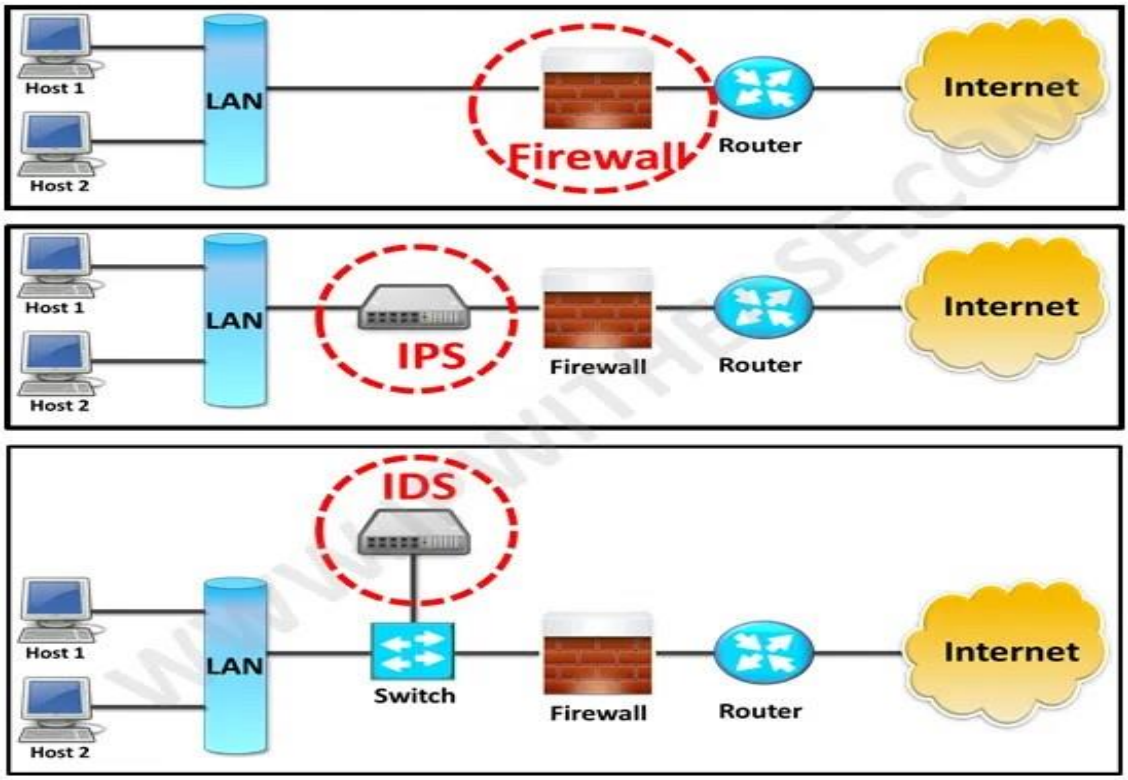

Figure 2: Firewall, IPS and IDP. Source: Rashmi Bhardwaj (2020)

The major differences in Firewall, IDS and IPS using Bhardwaj (2020) diagram above is that firewall performs actions such as blocking and filtering of traffic while an IPS/IDS detects and alert a system administrator or prevent the attack as per configuration. A firewall allows traffic based on a set of rules configured. It relies on the source, the destination addresses, and the ports. A firewall can deny any traffic that does not meet the specific criteria. IDS is a passive device which watches packets of data traversing the network, comparing with signature patterns and setting off an alarm on detection on suspicious activity. On the contrary, IPS is an active device working in inline mode and prevent the attacks by blocking it.

1. Network Monitoring Methods

The day-to-day operation of a network consists of common patterns of traffic flow, bandwidth usage, and resource access. Together, these patterns identify normal network behavior. Security analysts must be intimately familiar with normal network behavior because abnormal network behavior typically indicates a problem.

To determine normal network behavior, network monitoring must be implemented. Various tools are used to help discover normal network behavior including IDS, packet analyzers, SNMP, NetFlow, and others.

Some of these tools require captured network data. There are two common methods used to capture traffic and send it to network monitoring devices: Network taps, sometimes known as test access points (TAPs) and Traffic mirroring using Switch Port Analyzer (SPAN) or other port mirroring.

