SECURE UNIVERSITY NETWORK ARCHITECTURE, VULNERABILITIES, RISK PRIORITY LEVEL CLASSIFICATION AND COUNTERMEASURES

By

IDRIS ISMAILA * MUHAMMAD UMAR MAJIGI ** SHAFI'I MUHAMMAD ABDULHAMID ***

MORUFU OLALERE **** MUHAMMAD BASHIR ABDULLAHI ***** VIVIAN O. NWAOCHA ******

*-**** Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria.
***** Department of Computer Science, Federal University of Technology, Minna, Nigeria.
****** Department of Computer Science, National Open University of Nigeria.

Date Received: --/--/---- Date Revised: --/--/---- Date Accepted: --/--/----

ABSTRACT

In order to safeguard a University's networked assets, a network administrator must decide how to harden the network. To aid the decision-making process, network administrators may use network hardening suggestions. A critical drawback of currently available analyses is the lack of consideration for the network administrator on identified vulnerabilities, risk figure, risk priority level classification and network security mechanism. Nessus and Nmap are network vulnerability scanner used for this research. Internal and external scan results tabulated. The result shows that firewall constitute 81 on scale of 1-100 risk priority level classification of university Information and Technology Service (ITS) network with high risk security level and open email relay constitute 2 with low risk level. Thus, the research establish a university secure network architecture model that contributed towards understanding risk priority level and also overcome shortcoming in choosing appropriate security measures.

Keywords: Vulnerability, Campus Network, Risk, Security, Network Attacks.

INTRODUCTION

In the modern education institutions, universities campus network have become a routine for work, teaching, scientific research and sharing the important tool of all kinds of resources. In a network all kinds of leaks occur through computer which brought a lot of concern, to prevent the network attack, it is important to set up and improve the campus network against illegal invasion (Wei, 2016).

University network and large network possesses enormous similarities, however each has its own challenges and problems securing the networks. This has always been an issues to Information Technology (IT) administrators and expert in security. A considerable number of accused persons transiting inside the university network, finger point at students of the institution. To create a secure network system for convenient in a learning environment is a challenging task. Currently, universities gives attention to information technology which improve student's research experience (Al Maskari, Saini, Rau,t & Hadimani, 2011)

Security and network professionals have risen their primary concerns to network security vulnerabilities, network vulnerability provide severe threats to the effectiveness and efficiency of an organization. (Awodele, Onuiri, & Okolie, 2012) It is essential that network administrator identified the system's security weakness, before hacker intrude into organization network.

Information Technology (IT) security practices are critically significant for University System and its subsidiaries to protect large amounts of sensitive information stored on the Data base. For instance, more than 70,500 student and 11,200 workforce access the internet in a university. Universities traditionally have a strong academic freedom culture that values free exchange of ideas and open access to information this make them target for

computer hackers. Security problems in university ITS are happening more frequently through vulnerability web based, Network computer applications and programs as well as via social engineering techniques. With nearly half of Ministries, Departments and Agencies (MDA's) web apps contain both informational and low security vulnerability risk level of 45.82% and 27.88% respectively. A4-Insecure Direct Object Reference is the largest contributor of web security risk in MDA's websites in Nigeria (Idris, Majigi, Abdulhamid, Olalere, & Rambo, 2017).

1. Literature Review

A vulnerability is a hole or a weakness in an application and it consists of three fundamentals namely: a system flaw or defenselessness, attacker capability to exploit the flaw and attacker access to the flaw. A flaw can happen during coding, compiling or implementation of a software known as a bug and allows an attacker to indirectly harm the stakeholders of the software. Stakeholders are entities that depend on the software as well as the software owner and users (Maistry, Ramkurrun, Cootignan, & Catherine, 2015). Most vulnerabilities, if not all, may allow a hacker to take advantage of the system by introducing an attack.

1.1 Network Vulnerability Assessment Infrastructure

Nathan proposes a cyber vulnerability in facilities accommodating systems critical infrastructure and general methodology for physical assessment. The methodology intended to scale multiple installations, thus establishing a baseline for prioritizing improvements and allocating resources.

A developed critical systems illustrate interconnection diagram and dependencies demonstrated. The ordering of system repair and timing, emergency responder, spare parts, key personnel, and when defining the degree of dependency system changes are considered (Timbs, 2013).

