NETWORK VULNERABILITY: A REVIEW

Stephen O. Ohwo
Department of Computer Science
Delta State Polytechnic Ogwashi-Uku, Nigeria
steveohwo@yahoo.com
+234 08063357590

Abstract
Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Securing and protecting a computer network from possible attacks or intrusions is very difficult task. Intruders can attack vulnerable systems and networks and compromise data as well as critical systems. But by the review and analysis of the existing vulnerabilities using some of the available technological approaches, general point solutions are acquired, giving clues for strategic network protections. The research aim at x-raying some of the available network vulnerability technological approaches and some models which can be implemented to detect and measure intrusion tendencies of a network in order to ensure a secure network. The methodology adopted are; (1) Extensive review of relevant literatures on network security, network policy, and methods used in attacking computer network, (2) Analysis of vulnerability types, expected vulnerabilities in network and scanning tools to detect vulnerabilities. The result of the review and analysis x-raying some of the available network vulnerability technological approaches and models which can be implemented to detect and measure intrusion tendencies of a network in order to ensure a secure network.

Keywords
Computer Network, Network Security, Attackers, Vulnerability, Analysis tools

Introduction

A flaw within communicating device's software, hardware, or organizational processes is term as network security vulnerabilities. Network vulnerabilities can be either non-physical or physical. In network security, vulnerability means weakness in a system, which permits an intruder to violate the integrity of that system. These weakness can come from weak passwords, software bugs, a computer virus or other malware (malicious software), a script code injection, or SQL injection just to name the few (Amit and Santosh, 2015). A security risk with several instances of working and fully implemented attacks is known as an exploit. Programming languages Constructs that are difficult to use correctly can be a large source of vulnerabilities. Vulnerabilities existed all the time, but when Internet was at its early stage they were not as often used and exploited. Before now nodes on the network were trusted, secure protocols such as Secure Shell (SSH), Secure, Contain and Protect (SCP), Secure Sockets Layer (SSL) did not exist, but File Transfer Protocol (FTP) and plain text Hypertext Transfer Protocol (HTTP) were used to interexchange sensitive data. In the new age of global connectivity and e-commerce, interconnections via networks have heightened, creating for individuals and organizations, a state of complete dependence upon vulnerable systems for storage and transfer of information. According to Amit and Santosh, (2015) the power to deface websites, access personal mail accounts, and worse more the potential to bring down entire governments, and financial corporation's is through openly documented software codes.

Hacking is unauthorized intrusion into a computer or a network and the person engaged in hacking activities is known as a hacker (Gao, 2015). Hacker can alter system or security features to achieve their goals that differ from the original purpose of the system. This is done through

cracking of passwords and codes which gives access to the systems (Montoro, 2009). The hacking can be done on single systems, a group of systems, an entire LAN network, a website or a social media site or an email account. password cracking algorithms programs are used by hacker to have access to a password. Variety of techniques are use by hackers for hacking, some of these includes: Vulnerability scanner, Password cracking, Packet sniffer, Spoofing attack, Root kit, Trojan horse, Key logger, Denial of Service (DoS), Waterhole attacks, Fake WAP, Eavesdropping (Passive Attacks), Phishing, Virus, Trojan, etc.

Problem Statement

Despite the numerous benefits of using computer networks, networking raises a greater potential for security issues such as: data loss, security breaches, navigating the cyber security skills gap, malicious attacks, such as hacking and viruses. How can you ensure efficient and secure network access as your business evolves? , and managing the top cyber risks depends upon the ability to see them Hence there is a need to identify the various kinds of network vulnerability, methods of attack and tools for scanning for vulnerabilities in a network. This is the gap the researcher intends to fill.

Objectives of the Research

The review is aimed at enlightening computer network vulnerability analysis technological approaches and tools. While the specific objectives are:

- To analysis the various methods of network attack by intruders
- To highlighting the types of network vulnerabilities analysis and tools for network scanning
- To advice on the best practices in the management of a network to prevent attacks.

Concept of Network Security

Network security is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware approaches (Wright and Jim, 2009). Every organization requires a degree of network security solutions in place to shield it from cyber threats in the wild today. Network architecture nowadays is complex and is faced with challenges of threat environment that is dynamics with attackers that are always trying to find and exploit vulnerabilities. These vulnerabilities can exist in devices, data, applications, users and locations. There are many network security management tools and applications in use today that address network threats and exploits as well regulatory non-compliance noting that just a few minutes of attacks can cause widespread disruption and massive damage to an organization's data and reputation, thus there is a need to put in place network protection measures. Network security could be physical, technical or Administrative. Some of the methods of securing network are: Network access control, firewall protection, Antivirus and Antimalware Software, Firewall Protection and Virtual Private Network (Amit & Santosh, 2015).