Network Taps

A Network taps, sometimes known as test access points (TAPs) is typically a passive splitting device implemented inline between a device of interest and the network. A tap forwards all traffic, including physical layer errors, to an analysis device while also allowing the traffic to reach its intended destination.

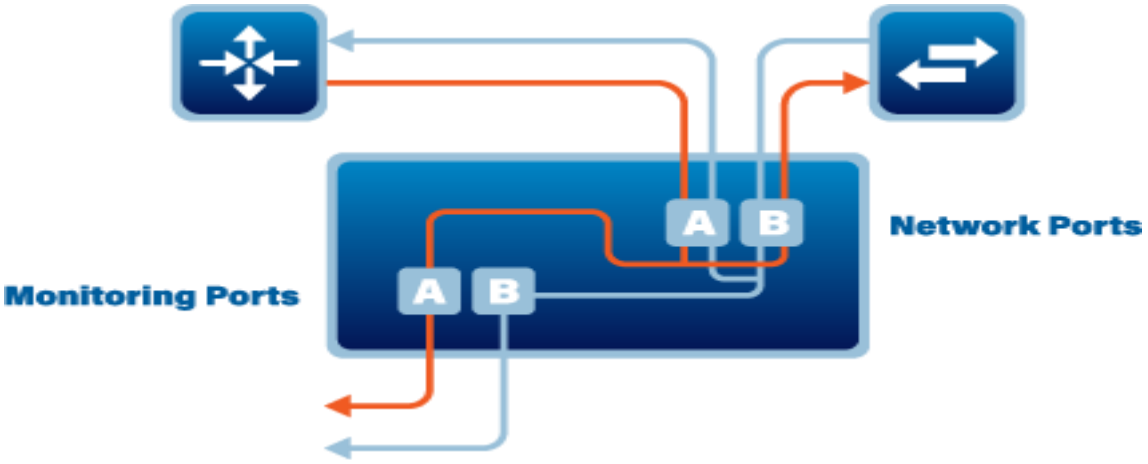

Figure 3 Implementation of Network Tap. Source: Bouchard (2020)

Notice in figure 3 above, how the tap simultaneously sends both the transmit (A) data stream from the internal system and the receive (B) data stream to the internal router on separate, dedicated channels. This ensures that all data arrives at the monitoring device in real time. Therefore, network performance is not affected or degraded by monitoring the connection. Taps are also typically fail-safe, which means if a tap fails or loses power, traffic between the firewall and internal

Switch Port Analyzer (SPAN)

Network switches segment the network by design. This limits the amount of traffic that is visible to network monitoring devices. Because capturing data for network monitoring requires all traffic to be captured, special techniques must be employed to bypass the network segmentation imposed by network switches. Port mirroring is one of these techniques. Supported by many enterprise switches, port mirroring enables the switch to copy frames that are received on one or more ports to a Switch Port Analyzer (SPAN) port that is connected to an analysis device.

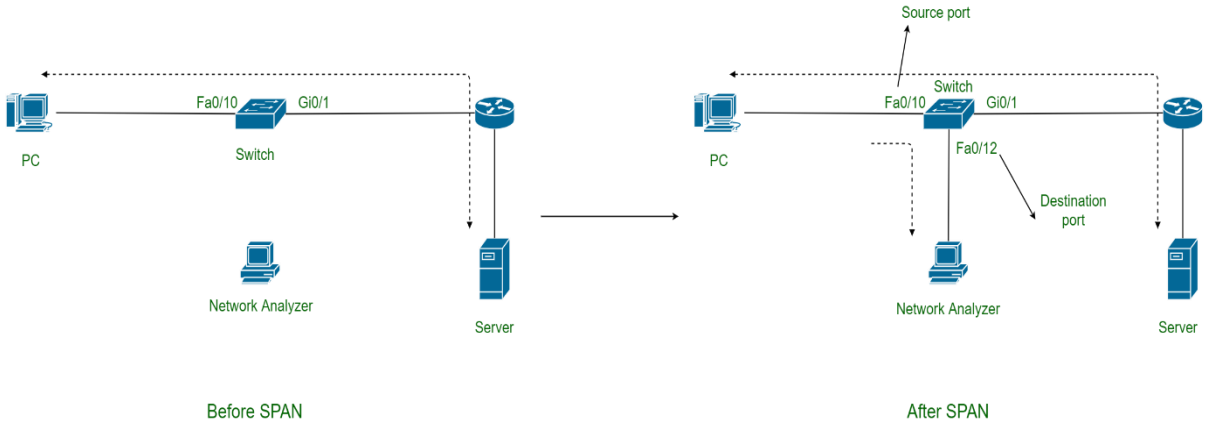

Figure 4: Frame Copying and Forwarding in SPAN. Source: GeeksforGeeks (2020)