1.2 Risk Assessment

Risk management typically starts with risk assessment, a process used to discover, define, and comprehend risk (Hoo, 2000). An intended risk assessment "prioritise, identify and organizational operations risk estimate (i.e reputation, image, mission, and functions), Nation organizational assets, persons and the other organisation resulting from the use of information systems and operation" (Shanthamurthy, 2011; Stoneburner, G., Goguen, & Feringa, 2011). Divides risk assessment into three different phases. First, preparation phase includes assessment scope, constraints and purpose are defined. Threat and vulnerability information sources are well-known. Finally, risk factors and risk models used to establish key terms are defined. Second, analysis phase includes threats, vulnerabilities, likelihood and outcomes are identified and analysed. A list of prioritized information security risks is produced which is used to make risk-related decisions concerning security controls. Third and final maintenance phase includes ongoing monitoring and updating of identified risks.

1.3 Security Issues in Campus Network

Campus network security are numerous, below are common types of threat on a network.

1.4 Network Attacks Types

Attack classes might consist of exploitation by insider, passive monitoring of communications, close-in attacks, attacks through the service provider and active network attacks. Networks offer attractive targets and information systems and full range of threat agents should be resistant to attack, from hackers to nation-states. System must recover rapidly to limit damage when attacks occur (Ali, Hossain, & Parvez, 2015). Figure 1 shows traditional campus network design.

1.5 Review of Related Works

Eight (8) related vulnerability and risk assessment based research works were review. Below are Meta table reviews of related literatures.

2. Methodology

The research is aimed at developing secure university network architecture based on identified vulnerabilities, risk priority level classification using Nessus and Nmap vulnerability scanner. In this section all materials, methods, steps and processes undertaking to achieve the paper's aim and objectives are listed and explained. Including thesoftware tools used, how to identify

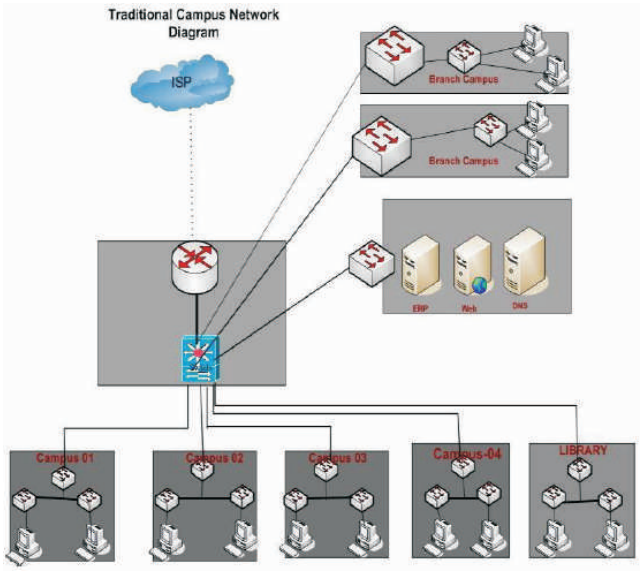

Figure 1. Traditional Campus Network Design (Ali, Hossain, & Parvez, 2015)

Types of Threat	External / Internal	Consequences of the Threat
Network Virus	External	Could enter through unprotected ports, compromise whole network
Email with Virus	External origination internal use	Could infect system reading email and subsequently spread throughout entire organization.
Web Server Attack	External to web servers	If web server is compromised hacker could gain access to other systems internal to network
Virus based web	External site to internal browsing	Might cause compromise on system doing browsing and affect further internal systems.
Network User Attack (NUA)	Anywhere to internal	Traditional border firewalls do nothing for this attack. Firewall internal segmentation can help contain damages.
Denial of Service (DoS) attack	Internal	External service such as web Email and ftp could become unusable. If router is attack, whole network could go down.

Table 1. Identify the Threats (Ali, Hossain, & Parvez, 2015)

vulnerabilities, techniques used for identification by the tool for the purpose of classification.

Network security scanners are used in order to successfully identify vulnerabilities for the purpose of classification and grouping. The study collect security reports related to some key university network. Although, two or more universities cannot have the same architecture. In some universities central IT group only provide high level service and bandwidth, departments will have its own IT staff, budget and department. Policy enforcement and policy making raises alot challenges having decentralized IT group. Figure 2 illustrate sample university network setup vulnerability points.

2.1 Maintaining Network Based - Vulnerability Assessment

In information Technology (IT) security today is uniquely ambitious and multifaceted concern fronting corporate institution. 99% of all attacks is as result of security breaches and faulty misconfiguration, known vulnerabilities which cost institutions millions of Naira in financial losses each year, a solution is not forthright. Security professional, application related vulnerabilities and operating system are growingly mindful of the basic to cope possible risks and assess on the systems and network with a myriad of networks. This requires a more intelligent approach to fortifying the enterprise and effectiveness

The research uses below Network Vulnerability Scanners:

- Nessus, by Nessus Project team
- Nmap;

2.2 The Nessus Vulnerabiity Scanner

According to Kak, (2016) Nessus is an open-source venture and remote security scanner. Nessus typically run on one mechanism to scan all the devices obtainable by a remote machine in order to determine whether the latter is protected against all known security exploits. Figure 3 shows Nessus login interface.