Network Security Policy

It is important that organizations develop, educate, and enforce an enterprise-wide wireless local area network (WLAN) security policy. The aim of the security policy should address a framework for the development such as installation, protection, management, and usage procedures. A WLAN security policy should be flexible in components and technologies it can support. The main challenge for the IT organization is to develop advanced security that will support end-user requirements (Dwianto, 2016). The WLAN security must integrate with the organizations wired network security policy to ensure

proper management and protection across the network branches. A WLANs unique security challenge is that security is still dependent on controlling who has access to specific information. The proper documentation and management will help to understand specific WLAN vulnerabilities. It also deploys a suite of tools to minimize their enables organization and cooperate to enjoy following functions such as the mobility and productivity benefits of WLANs without putting valuable information data in a risk. A good WLAN security policy should identify who may use WLAN technology and what type of access required implementing, it should describe who can install access points and other wireless infrastructure equipment, it should describes the type of information that can or cannot be sending over internet link, it should reduces the number of staffs that can have access to the network database, it should describe the hardware and software component and configuration for any access device and it should provide guidelines on reporting losses of the network devices and security incidents as well as define the frequency and scope of security assessments, audits and report generation (Irvine, 1998; U.S Robotics, 2009).

Methods of Network Attacks

When an organization security measures and controls are not properly put in place, an unauthorized user might interrupt implemented valuable information. There are various types of attack; which is passive (monitoring of information) and active (data are targeted with intent to corrupt or destroy the database) (Casey, 2001). Below are some of these attacks:

I. **Eavesdropping:** Figure1 depicts the network topology that represents an eavesdropping situation, when communications occur in an unprotected or clear text format, which allows man-in-middle to gain a read/write access to the packets in the network's database. A network experience eavesdrops when communications are sniffing or snooping. The ability of administrator to monitor the network is a big challenge. The network administrators are facing with a lot of network security problems in an enterprise e.g. casual War-drivers are set of attackers (those with laptops roaming around looking for network to hop onto). These attackers do no damage as they are motivated by the thrill and ease of gaining access to open and free networks which they map and share with friends and pals. Without proper management and strong authentication services that based on integrity and cryptography information can be read and rewritten by unwanted users(Arash *et al.*, 2009)..

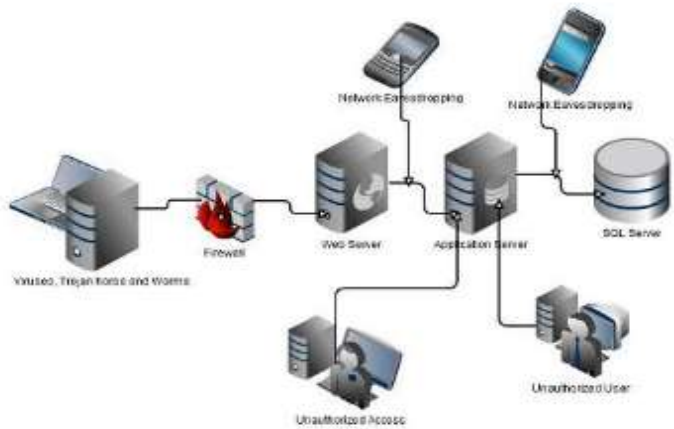

Figure 1: Eavesdropping (Utkarshni and Ankita, 2016)

II. **Data Modification:** Sophisticated software is use by attacker to collect data and break the security of a network. For example, the figure 2 shows how an attacker (MTM connection) sends a fake message in order to comprise the client network (victim) and pretend like a legal ISP provider. Man-in-the-middle or hacker are refers to as as criminals by United States FBI because they are involved in various crimes via the internet such as exploitation of valuable information, stealing of documents and accessing databases illegally (Ghappour, 2017). Unauthorized users (hackers), virus attacks and ignorance of others are threats that arise from both external and internal entities in any network. All the exploits data have modified and rewritten or read by attack without the knowledge of the legitimate owner. For example, a victim is a person that unauthorized users (Casey, 2001), exploit his or her computer information.