Consider figure 4, given above containing switch, server, PC and network analyzer. Until the configuration of SPAN on switch, the frames flow normally from PC to server and vice-versa. But after the configuration of SPAN on switch, switch starts making copies of frames passing through its ports and send them to network analyzer.

2. Network Security Monitoring Tools

Network security monitoring is the responsibility of a security analyst who apply monitoring tools such as:

(a) Network protocol analyzers such as Wireshark and Tcpdump
(b) NetFlow
(c) Security Information and Event Management Systems (SIEM)

To monitor networks, it is pertinent for users connected to the network to have an understanding of how these tools are utilize in a network and be familiar with them. In tertiary institutions staff and students having a grip on these tools can assist in securing the cyber space of our various schools. Security is everybody's business.

Network Protocol Analyzers

Network protocol analyzers (or "packet sniffer" applications) are programs used to capture traffic. Protocol analyzers show what is happening on the network, often through a graphical user interface. Analysts can use these applications to see network exchanges down to the packet level. If a computer has been infected with malware and is currently attacking other computers in the network, the analyst can see that clearly by capturing real-time network traffic and analyzing the packets. Not only are network protocol analyzers used for security analysis. They are also very useful for network troubleshooting, software and protocol development, and education. For instance, in security forensics, a security analyst may attempt to reconstruct an incident from relevant packet captures.

Wireshark, a very popular network protocol analyzer tool that is used in Windows, Linux, and Mac OS environments. Wireshark is free software that can be downloaded and used by anyone. It is a very useful tool for learning about network protocol communications. Network protocol analyzer skills are essential for cybersecurity analysts.

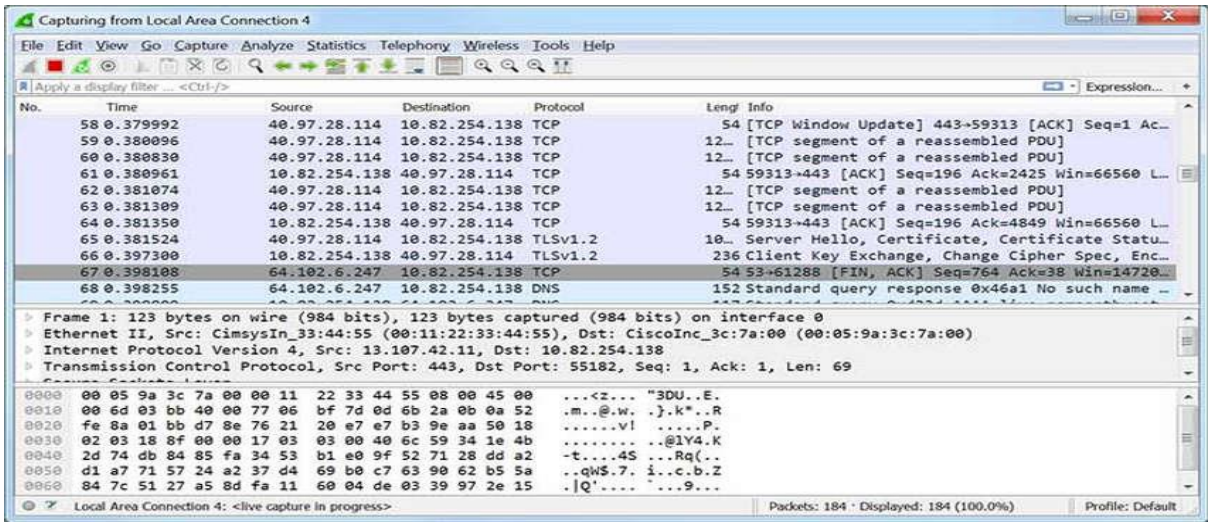

Figure 5: Frames Captured by Wireshark. Source Cisco (2020)

Figure 5 shows frames that are captured by Wireshark are saved in a PCAP file. PCAP files contain the frame information, interface information, packet length, time stamps, and even entire binary files that are sent across the network.