To scan on Nessus environment: Open a web browser and connect user interface of the Nessus scanner and clickon

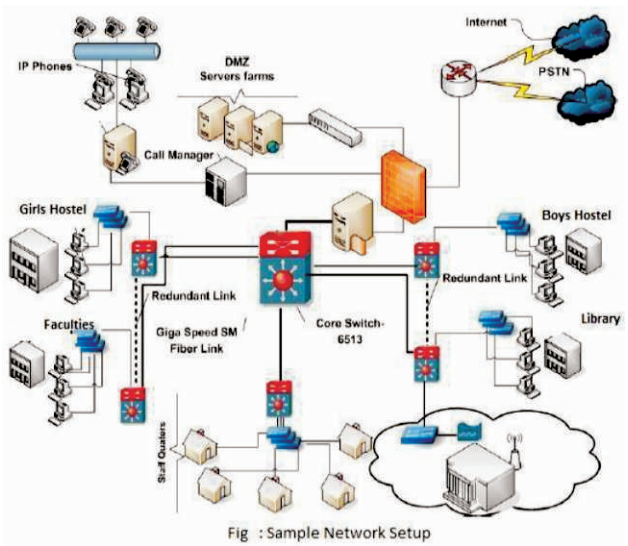

Figure 2. Sample University Network Setup

	One	Two
Tittle of article	Security and vulnerability issues in University Networks	The Unified Approach for Organizational Network Vulnerability Assessment
Authors(date)	Sanad Al Maskari, Dinesh Kumar Saini, Swati Y. Raut and Lingraj A. Hadimani (2011)	Dhanamna Jagli, Rohoni Temkar (2013)
Focus	Security Architecture, Vulnerability Analysis, Campus network and its Implementation	Network Vulnerability Assessment using new approach called unified process
Methodology	CVAT, Firewalls, Intrusion Detectors and Anti – Malicious Software	Firewalls, Access controls, and auditing
Result	Identified all the potential discrete points and offers complete terms to implement the security control on them	Unified Network vulnerability approach is helpful for finding network vulnerabilities in any organization infrastructure
Limitation	Tools not reconfigured on the network	The research do not address adequate policies and procedures for assessment and evaluation
	Three	Four
Tittle of article	Cyber Security: Threats, Vulnerabilities and Counter measures - A Perspective on the State of Affairs in Mauritius	The problem in Campus Network Information Security and its Solutions
Authors(date)	Tikshnayay, N., M. Nomesh , R., Mageshwaree, C., and Pierre, C. C. (2015)	Guihong, Wu. (2010)
Focus	Most common vulnerabilities and threats, also provides an overview of its countermeasures	Current Security status of the University Network, maintenance of Network Security, also analyzing threatens to campus network security
Methodology	Encryption, Back-tracing and protocol (ISO 127K)	Firewalls, VLAN, VPN, Encryption technology and PKI technology
Result	IPV6, IOTs and Cloud computing are introduced as emerging technology. It provides resilient cyber security framework.	Establish a suitable campus network security system and introduce some recent University Network Security solutions
Limitation	Need for stronger cyber security infrastructure to enhanced capacity to identify recent research and react to cyber - attacks today.	Secured campus network architectural model not included on the contribution to knowledge.
	Five	Six
Tittle of article	Physical Security Assessment of a Regional University Campus Network	Design and Implementation of a Secure Campus Network
Authors(date)	Michael, L., C, Philip, E., P, Rita, M., B. (2013)	Mohammed, Nadir Bin Ali, Mohamed, E., Hossiani, Md. Masad., P. (2015).
Focus	Validation of PSA Tool, a prototype application for assessing the physical security of a networks	University Campus Network and proposed realizable adaptable infrastructure
Methodology	PSA Tools	Firewall, VLAN, Cyberoam security device Virtual Private Network (VPN)
Result	PSA Tool expose 95 threats, hazards and vulnerabilities in 82 DFs security.	Model Architecture of the UniversityCampus Network configured with different types of security issues for ensuring the quality of service with compact cost effective secure campus network design based on the work environment
Limitation	Shunt trip hardware not install in location where sprinklers could damage equipment or create a hazard for electric shock	Virtual Private Network (VPN) has a 20 hours session.
	Seven	Eight
Tittle of article	Vulnerability assessment and penetration testing.	The Campus Network Security Hidden Danger Analysisand Countermeasures
Authors (date)	Umrao, S., Kaur, M., & Gupta G. K. (2012).	(Wei, 2016).
Focus	Used of penetration testing to patch the weakness and vulnerabilities assessment to detect vulnerabilities	Issues related to student personal privacy in campus network security and its countermeasures
Methodology	Nmap,Nessus and Wiresharp	Firewall, Intrusion Detection Systems (IDSs) and Virusprotection Software
Result	A unified method was developed for establishing outline that can be simply identified instead the physical tester	Noted some of the hidden dangers of the university network and highlighted some countermeasures.
Limitation	The researcher do not emphasis on penetration testing and the practical implementation of vulnerability analysis by means of wireshap, Nmap and Nessus	Do not have information security firewall.