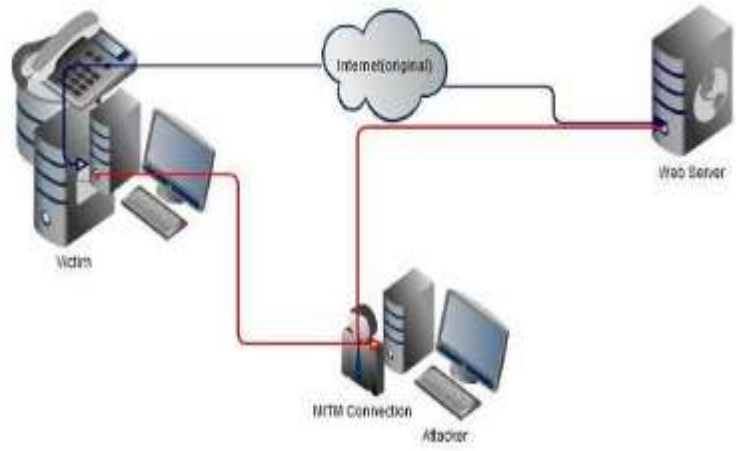

Figure 2: Data Modification (Utkarshni and Ankita , 2016)

III. **Identify Spoofing (IP Address Spoofing):** The network equipment with an operating system uses the IP address of a computer to identify a valid address. From the figure 3 below, it is possible for an IP address of a client to modify by an attacker in order to able to read and write their information. Special application can also be use by attacker to manipulate IP packets that appear to originate from valid addresses inside the corporate internet. An attacker after having access to the network as a result from modifying valid IP address can rewrite, or delete the information. For example, the figure 3 show how evil is an ssh attacker with a reddish devil hearth.

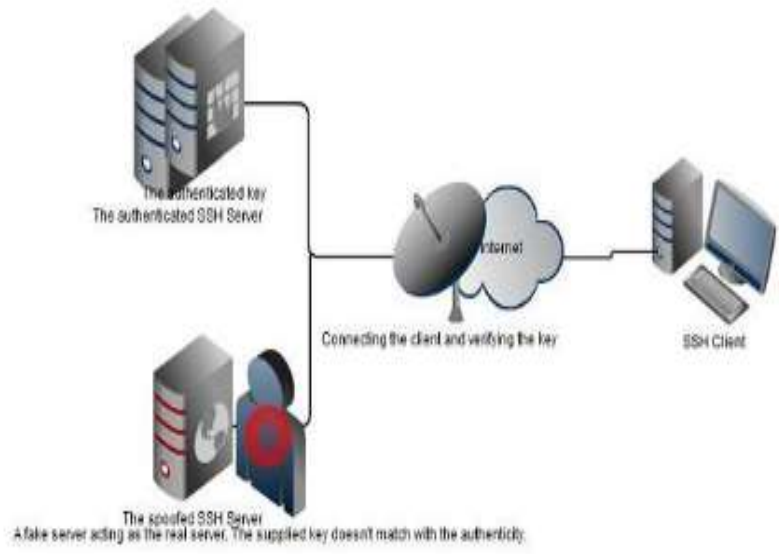

Figure 3: Identify Spoofing (Utkarshni and Ankita, 2016)

IV. Sniffer Attack: A sniffer attacker uses an application or device to read, rewrite, monitor, and capture network information that is exchanges during transmission of packets. If the packet is not well encrypted, the sniffer gains a full view of the data inside the packet. Even encapsulated packets are compromise and read by an attacker unless encrypted, and no access to the key. If access is gain, the network will be analyse and gain information to eventually cause the network to crash or become corrupted and also read the IP packet sent over the communication (Casey, 2001).

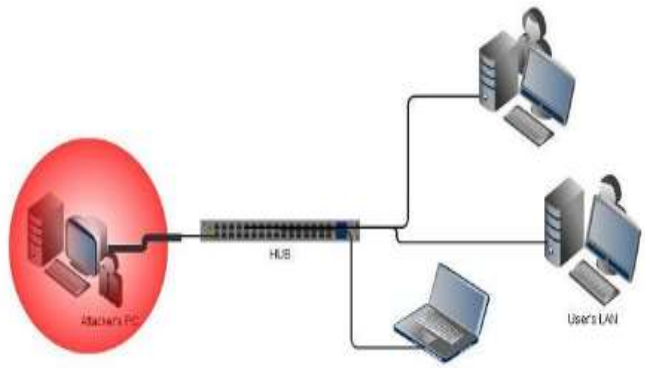

Figure 4: Sniffing (Utkarshni and Ankita, 2016)

A typical example of sniffer attack is the figure 4 diagram, shows how an attack carried out their operations a network environment. The attacker use special application program sniff the client network by injecting or capture network address. It reads and compromise client address in order to exploit their valuable information.

