Vulnerabilities in Network Infrastructures and Prevention/Containment Measures

Oludele Awodele, Ernest Enyinnaya Onuiri, and Samuel O. Okolie,
Department of Computer Science, Babcock University, Ilishan-Remo, Ogun State; Nigeria

delealways@yahoo.com, nesto4eva@gmail.com, samuelokolie2003@yahoo.com

Abstract

Computer networks have arguably become ubiquitous (having grown exponentially over the last 15 years) and synonymous with organisations that thrive on excellence. Hardly will anyone setting up a firm today, do so without thinking of the modalities of incorporating an efficient computer network infrastructure that connects the business to the outside world especially via the internet. This is because present day businesses depend heavily on platforms and network infrastructures that make communication easy, efficient, available and accessible. Robust computer networks provide such basis for interactivity, thereby bringing a whole lot of people and businesses together. Also, in this age of the internet, almost anyone anywhere, can access information from any part of the world. Consequently, all these have amounted to growing security concerns over the years, critical across sectors and industries. In this paper, a comprehensive study of some network vulnerabilities is carried out and counter-measures on how they can be prevented or contained to prevent malicious attacks and how to prevent wanton escalation in the event of a successful attack.

Keywords: Networks; Vulnerability; Threat; Infrastructure; Prevent; Contain; Attack

Introduction

Computer networks are devoted infrastructures setup to facilitate the carrying of traffic such as data, voice, video etc. from one node to another. They consist of a varying number of nodes or stations, connected by various communication channels and devices.

Given the numerous attacks which computer networks encounter, the question of network security becomes indispensable given the fact that the damages are most times colossal and highly detrimental to the victims, whether as an individual or as a corporate entity. The complexities in today's networks have brought about bigger challenges in preventing security breaches. Today's network support cutting-edge capabilities and functionalities such as teleconferencing, video conferencing, file sharing, wireless connectivity, remote access, voice over internet protocol (VoIP), unified communications, mail services, e-business and resource sharing (e.g. printers), to mention but a few.

The integration of these cutting-edge and complex functionalities coupled with other factors has made networks vulnerable to countless disastrous security threats and attacks. Some of these threats include phishing, SQL injection, hacking, social engineering, spamming, denial of service attacks, Trojans, virus and worm attacks, to mention but a few – the list is endless and on the increase. Whereas measures are being taken every now and then to curtail the extent to which systems are vulnerable to these sorts of attacks, perpetrators of these vices are improving on the sophistication of their attack procedures, tools and mechanisms.

In November 1988, a programmer named Robert Morris launched the first prolific worm. The worm was a self-replicating computer program released into the internet as an experiment on diffusion. Though Morris originally launched the program at MIT, within a few hours, the worm had rendered computers throughout the university system, military, and medical research facilities, useless. The worm was only intended to spread; instead, it spread and, on account of bugs in the software, crashed many systems along its path. Consequently, the United States General Accounting Office (GAO) went on to estimate that the total cost of damage caused by the "Morris Worm" was approximately USD $10-$100 million. Ironically, when Morris and his friend realized the extent of the damage, they made efforts to send warning messages throughout the network. However, on account of system breakdowns, or because people had terminated their connection to the network entirely, the message did not reach users quickly enough, or rapidly enough. Morris was eventually charged over $10,000, sentenced to community service and three years of probation, for violating the Computer Fraud and Abuse Act. Importantly, this is an example of unintended consequences. However, a lot of malicious and deliberate efforts are made today by attackers to launch such malicious codes capable of causing serious harm to networks on both the local and global scale (Kellermann & Nishiyama, 2003).

Security vulnerabilities associated with computer networks have risen among the foremost concerns for network and security professionals because it consistently provides serious threats to the efficiency and effectiveness of organizations (Curry, Hartman, Hunter, Martin, Moreau, Oprea, Rivner, Wolf, 2011). Before a hacker breaches the security of an organization it is without a doubt important for the network administrator to proactively determine the network's security vulnerabilities. Given the imminent challenges arising from this, it becomes necessary for organisations to adequately invest in measures that will proactively curb this security menace that has at some point, brought supposed robust computer network infrastructures to a standstill. The implementation of standardization and compliance measures is also of the essence. Consequently, network vulnerabilities need to be identified and eliminated or curtailed to bridge the gulf between an organization's present stage and desired future expectations.