Table 2. Meta-Analysis Table

the Policies tab to edit an existing policy or create a new policies, select the credentialstabon the left. Select windows credentials from the menu at the top and drop down.

Optional domain, account name and password should be specify.

Click at the bottom of the window and configuration will be completed then submit. The list of managed scan

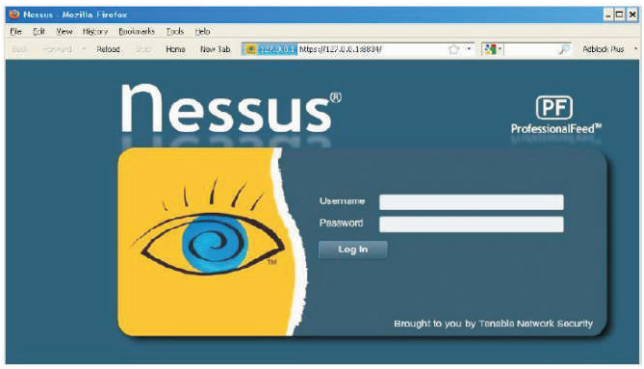

Figure 3. Login Interface for Nessus

policies and the new scan policy are added together.

The main feature of Vulnerability Scanner Nessus includes (Singh, 2011)

- Detect open ports and scan
- Identifies services running on the network,operating system, databases and applications
- Antivirus Software Audit
- Missing security patchesidentifies

2.3 Network Mapper (Nmap)

Network Mapper is a licence free open source utility for network auditing security/ exploration. Nmap is also valuable for tasks like managing upgrade schedules services, network inventory and service uptime or monitoring host. Nmap official binary packages are obtainable for Windows, Mac OS X and Linux, it runs on all main computer OSs (operating systems).

Common characteristics of this tools are (Singh, 2011) Flexibility, Powerful, Portable and popular.

Some important Nmap features are: Port Detection, Host Discovery, Version detection and OS Detection using Nmap.

Below Table 3, shows scan manifest of university ITS.

Table 3 summarize scan manifest: The external and internal scans vulnerability are used as an instrument to collect data to evaluate the efficiency of recent security control measures in use at the system level of University's ITS network. However, insecurity assessment document this data will be used as evidence to backing recommendations found and finding. The internal scan took place at the University ITS to determine all vulnerabilities. The switch that is situated inside ITS's network, the scanner was plugged in to it.

To get a detailed look at system configurations, is to side-step countermeasures and external security controls. The 123.123.123/123 network for internal scan was selected by ITS staff. The security posture of the external scan is see through the eyes of Internet user. The University ITS's network is to know what a hacker would see if he were trying to probe. The IP address 12.12.12/12 was chosen by ITS staff for external scan.

External and internal groups that may be affected by the scan are informed. The three phases invulnerability scan are: vulnerability assessment, manual checks (optional) and network discovery. The first and third phases call for the use of scanning tools. Discovering live hosts on the directed networks involved only network discovery phase. To determine hosts on the network Nmap tool is used. Phase three output is inputted into phase one. External scan is conducted only on phase two.

Result findings generated from the external and internal scan using Nessus and Nmap are tabulated in Table 4.

3. Result of Risk Figure

The Table 4 shows estimated product of probability of attack via vulnerability, cost if attack succeed via such vulnerability at scale of 1-10 and risk Figure.

Similarly, risk level was also calculated. Low Risk Value (RV) is between 1-30, medium is on interval of 31 -69 and high risk value is between 70-100 as shown above. Table 5 below shows risk level order of priority starting from most to least.