V. Application-Layer Attack: An application-layer attacker targets application servers by using a special technology to crack a server's operating system or password, given war-driver attackers to gain the ability to bypass access controls of a given network. The attacker

takes an advantage of this situation such as controlling the application, system, and network. Some examples of these attacks are; virus program that uses software applications to launch viruses over the network should be implemented, sniffer program to capture the network information should be introduce, that is used as a cracking tool or to corrupt the network, abnormally terminate of the applications and operating systems, and disabling the security component of a network to enable him to have future control and access over the network (Casey E., 2001). Figure 5 depict the above tasks:

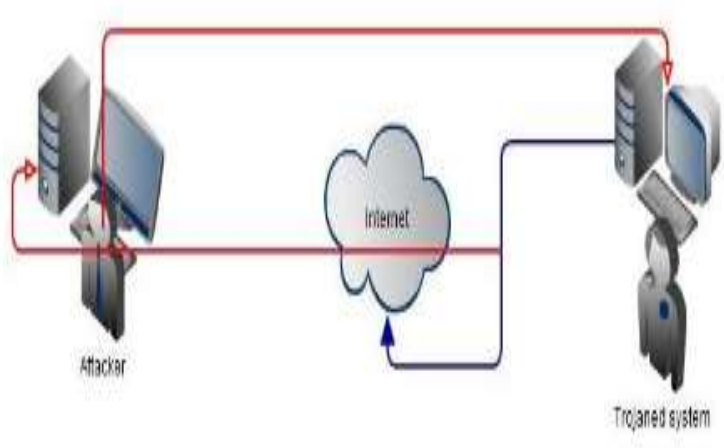

Figure 5: Application-Layer-Attack (Utkarshni and Ankita , 2016)

VI. **Password-Based Attacks:** This is a situation whereby an attacker compromises a valid account from original users and, the attacker pretends as the legitimate owner of the account to enable him/her, perform the same right as the real user. Therefore, both the legitimate and attacker has the same right. For example, if the user has administrative rights, the hackers also create accounts for subsequent access at a time. The man-in-the-middle can perform the following tasks: (i). Password calculator software was one of method required for brute force attack. (ii) To modify IP addresses and network configurations, including access controls, MAC address and routing tables. (iii) To modify, rewrite, or delete valuable information (Utkarshni & Ankita , 2016).

VII. Compromised-Key Threats: A unique code or number necessary to interpret secured data is term as a key. Obtaining a key is a difficult process and resource-intensive for an attacker, but with the help of brute technique. For example, fig. 6 below shows how it is possible for the hacker to compromise network address, after the attacker has access to the code, and these codes are referred to as a compromised key. It used the compromised tool key to gain access to a protected data during communication without the awareness of the sender and receiver. With the compromised technique, the attacker can decrypt and modify the database and, to use the compromised tool key to compute additional keys. According to Casey (2001) this kind of threats allows the unwanted users or friends of attacker gain access to other secured networks.

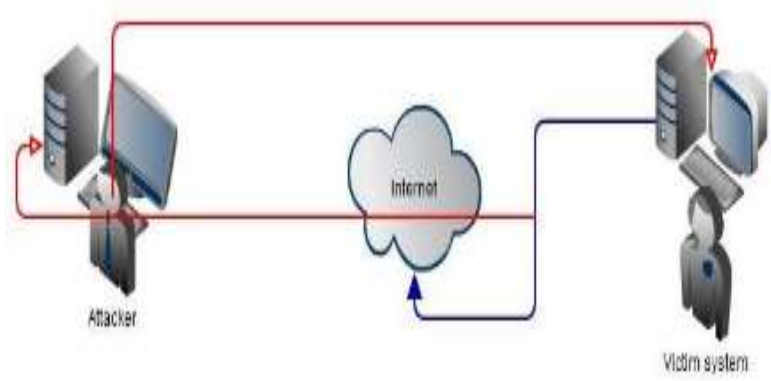

Figure 6: Compromised-Key-Attack (Utkarshni and Ankita, 2016)