Wireshark can also open files that contain captured traffic from other software such as the **tcpdump** utility. Popular among UNIX-like systems such as Linux, **tcpdump** is a powerful utility with numerous command-line options.

NetFlow

Clavel (2020) describe NetFlow as a network protocol system created by Cisco that collects active IP network traffic as it flows in or out of an interface. The NetFlow data is then analyzed to create a picture of network traffic flow and volume — hence the name: *NetFlow*

NetFlow can be used for network and security monitoring, network planning, and traffic analysis. It provides a complete audit trail of basic information about every IP flow forwarded on a device. This information includes the source and destination device IP information, the time of the communication, and the amount of data transferred. NetFlow does not capture the actual content on the flow. NetFlow functionality is often compared to a telephone bill. The bill identifies the destination number, the time and duration of the call. However, it does not display the content of the telephone conversation.

NetFlow is a Cisco IOS technology that provides 24x7 statistics on packets that flow through a Cisco router or multilayer switch. NetFlow is the standard for collecting IP operational data in IP networks. NetFlow is now supported on non-Cisco platforms. IP Flow Information Export (IPFIX) is a version of NetFlow that is an IETF standard protocol.

SIEM and SOAR

Generally, both Security Information and Event Management (**SIEM**) and Security Orchestration, Automation, and Response (**SOAR**) tools aim to tackle the same problem, which is generally stated as handling the overabundance of security-related information and events that modern organizations generate. (Scott, 2020)

Network security analysts must quickly and accurately assess the significance of any security event and answer the following critical questions:

- Who is associated with this event?
- Does the user have access to other sensitive resources?
- Does this event represent a potential compliance issue?
- Does the user have access to intellectual property or sensitive information?

- Is the user authorized to access that resource?

To help answer the herein above indicated questions, security analyst uses SIEM and SOAR.

SIEM

Security Information Event Management (SIEM) is a technology used in enterprise organizations to provide real time reporting and long-term analysis of security events.

Network devices including firewall, IPSs, ESAs, WSAs, routers, switches, servers, and hosts are configured to send log events to the SIEM software. The SIEM software correlates the millions of events using machine learning and special analytics software to identify traffic that should be investigated. The functions perform by SIEM system include: Forensic Analysis, Correlation, Aggregation and Reporting.

An open-source product called Security Onion that includes the ELK suite for SIEM functionality. ELK is an acronym for three products from Elastic:

- **Elasticsearch** - Document oriented full text search engine
- **Logstash** - Pipeline processing system that connects "inputs" to "outputs" with optional "filters" in between
- **Kibana** - Browser based analytics and search dashboard for Elasticsearch

SOAR

SOAR (Security Orchestration, Automation and Response) is a solution stack of compatible software programs that allow an organization to collect data about security threats, and respond to low-level security events without human assistance. Data about these threats can be collected from multiple sources. The goal of using a SOAR stack is to improve the efficiency of physical and digital security operations. The term was coined by the research firm Gartner and can be applied to compatible products and services that help define, prioritize, standardize and automate incident response functions.

IV. RECOMMENDATIONS

From the foregoing, this piece of work recommend as follows:

1. That the federal government of Nigeria institutes without delay necessary policies that will strengthen the development of cybersecurity policies in tertiary institutions.
2. That management of tertiary institutions makes effort in training and re-training of her staff vertically and horizontally with the single aim of making the workers current in ever evolving cyber security technology.
3. That adequate orientation on cyber security be given to students and newly employed staff in order to inform and make them conversant with the cyber security policies of the institution.
4. That all institutions should make frantic effort to establish the department of cyber security for future manpower in the sector.
5. That all tertiary institution should establish and owned security operation center (SOC) to provide a broad range of cybersecurity services.
6. That staff and students should be encouraged to always update their software especially the operating system since we are in the era of BYOD.
7. That ICT centers in our schools be physically secured to prevent threat actors from mounting devices that can monitor their networks.
8. That government increase budgets of tertiary institutions for the acquisition of all that is required to implement robust cybersecurity policies.