Customer	University ITS
Scan Identifier	Internal Scan External Scan
Date	Internal Scan: 3rd September, 2016 External Scan: 7th September, 2016
Time Started	Internal Scan: 7:30 am External Scan: 9:45 am
Tools	Nessus 4.1.2 Nmap 7.3.0
Scope	External Scan: 12.12./12 Internal Scan: 123.123.123,123/123
Description	This Scan is envisioned to identify all vulnerabilities and collect supporting evidence for the security assessment. The scan result will be used to determine the control and types of security counter measures put in place and their efficiency.

Table 3. University its Scan Manifest

3.1 Network Vulnerability Assessment Strategy

Two ways approaches to network vulnerability scan: External and Internal. To get a complete status picture of all machines, internal scanning should be carry through network from inside. The firewall and router external scanning is done outside the network from a host. The Network manager is able to see his network the way an external aggressor might. The external scans when perform comes with downside that only safeguards the administrator's network from an external aggressor. No protection from a vicious member of staff. Internal scans permit the security manager to remedying security vulnerabilities and provide additional information. The external IP galaxy in a university network be separated into each subnet scanned for security weaknesses and subnet. Similarly, to check for application vulnerabilities related and errors configuration form critical parts of the network should be scanned internally. Toward ensuring that communication channel is not back through from the web tier to the Internal Network/database tier used by the administrator, internal scan is used.

Risk Priority Level Classification of University its Network

Pr (AV) = Probability of Attack via Vulnerability (at scale of 1-10)

C(AS) = Cost if Attack Succeed via Vulnerability (at scale of 1-10)

Risk Figure = Pr(AV)*C(AS) (at scale of 1-100)

Risk Level Scale : Low = (RV = 1-30) Medium = (RV=31-69) High = (RV=70-100)

Vulnerability	Pr(AV)	C(AS)	Risk Figure (RF)	Risk Level (RL)
Open Email Relay	1	2	2	Low
Unnecessary Services	2	3	6	Low
Hindsight is 20/20	1	7	7	Low
Logical Access Controls	4	3	12	Low
Miscellaneous USB devices	3	4	12	Low
Insecure / Exposed Ports:	2	7	14	Low
Application Back doors	5	3	15	Low
Trojan Human	2	8	16	Low
Old Passwords	3	7	21	Low
Old Patch Levels	4	6	24	Low
Poor Attention to Security Indicators	5	5	25	Low
Inside Connections	6	6	36	Medium
Poor Intrusion Detection System (IDS) Setups	7	6	42	Medium
Anti-Virus Implementation	6	7	42	Medium
Lack of Appropriate Security Policies	8	6	48	Medium
Wireless Access Point	9	8	72	High
Ineffective Procedure	9	8	72	High
Firewall	9	9	81	High

Table 4. Grouping of Risk Level Based on Identified Priority

Risk Level	Order of Priority (1=most, 17=least)
High Risk	1. Firewall 2. Ineffective Procedure 3. Wireless Access Point
Medium Risk	1. Lack of Appropriate Sec. Policies 2. Anti-Virus Implementation 3. Poor Intrusion Detection System Setups 4. Inside Connections
Low Risk	1. Poor Attention to Security Indicators 2. Old Passwords 3. Trojan Human 4. Application Back doors 5. Insecure/ Exposed Ports 6. Miscellaneous USB devices 7. Logical Access Controls 8. Hindsight is 20/20 9. Unnecessary Services 10. Open Email Relay

Table 5. Risk Priority Level Classification of the Network Vulnerability

4. Discussion of Results

The proposed counter measures (security mechanism) based on identified vulnerabilities were outline. Vulnerability scanners detect vulnerabilities and offer patches to identified vulnerabilities. For this reason vulnerability scanners do not consider the inter dependencies that may exist between vulnerabilities.

The selection of the appropriate set of security measures is nontrivial; however, removal of security flaws is performed by implementing one or more security measures.

Below chart shows the vulnerabilities, probability of attack via vulnerability, cost if attacks succeed via vulnerability and risk figure of the vulnerabilities.

Firewall, ineffective procedure and wireless access point are most high risk level security and open email relay is the least low risk level security as shown in Figure 4.

Risk figure graph shows that firewall have the highest risk level of 81 on 100 risk figure and open email relay with lowest risk of 2 on scale of 1 -100 risk figure. The linea rline on the graph, illustrate the order of priority (High, medium and low risk level).

4.1 Security Mechanisms based on Identified Vulnerabilities

Ways to prevent or recover in good time from security glitches, below are itemized counter measure steps for the secure university network based on identified vulnerabilities.