VIII. **Denial-Of-Service Attack (DoS):** Unlike a password-based attack, the denial-of-service (DoS) attack prevents normal use of the computer valid accounts and, According to Casey (2001) DOS performs the following functions: (i) it randomizes the attention of the administrative staff so that they do not acknowledge the threat immediately, which allows the attacker successively, carries out the attacks during the diversion. (ii) It also sends invalid applications or network services which causes the vulnerabilities behaviours of the applications. (iii) It floods the entire computer network with packets until a shutdown occurs because of (due to) the overload, (iv) It blocks traffic, because of loss of access to network resources by authorized users

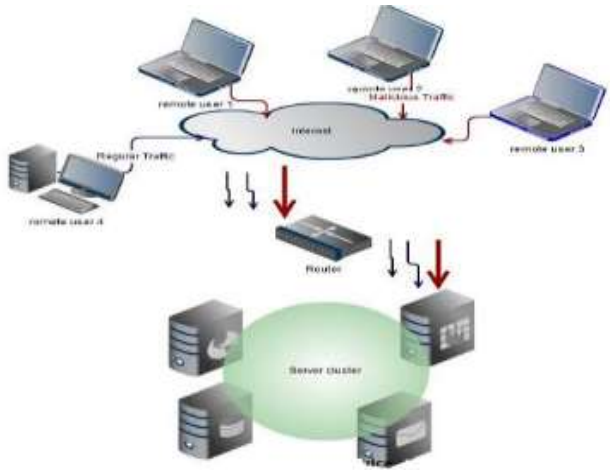

Figure 7: Denial-of-Service Attack (Arash *et al.*, 2009).

From the figure.7, a denial of service attack is special among all other threats that attack large websites on the internet. Denial of service hack the system that designed to bring the network to compromises stage by flooding it with unnecessary packet. The denial of service can experienced when a system such as a web server and database, has been flooded with illegitimate requests, thus making it impossible to respond to real tasks. For example, Yahoo!, MSN, Face book, and EBay were both victims of such cyber threats. The function of DOS attacks is the following: (i) Slow network performance, (ii) Restriction of client's right to access any website and (iii) A dramatic increase in spam receives in the email account (Casey E., 2001).

IX. **Malware Attack:** A malware is the so-called malicious software that can cause damage to home, office, and business computer systems. A cyber attacker's intention to always to able to have full control over client's private information such as credit cards, name, email address, social security numbers aiding attackers to steal people's identity or money. For example, a malware is a Tsunami Trojan. The Tsunami Trojan has effect mostly on the window such as Mac is UNIX and derives a platform that can increase a user base follows prospect of vulnerabilities exploit.

X. **Social Engineering:** Figure 11 depicts Social engineering scenarios where attackers use deception to gain access to information database. The method such as telephone, e-mail message and spam logs. The man-in-middle usually pretends to be a real owner or a director in the company such as travelling agent, business organization with a deadline to get some valuable data left on their network drive. Inquiries are make from the help desk to give them the toll-free number of the RAS server to compromise and sometimes get their password reset. The main target of the social engineering attack is to place the human element in the network-breaching loop and use it as a weapon. The human elements refer to as the weakest technique in the global network security.

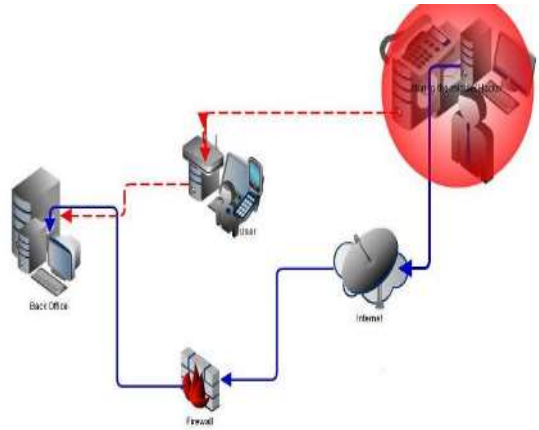

Figure 11: Social Engineering (Arash *et al.*, 2009).