V. CONCLUSION

In this work, we have attempted to advance the course of cyber security enhancement in tertiary institutions by examining some of the activities, technologies/tools of threat actors and the technologies and tools that can be deploy to mitigate incidents of attack. Defending, preventing and against COVID-19 epoch cybersecurity threats requires a formalized, structured, and disciplined approach. Tertiary institutions with inherent increase in traffic on their network typically needs a broad range of awareness and understanding of services, from monitoring and management, to comprehensive threat solutions and hosted security that can be customized to meet requirements of the time. In the end, it is hoped that there will be a sound knowledge of cybersecurity techniques by staff and students in our tertiary institutions will contribute to the safeguarding of our cyberspace against theft, hacking and damages of data, information, software, hardware and disruption or misdirection of system services, fighting criminals and keeping the necessary confidentiality, integrity and availability on our data and information through the development of good and sustainable cybersecurity awareness in this era of COVID-19.

REFERENCES

Adelakun I. S. (2020) Corona virus (COVID-19) and Nigerian Educational System. Thermofisher Scientific. 3(4), 2617-4588. https://doi.org/10.31058/j.edu.2020.34009

Ajisegiri W S, Odusanya O. O & Joshi R. (2020) COVID-19 Outbreak Situation in Nigeria and the Need for Effective Engagement of Community Health Workers for Epidemic Response. Global Biosecurity. Retrieved from https://jglobalbiosecurity.com/article/view/69/

Beaudin, K. (2015) College and University Data Breaches: Regulating Higher Education Cyber-Security Under State and Federal Law. Journal of College and University Law, 41(3), pp. 657-694.

Bouchard, George (2020) What Are Network Tap? And Why Do We Need Them. Profitap Blog. Retrieved From https://insights.profitap.com/what-are-network-taps

Cavelty, Myriam Dunn (2012) Cyber Security. Contemporary Security Studies. Oxford University Press

Clavel, Tom (2020) What Is NetFlow? How NetFlow Works and Why to Use It. Retrieved From https://blog.gigamon.com/2018/01/08/what-is-netflow/

Cisco (2020) Cisco ITC Cyberops Network Acad. Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Cybersecurity & Infrastructure Agency (2019) Security Tip (ST04-015) Understanding Denial-of-Service Attacks. Retrieved from https://us-cert.cisa.gov/ncas/tips/ST04-015

Dobran, Bojana (2019) What are Man in the Middle Attacks & How to Prevent MITM Attack with Examples. In Security Strategy, Ransomware, Data Protection, Retrieved from: https://phoenixnap.com/blog/man-in-the-middle-attacks-prevention,

Jake, Frankfield (2020) Eavesdropping Attack. Financial Technology and Automated Investing. Retrieved from: https://www.investopedia.com/terms/e/eavesdropping-attack.asp

GeeksforGeeks (2020) Switch Port Analyzer (SPAN) Retrieved from https://www.geeksforgeeks.org/switch-port-analyzer-span/

Mello, John P. (2020) Microsoft Squelches Trickbot Ransomware Network, TecnNewsWorld. Retrieved from https://www.technewsworld.com

Oladimeji S. A., Agbakwuru O. A., Opara C. C., Etim E. O. (2019) Development of a Secured Database System for Higher Educational Institutions in Nigeria. International Journal of Advanced Research in Science, Engineering and Technology, 12(6) ISSN: 2350-0328.

Rashmi Bhardwaj (2020) IDS vs IPS vs Firewall – Know the Difference. Retrieved from: https://www.ipwithease.com/what-are-routing-protocols/

Sadiq Oyeleke (2021) Flubot: Things to Know about the New Virus that Steals Banking Details from Android Devices; Punch Newspaper; October 23, 2012.

Security Week (2020) Internet and Enterprise Security News, Insight & Analysis. Everything You Need to Know About the SolarWinds Attack. Retrieved from http://www.securityweek.com

Scott, Andrew (2020) SIEM vs SOAR, What's the Difference? Retrieved From https://medium.com/swlh/siem-vs-soar-whats-the-difference-f81cf830fd03

Techpoint (2020) Nigerian companies record 2nd highest percentage of global cyberattacks. Retrieved from https://techpoint.africa/

Tunggal A. T. (2021) IDS vs IPS: What is the Difference? Retrieved from: https://www.upguard.com/category/cybersecurity