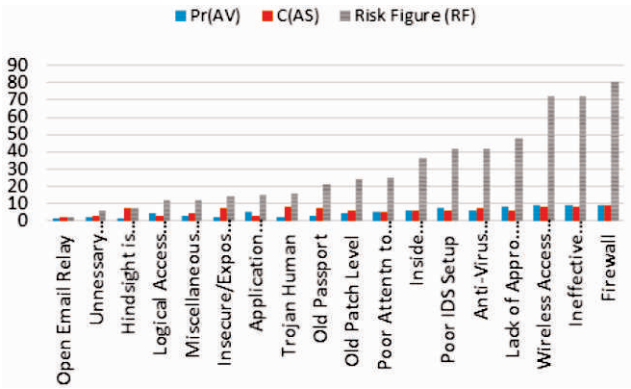

Figure 4. Risk Priority Figure Classification of the Network Vulnerability

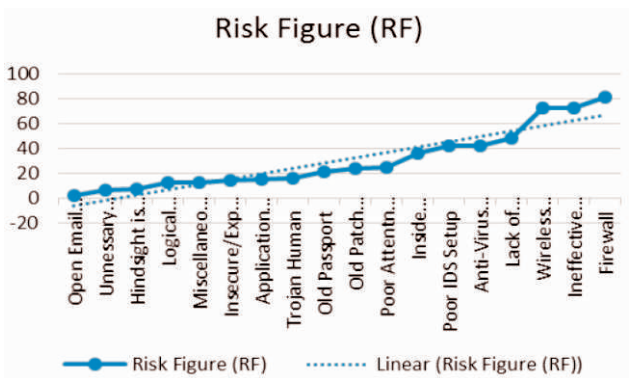

Figure 5. Risk Figure (RF) Graph

Wireless Access Point: Using RADIUS in WPA2 enterprise is intensely recommended with Access Point (AP) that is capable of implementing security measures and performing authentication. Frequent password change on regular basis and very strong mixed passwords should be used.

Miscellaneous USB Devices: If enforce asset control and policies are implemented around what devices should be connected and when should it be connected. And frequent policy reminders should follow up. For instance US Department of Defense in 2008, developed policies banning removable media and USB from exiting/entering their environments.

Inside Connections: Access levels for any staff and authentication, employee is require to a have access to systems/file shares for their schedule duties only. Passwords are change regularly. Any special requests should directed always to appropriate team who can approve the call.

The Human Trojan: Employees should always be remind of authorizing third parties. Ask question to source of the person, don't make assumptions on save guiding network infrastructures.

Hindsight is 20/20: Alert and being mindful about this threat whenever working on sensitive material is the best safeguard, momentarily stopping what you doing is to observe your surroundings against hindsight.

Firewall: These are hardware devices or program that gives protection to the assets of a private network from other networks users. To allow incoming traffic to pass, refuse or block fire walls are responsible for that and they also work with proxy servers. They protect private networks from attackers or intruder.

Making Security Policies: Security policies are drafted documents which define the security measures that is expected to be implemented in an organization at a high level without it, the organization cannot protect itself from likely lost revenue, lawsuits, basic security attacks and bad publicity. The rules and objectives of these policies set behavior for users, administrators and suggest the safety measures to be followed in a university. Three goals achieve by policies are:

- They prevent waste of university computing assets.
- They eliminate or reduce legal responsibility to personnel.
- They safeguard patented information, confidential from mismanagement, unauthorized modification, and theft.

Intrusion Detection Systems (IDSs) / Prevention: Mechanisms used to monitor network traffic, prevent/ alerts them from the attacking the network and check for suspicious actions. For instances in some cases, the IPS/IDS react to anomalous traffic or malicious and will take action such as barring the IP address source or user from gaining access to the system. In this view, both Network and Host Based Intrusion/Prevention Systems are recommended for the university network.

Patch Management: The process to make sure that suitable patches are installed on a system is called Patch Management. It includes the following:

- Verifying, choosing, applying patches and testing.
- Present and past applied patches are updated.
- Previous patches applied to date are listed.
- Repositories/recording depots of patches for easy choice.
- Set up applied patches and assigning.

Logical Access Controls: Fire walls enforced Logical Access controls for networks, local Area Network (LAN) on dedicated computers restrict traffic to and from the network in such features communications protocol and origin. Regrettably, access controls may also be vulnerable to attacks stated above, in general it may not protect against attacks by insiders such as staff with technical know-how.