Possible Solutions to Network Threats

i. **Users Catalogue:** The training such as scanning attachment download files before the opening them and logging off the computer if not used should be done. Educating the users about possible threats and damage caused by ignorance are very important.

ii. **Create a User Profile of Each Client:** Avoiding using the administrator account all the time, install or remove network component's software. A strong password of eight characters that contain at least three digits and a special character is advice, it make it tough for hackers or man-in-the-middle to break into a network. The technique of implementing user control, it is a very good method to mitigate and control the information security policy without linked out to the unwanted users.

iii. **Restricting Management Access Using Control List:** Access control list (ACL) should be use to manage and restrict remote access traffic in the prevention of unauthorized access and denial of service attack against a management interface. In conjunction with distance vector and link-

state routing protocols an ACL mechanism should be used. The idea of reducing access of co-workers to database account of a particular organization is one of major technique to govern and secure database information from modification or exploit by unwanted users.

iv. **Update the Operating System:** Updating the operating system helps reduce the vulnerabilities such as the developer identifies patch, weaknesses in the operating system. If your devices are malfunctioning because you didn't perform your update, it is possible you lost your valuable data to a cyber threat, or spent whole days trying to scan for a virus, you learned a valuable lesson about the need to secure your computer. All users have to update their systems and stop using devices prone to vulnerabilities such as Microsoft Windows 95, Windows 98, and Windows ME. These obsolete versions of Microsoft Windows are prone to attack and vulnerabilities. Every time you use your computer to transact or send vita information via the internet may put you at risk such as losing your vital information to the hacker. The method of upgrading device to Windows operating system such as: XP Service Pack 2, Vista, Win7, and Win8, which designed to replace older Windows and considered more secure.

v. **Vulnerability Scanner:** Checking whether a website and applications are vulnerable to SQL injection and PHP attack is by installing a licensed anti-virus (web scanner). Web scanners crawls entire website and automatically check for vulnerabilities to cyber threats. It will indicate which script is vulnerable and fix the vulnerability easily. It also ensures a website is secure by checking across site scripting program and other vulnerabilities. It performs so many tasks such as authentication pages, auditing shopping carts, forms, dynamic content, and other web applications. It is designed or program in such a way that after completing scanning of system, it produces detailed reports that pinpoint where vulnerabilities exist and remediation techniques.

vi. **Wired Equivalent Privacy (WEP):** The WEP security technology was originated from RC4'RSA data encryption technology. The WEP is use for different wireless end devices' encrypted communication that prevents unauthorized users sniffer the network or intrude into the wireless network. The WEP has two authentication mechanisms such as (open system authentication) and (share key authentication). The WEP is not perfect for use in wireless network systems because RC4 is one kind of a stream cipher in which the same key cannot use as second timers. The password is not secure when users transmit plain text password. The plain text password is very easy to break by malicious people (AvHarold et al., 2009)

vii. **WI-FI Protected Access (WPA):** The WPA is a mechanism used for project wireless network systems that provide an effective encrypt passwords between different wireless ends. The WPA uses one standard method to encrypt, which is (Temporary key integrity protocol). There are two types of authentication e.g. 802.1x authentication mechanism and pre-shared key mode. According to Arash *et al. (*2009) WPA versions and protection mechanisms can be differentiated based on the (chronological) technological operation of WPA and the target end-user (according to the method of authentication key distribution), and the encryption protocol used.

viii. **Wireless Intrusion Prevention System (WIPS):** The Wireless Intrusion Prevention system is an effective way to prevent unauthorized access to local area networks and the other information that may influence wireless network performance (Arash *et al*., 2009). The WIPS is a good way to project wireless network infrastructure. The WIPS consist of these components such as a sensor, server, and console (David *et al.*, 2003). Finally, the sensor performs various kinds of test such as scans the wireless spectrum packets, discovers server and captures the

unauthorized behaviours. After that the console provides, the primary user interface into the system for administration and reporting.

ix. **Wireless Intrusion Detection System (WIDS):** The wireless intrusion detection system monitors the radio spectrum for unauthorized behaviours. This system monitors the wireless spectrum based on the wireless local area network. If the WIDS detect unauthorized information, it will immediately send awareness to administrator (David M.*et al.*, 2003). Sensors, Server, and Console are the three components of WIDS. A WIDS can be a single system that connected to a wireless radio signal device, and antennas placed throughout the facility.

x. **Firewall:** The Firewall and endpoint anti-malware products are essential security tools, but they are inadequate in the face of these bad omens (hackers). The firewall is an important cornerstone of the network security and it is generally, first line of defence against internet-based threats. The traditional firewall most are inbuilt into devices system and some new generation firewall can installed by following the guide and manual catalogue provided from the manufacture. It is easy to operate and maintain, but are also relatively unsophisticated and therefore ineffective against many of today's advance network threats. The traditional firewall is not design to inspect the application content. An attack from an allowed IP address or port can often simply bypass a firewall. Due to the weakness of traditional firewall, the new generation firewall is programmed such as to recognize and discover threats so fast and acknowledge by giving alarm sound. The endpoint anti-malware detects and blocks many unwanted mail and attacks, but its effectiveness has decreased in the face of extremely sophisticated techniques.