Related Works

Anderson (2002), reckons that computing systems that are connected to a network are subjected to one form of security risk or the other. Though efforts have been made on different fronts to identify the different causes of causes of vulnerabilities and viable countermeasures, it is only recently that development of systematic and quantitative methods begun. Also there exists a considerable debate that attempts to compare the security attributes of open source and proprietary software.

Pfleeger C.P and Pfleeger S.L. (2003) define vulnerability as a software defect or weakness in the security system which could lead to exploitation by a malicious user thereby causing loss or harm. They further opine that the security of systems connected to the internet depends on several components of the system. These components include the operating systems, HTTP servers and browsers.

Reza, Mohammad, Marjan, Rasool and Ali (2010) showed how an attacker may chain what could be termed as a simple attack to launch a complex attack. This goes to show how security evaluation has become a very important requirement in the design and management of computer networks. Consequently, in the process of evaluating the security of a network, it is no longer enough to simply consider the single vulnerabilities without considering the other hosts, their association and how they communicate, as well as their network infrastructure. Without a doubt, many of these attacks exploit the global weaknesses in a network as facilitated by their interconnections.

Menkus(1990) posits that all data communications processes can be said to be structurally insecure. Also, these processes are classified as some number of links. Each of these links has three components irrespective of how large or complex the data communication network involved may be. These components are origination, transmission, and reception. Almost all telecommunication theory and computing management attention is given to the first and third of these components. These components are functionally reciprocal. They are the elements of the data communications process that are tangible and that can be subjected to some form of direct control by those involved in this activity.

Findings carried out by Kraemera, Carayonb & Clemc (2009) suggests that human and organizational factors play a significant role in the development of Computer and Information Security (CIS) vulnerabilities and place great emphasis on the complex relationships that exist between human and organizational factors. They further categorized these factors into 9 areas: external influences, human error, management, organization, performance and resource management, policy issues, technology, and training. Security experts who manage networks need to be aware of the different roles of human and organizational factors. Also, CIS vulnerabilities cannot be said to be the sole result of a technological problem or programming mistake. The design and management of CIS systems need an integrative, multi-layered approach to improve CIS performance.

In recent times, Lai and Hsia (2007) reckon that the security problem has become very important to computer users. This is also baring in the mind the fact that vulnerabilities on computers are found so frequently that system managers are not able to fix all these vulnerabilities on hosts within the network in a short time. This is because they need to carry out risk evaluation so as to ascertain the priority of fixing the vulnerabilities. To isolate these vulnerabilities on hosts from possible exploitation, system managers can set the ACL scripts on network devices. This measure is able to improve security in the network right away, due to the fact that some endangered service ports on hosts are blocked from access. They adopt this method to improve network security, which consists of the network management, the vulnerability scan, the risk assessment, the access control, and the incident notification.

Computer Networks

A computer network is a collection of devices that can communicate together through defined pathways. It is in a sense the fabric that binds business applications together. It ranges from peer-to-peer, personal area networks (PANs), local area networks (LANs), campus area networks (CANs), storage area networks (SANs), metropolitan area networks (MANs) and wide area networks (WANs). Sometimes, there is the need for internet connectivity to facilitate wide coverage area reach. A functional computer network can basically be composed of personal computers, network interface cards, servers, routers, switches, cables, protocols, applications and so on.

Common topologies used to implement network connections include ring, bus star, mesh, and hybrid. However, star is the most widely used topology due to its flexibility, efficiency and robustness. The medium of communication may be based on wired or wireless technologies and can be necessitated by varying factors.

In addition, an internetwork can be created by connecting two or more LANs or WANs. Applications that run on these networks include e-mails, instant messengers, online games, web browsers, file transfer protocol and database applications to mention but a few. Transmission of data follows a set of rules and guidelines prescribed by the Open Systems Interconnection (OSI) Model which consists of seven layers namely – application, presentation, session, transport, network, data-link and physical layers.