To prevent Password Cracking:

- Word list that can be easily found should not be use as passwords.
- Choose passwords of eight characters and above.
- Combination of upper and lower case letters, special characters, numbers etc. Should be use as passwords, this makes it difficult for cracker.
- Avoid use of public information, like ATM card number, Date of birth and Credit card number as passwords.
- Passwords and user names should be unlike.
- University ITs manager should setup strong policies to improve the security of the networks, using strong passwords can further enhance security of university network.

Physical Security: These defines the apparatuses set in place to safeguard network critical assets against intended and unintended threats. To prevent pilfering and tampering of data, unauthorized access, natural disaster to data and trustworthiness of the data stored in the computer system. Below are mitigations:

- *Physical:* To secure network resources e.g security personnel deployed.
- *Technical:* Information technology elements and service maintenance should be Secure e.g. security for expensive gadgetry and server rooms.
- *Operational:* before performing an operation measures taken like taking appropriate counter measures and analyzing attacks of an activity.

Universities go all-out to create a suitable education environment via IT infrastructure. In a university network there are many software applications, network devices, online systems and various servers running. Knowing what is inside a network is a critical security requirement.

From Figures 3 and 6 the research identified vulnerabilities on the network using Nessus and Nmap. However, the research proposed a secured university network infrastructure in Figure 7 in accordance with best practice

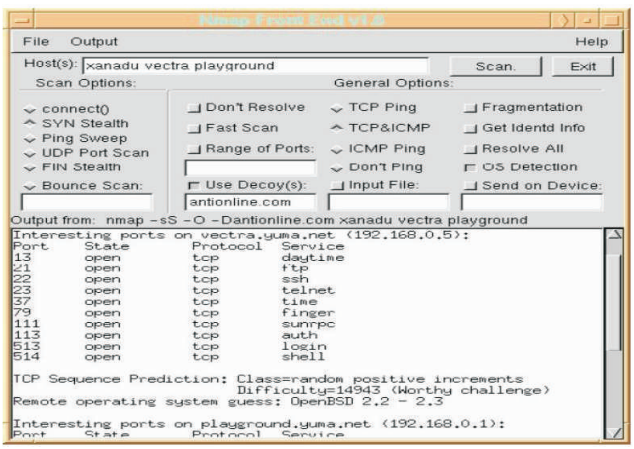

Figure 6. Basic Nmap Command (Saxena & Kumar, 2006)

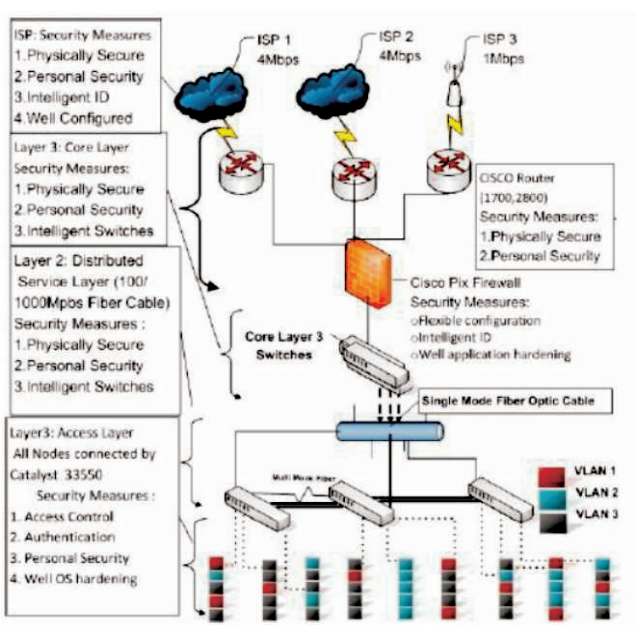

Figure 7. University Secure Architecture

in the world to fixed and provide counter measure for feature vulnerabilities.

4.2 Mitigiting the Known Attacks

Proposed steps for mitigating the known attacks of a University ITS network are:

- Design of a secure campus Network.
- External and internal security fire walls Implementation.
- Creation of Virtual LAN (VLANs) for security.
- Branch campuses Virtual private network VPN Figure7 illustrate secure university network architecture.

Measures for the secured University network can be shown in the collected form according to the Figure 7. Numerous measures and discrete points are clearly stated.

5. Recommendation and Conclusion

5.1 Recommendations

- Simple configurations should be deploy by the administrator that are easy to maintain and work.
- For efficient and proper configuration of the system, importance on disabling unnecessary applications/ services.
- Recent security update should be kept, a network manager should routinely run vulnerability check.
- Computer crime related offences should reported to law enforcement agency regulated it, for proper legal according Nigeria cyber crime prohibition act, 2015
- Implementation of efficient and good security procedures and policies. Employees handling sensitive infrastructure should be train on routine.
- Managers should be well-informed in incident handling and Computer forensic.