Methods and Material Adopted for the Research

The methodology adopted in the research of the work was the qualitative research methodology. Extensive review of relevant literatures on computer network, vulnerabilities and approaches use by attackers in penetrating a given network was carry out for deep understanding of the title in question.

▪ Vulnerability Analysis of a Computer Network

The processes of reviewing and analyzing endpoint and device networks for security issues is refer to as network vulnerability assessment. The assessment may detect network flaws and holes in the network that can expose an opportunity for hackers to exploit. Porous defense vulnerabilities, Risky resource management vulnerabilities, Vulnerabilities related to insecure interaction between components are some types of security vulnerabilities (Daniel, 2018). Most often, vulnerability assessment and penetration test of a network are mixed up in the discourse of the issues of network security but are not completely same. Both happen to be part of the activities being carried out in the vulnerability analysis of a network.

▪ Vulnerability Analysis/Assessment and Penetration Test

Vulnerability assessment is the security test for compiling a complete list of vulnerabilities in a network (Daniel, 2018). Vulnerability assessment is designed to yield a prioritized list of vulnerabilities to help clients who already understand they vulnerabilities issues terms of security. The customer already knows they have issues and simply need help identifying and prioritizing them. The more issue identified the better. When possible a white box approach should be embraced. The deliverable for assessment is most importantly, therefore a prioritized list of

discovered vulnerabilities and how to remediate them is needed. While Penetration tests are designed to achieve a specific, attacker-simulated goal and should be requested by customers who are already at their desired security posture. A prized customer database on the internal network, or to modify a record in a high ranking system is a good example. An example is the deliverable for penetration test of how security was breached in order to reach the agreed-upon goal and how to remediate it.

- **Tools used in Vulnerability Analysis of a Network**

A vulnerability Scanner is a program that performs the diagnostic phase of a vulnerability analysis. According to Noel (2016) vulnerability analysis helps to defines, identifies, and classifies the security holes in a computer, server, network, or communications infrastructure Vulnerability scanners are used for different kinds of vulnerability analysis. The table below shows different kinds of vulnerability analysis, the expected vulnerability and the scanning tools used.

Table1: Vulnerability analysis, the expected vulnerability and the scanning tools used (Noel, 2016).

TYPES OF VULNERABILITY ANALYSIS	**EXPECTED VULNERABILITIES**	**SCANNING TOOLS**
Network Vulnerability Scanner	• Missing Patches (known vulnerabilities) • Insecure Server Configurations • Open Ports	• NMAP • Nessus • OpenVAS • Retina
Database Scanner Specifically designed for databases	• Weak password policies • Default accounts • Security of admin accounts • Misconfiguration	• Scuba • Qualys
Source Code Analysis Static Application Security Testing (SAST)	viii. SQL Injection ix. OS Command Injection x. Buffer Overflows xi. Cross Site Scripting xii. Missing authentication for Critical Function	x. Coverity xi. Cpp Check xii. HP Fortify xiii. Parasof
Fuzzing	v. Feeding variations of unexpected input into a vi. program in an attempt to uncover unexpected ii. Behavior.	• Basic Fuzzing Framework (BFF) • OWASP • WebScarab • Peach Fuzzer

- **Steps for Identifying Vulnerability in a Network**

There are pertinent steps to be followed to identifying vulnerability of any network. Below are those steps (Khajeh *et al.*, 2010);

- Identify and realize the approach of your company or industry like how it is structured and managed.
- Trace the data, systems, and applications that are exercised throughout the practice of the business.
- Examine the unobserved data sources capable of allowing simple entry to the protected information.
- Classify both the virtual and physical servers that run the essential business applications.
- Track all the existing security measures which are already implemented.
- Inspect the network for any vulnerability.