Network Vulnerabilities

Malicious users are always on the prowl to sneak into networks and create problems and consequently, they adversely affect several businesses around the world as a whole. In 2002, the CSI/FBI Computer Crime Security Survey noted that 90 percent of respondents acknowledged security breaches, but only 34 percent reported the crimes to law enforcement agencies (Knapp & Boulton, 2006). This fact goes to show that no system is absolutely immune from such potential security breaches.

In general terms, system vulnerability is a flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect an organization's operations or assets through a loss of confidentiality, integrity or availability (NIST, 2010).

What then is network vulnerability? As plain as this might seem, this concept is quite an uneasy term to define. On the surface, network vulnerability is anything that poses a potential avenue for attack or security breach against a system. This can include things like viruses, passwords written on sticky pads, incorrectly configured systems and so on. This sort of vices increase the risk to a system, however there is a wider context to this concept than have been stated above as well as within the security community.

In view of the foregoing and in the context valuable to security professionals, network vulnerability is a security exposure that has the propensity to cause an unexpected and undesirable event that compromises the security of a network infrastructure as a result of the existence of a weakness, design, or implementation error. Inotherwords, network vulnerability is a flaw within a system that makes it impossible even where implementation and deployment is properly done, to prevent an intruder from unauthorised access to a network and a consequent alteration operation and data compromise on it; or the illegal usurping of trust. In most cases, especially where the vulnerability is software oriented, it is expected that such discovered flaws are fixed by the vendor through the release of patches.

The need for secure network has and will always be of paramount importance to anyone designing or administering it. The security of any network involves the well-being of information and infrastructure in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable (Kuhn, Walsh & Fries, 2005). A security network is one that boasts of an acceptable integrity (trustworthiness of data and network resources), authenticity (recognition and guarantee of the information origin), availability (condition whereby desired resources are accessible and obtainable) and confidentiality (privacy of information or resources). It is often said that if a hacker wants to get inside your system or network as the case may be, there is nothing you can do about it. Perhaps, what can be done is to exhaust all avenues at making it extremely harder for the hacker to breach the system's security.

Some network/system vulnerabilities include (but not limited to) the following:

1. Insecure/exposed Ports.
2. Indiscriminate enabling of services.
3. Improper system configuration.

4. Poor anti-virus implementation.
5. Poor firewall deployment.
6. Poor intrusion detection system (IDS) setups.
7. Week password implementation.
8. Easy access to information.
9. Downloading of files and applications from sites that are not trusted.
10. Unsecure applications/programs as a result of poor programming practices.
11. Application backdoors.
12. Lack of appropriate security policies.
13. Not giving attention to security indicators – users fail to give proper attention by refusing to read the warning messages or security indicators.
14. Disgruntled employees.
15. Lack of efficient physical security.
16. Insufficient security training and awareness.
17. Carelessness on the path of users.
18. Corporate Espionage.

The causative factors listed above can be summarised into two categories:

1. Application/software vulnerabilities
2. Human related vulnerabilities – users being weak links through which breaches can be made to the security of networks/systems.

Some Modes of Attack

1. Hacking: this is the unauthorised accessing of a computer system for data or information belonging to someone else. The hacker does this by exploiting a target systems' weakness or vulnerability. A hacker has the ability to use the techniques of both viruses and worms, however, the hacker may avoid IDS (Intrusion Detection System) detection by cleverly disguising the attack. Kevin Mitnick, notable for his hacking exploits, largely used social engineering techniques to break into systems (Newson, 2005). In view of the foregoing, there are various channels through which a hacker can gain access to a system. These include:
    a. Application-level attacks: this is because today, software developers are most times under pressure to deliver products in good time coupled with the increase in demand for extreme programming within software engineering methodology. The complex solutions being solved today have given rise to huge amounts of features and functionalities in what applications deliver. All these needs sometimes make time of the essence and because this factor is not always sufficient, total and conclusive testing is scarcely accomplished before the product is released. Most times implementation of security tools become an afterthought and are delivered as "add-on" components. Buffer Overflow Attacks can be used to breach such insufficiently secure applications due to poor or non-present error-checking features (Berg, 2007).
    b. Misconfiguration attacks: hackers get a field day around improperly configured system as a result of unprofessional management of such systems. Due to the complexities of systems today, administrators who are not very skilled are caught off guard by lurking hackers.
    c. Operating systems attack: due to the complexities of today's networks, operating systems run many services, ports and modes of access and would take an awful lot to prevent a potential security breach. Great deals of services are kept running likewise open ports when the default settings of operating systems are implemented during in-