Conclusion

The research proposed a secure university architecture design based on the required scalability, security and work environment. To offer high assurance of suitable level of availability, confidentiality and integrity of information, vulnerability assessments are significant through which universities can identify possible security threats.

Ness us and Nmap are two network vulnerability scanners used for discovering of vulnerabilities. Internal and external scan results are tabulated. Conversely, we can deduced that Firewall, ineffective procedure and wireless access point are most high risk level security and open email relay is the least low risk level security. Fire wall have the highest risk level of 81 on 100 risk figure and open email relay with lowest risk of 2 on scale of 1 - 100 risk figure.

The research establish a university secure network architecture model that contributed towards understanding risk priority level and also overcome short coming in choosing appropriate security measures.

References

[1]. Al Maskari, S., Saini, D. K., Raut, S. Y., & Hadimani, L. A. (2011). Security and vulnerability issues in university networks. In *Proceedings of the World Congress on Engineering* (Vol. 1).

[2]. Ali, M. N. B., Hossain, M. E., & Parvez, M. M. (2015). Design and Implementation of a Secure Campus Network. *International Journal of Emerging Technology and Advanced Engineering,* 5(7), 370-374.

[3]. Awodele, O., Onuiri, E. E., & Okolie, S. O. (2012). Vulnerabilities in Network Infrastructures and Prevention/ Containment Measures. In *Proceedings of Informing Science & IT Education Conference* (InSITE).

[4]. Hoo, K. J. S. (2000). A Risk-ManagementApproach to Computer Security. *Consortium for Research on Information Security and Policy (CRISP)* pp. 1-88

[5]. Idris, I., Majigi, M. U., Abdulhamid, S., Olalere, M., & Rambo, S. I. (2017). Vulnerability Assessment of Some Key Nigeria Government Websites. *International Journal of Digital Information and Wireless Communications,* 7(3), 143-153.

[6]. Jagli, M., & Temkar, M. (2013). The unified approach for organizational network vulnerability assessment. arXiv preprint arXiv:1310.2365. *International Journal of Software Engineering and Application (IJSEA),* 4(5) Doi: 10.5121/jisea,2013.4503

[7]. Kak. A. (2016). Port and Vunerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing. *Lecture Notes on Computer and Network Security.*

[8]. Maistry, T. N., Ramkurrun, N., Cootignan. M., & Catherine, P. C. (2015). Cyber security: Threats, Vulnerabilities and Countermeasures - A Perspective on the State of Affairs in Mauritius. In *Proceedings of the Second International Conference on Data Mining, Internet Computing, and Big Data, Reduit, Mauritius* (pp.54-68).

[9]. Saxena, A. K., Kumar, S. (2006). Network Penetration Testing. AKS Information Technology Service Ltd. Retrieved from https://cert-in.org.in/Downloader?pageid=5&type=2&fileName=CIPS-2010-0167.pdf

[10]. Shanthamurthy, D. (2011). NIST SP 800-30 standard for technical risk assessment: An evaluation. In ComputerWeekly.com. Retrieved from https://www.computerweekly.com/tip/NIST-SP-800-30-standard-for-technical-risk-assessment-An-evaluation

[11]. Singh. G. (2011). Profilling Campus Network using Network Penetration Testing. Master Thesis in Software Engineering. *Computer Science and Engineering Department,* pp.1-59

[12]. Stoneburner, G., Goguen, A., & Feringa, A. (2011). Risk Management Guide for Information Technology Systems. *National Institute of Standards and Technology (NIST).*

[13]. Timbs, N. H. (2013). Physical Security Assessment of a Regional University Computer Network. Electronic Thesis and Dissertations. http://dc.etsu.edu/etd/2280

[14]. Umrao, S., Kaur, M.,& Gupta, G. K. (2012). Vulnerability assessment and penetration testing. *International Journal of Computer & Communication Technology,* 3(6-8), 71-74.

[15]. Wei, J. (2016, May). The campus network security hidden danger analysis and countermeasure research. In *2016 2nd Workshop on Advanced Research and Technology in Industry Applications (WARTIA-16).* Atlantis Press.

[16]. Wu, C. (2010, July). The problems in campus network information security and its solutions. In *Industrial and Information Systems (IIS), 2010 2nd International Conference on* (Vol. 1, pp. 261-264). IEEE..

ABOUT THE AUTHORS

P