Discussion

In the research work vulnerabilities phenomenon, types of vulnerability analysis, expected vulnerabilities associated with type of vulnerabilities and scanning tools were review. The research enlightens network administrators and organization the importance of vulnerabilities analysis in their network to prevent network attackers from intruding into their network. The result of the review shows that issue of vulnerabilities analysis using the available scanning tools should not be taking lightly. Vulnerabilities are usually assessed in isolation, without considering how they contribute to overall attack risk. Similarly, intrusion alarms are logged as isolated events, with limited correlation capabilities. Security professionals are overwhelmed by constant threats, complexity of security data, and network growth. Vulnerability testing processes are mostly carried out in two levels, the external and internal vulnerability testing levels. In external vulnerability testing, we test your network from the outside from a "hacker's point-of-view". We use the same tools criminals use to try and compromise your network and servers. While in internal vulnerability testing, the same tools used in the external test is used. This type of assessment is essential in understanding how and why hackers, viruses and worms spread so quickly through an organization (Kellep, 2015). In Dwianto, (2016) several evolution processes where highlighted to have led to the emergence of network vulnerability analysis. This ranges from: Attacks on computer systems via the use of Trojan horse or spyware, launching of denial of service attacks (DOS), on a node in a network, data interception and theft in a network, website phishing (cloning) and flooding, creation of security holes on server systems, radio jamming through wire sniffer on network devices, etc.

Conclusion and Recommendation

The importance of network vulnerability analysis cannot be over emphasized. Organizations that are information security conscious, implement network vulnerability analysis that made up of vulnerability assessment and penetration test activities in order to detect possible holes, get professional advice and harden their systems. The external and internal vulnerability testing levels of vulnerability analysis provides organizations advice to consider the perspectives of all the stakeholders and supposed intruders of a given in system as regards possible attacks. Numerous tools are available to help in the analysis of network and can equally help in the remediation of identified holes. The research highlighted steps to followed in order to achieve quality analysis and

system strengthening. This is limited to the exposition of the concept of network vulnerability analysis, the possible activities to be undergone and the tools and steps to analyzing a network.

From the results of the vulnerabilities analysis carry out and the resources materials such as textbooks, journals, articles, consulted it recommended that any organization using computer network should make use of the vulnerabilities scanning tools (examples: NMAP, Scuba) to analysis its network for any possible vulnerabilities to prevent cyber attackers from intruding into their network. Also, all possible methods of attacks should be acquitted with. Software intrusion detection system should also be installed to complement the existing method of attack on ground. Strengths and weakness of network protocols should be deeply understand. While current security technology should be put place to tackle this security menace.

Reference

Amit K. & Santosh M. (2015). Network security threats and protection models. Available at http://arxiv.org/abs/1511.00568.

Arash H. L., Masood M. & Aamir S. D. (2009). Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). International Conference on Signal Processing Systems, Singapore.

AvHarold F. Tipton & Micki K. (2009). Information security management handbook. Auerbach Publications.

Casey, E. (2001). Handbookof Computer Crime Investigation: Forensic Tools and Technology, Academic Press, Singapore.

Daniel M. (2018). Differences between vulnerability assessment and penetration testing. Available at: http://danielmiessler.com/study/vulnerability-assessment-penetration-test.

David M., Vern P., Stefan S., Colleen S., Stuart S., & Nicholas W., (2003). Inside the Slammer worm. IEEE Security and Privacy, 1:33–39.

Gao, X. (2015). Information security investment for competitive firms with hacker behaviour and security requirements, Annals of Operations Research. 235: 277–300. doi:10.1007/s10479-015-1925-2. S2CID 207085416.

Ghappour, Ahmed (2017). "Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web". Stanford Law Review. 69 (4): 1075.

Irvine, C. (1998). 'Center for Information Systems Security Studies and Research, NPS Research,

Khajeh-Hosseini, A., Greenwood D., James, J. W. & Sommerville, I. (2010). The Cloud Adoption Toolkit: Supporting Cloud Adoption Decisions in the Enterprise, Cornell University Library.

Montoro, M. (2009). Brute-Force Password Cracker.

Kellep A. C. (2015). The Security Vulnerability Assessment Process, Best Practices and Challenges.

Dwianto D. C. (2016). Vulnerability Assessment Network Security Workshop. http://www.slideshare.net/mobile/hack2secure1/vulnerability-assessment-tools-your-solution-for-fool-proof-system-protection.

Noel S. & Jajodia S. (2016). Advanced Vulnerability Analysis and Intrusion Detection through Predictive Attack Graphs. Available at: www.google.com/Advanced-Vulnerability-Analysis-and-Intrusion-Detection-Through-Predictive-Attack-Graphs.pdf.

Steven N. & Sushil J., (2017). Advanced Vulnerability Analysis and Intrusion Detection through Predictive Attack Graphs.

Utkarshni S. & Ankita G. (2016). Network Vulnerability Assessment, International Journal of Technical Research and Applications, Volume 4, Issue 1. Available at: www.ijtra.com.

Wright, J. & Jim H. (2009). Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257