stallation. Hence, in order to gain unauthorized access to network systems, hackers look for and exploit operating system vulnerabilities (Chen & Davis, 2006)).

2. SQL injection: this is a type of security exploit whereby the attacker injects Structured Query Language (SQL) code through a web form input box, to gain access to resources, or make changes to data. Here, the attacker injects SQL commands to exploit non-validated input vulnerabilities in a web application database backend and consequently execute arbitrary SQL commands through the web application. Because programmers use sequential commands with user input, it makes it easier for attackers to inject commands. (Dahse, 2010)

3. Password cracking: Password cracking is a term used to describe the penetration of a network, system, or resource with or without the use of tools to unlock a resource that has been secured with a password. Password cracking doesn't always involve sophisticated tools. It can be as simple as finding a sticky note with the password written on it stuck right to the monitor or hidden under a keyboard. Another crude technique is known as "dumpster diving," which basically involves an attacker going through garbage to find discarded documentation that may contain passwords. Of course, attacks can involve far greater levels of sophistication and this includes the use of techniques such as brute force, dictionary and hybrid attacks. There exists the possibility for password crackers to identify encrypted passwords, retrieve such from a computer's memory and then decrypt it. The aim of a password cracker is mostly to obtain the root/administrator password of the target system; this is because the administrator right gives the attacker access to files and applications and can install a backdoor, such as a Trojan, for future access to the system. The attacker can also install a network sniffer to sniff the internal network traffic so that he will have most of the information passed around the network. After gaining root access, the attacker escalates the privileges to that of the administrator. Usually, the attacker uses a system that has a greater computing power than that of the target for efficient cracking of the password (Shimonski, 2002).
4. Phishing: this is a way of attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public and consequently a user is convinced to give away valuable information. This is further achieved by redirecting the user to a different website through emails, instant messages etc. Phishers offer illegitimate websites to the user to fill personal information. The main purpose of phishing is to get access to the customer's bank accounts, passwords and other security information. Attackers can get the audience through mass-mailing millions of email addresses around the world. Phishers can fool users by convincing them to get into a fake website with the domain name slightly different from the original website which is difficult to notice. They use the images of the legitimate hyperlink, which itself helps as a hyperlink to an unauthorised website. Sometimes, Phishers also exploit SMTP (Simple Mail Transfer Protocol) flaws. In general, phishing involves registering a fake domain name, building a look alike website and then sending emails to many users (Tan, 2006).
5. Social engineering: this is the human side of breaking into a corporate network. Companies with authentication processes, firewalls, virtual private networks (VPNs) and network monitoring software are still open to attacks. An employee may unwittingly give away key information on an email or by answering questions over the phone with someone they do not know, or even by talking about a project with co-workers at a local bar

after work hours. It is the tactic or trick of gaining sensitive information by exploiting the basic human nature such as: trust, fear and the desire to help. Social engineers try to gather information such as: sensitive information, authorization and access details. Social engineering is the hardest form of attack to defend against because it cannot be defended with hardware or software alone and because people are the weakest link in the security chain, a successful defense will be to have good policies and the education of employees to follow such (Peltier, 2006). Eavesdropping, shoulder surfing, dumpster diving (searching waste/trash bins for valuable information), tailgating, piggybacking etc. are all ways through which social engineers carry out their activities.

6. Sniffers: this is a program or device that captures the vital information from the network traffic specific to a particular network. Sniffing is basically a data interception policy whose objective is to steal passwords (from email, the web, FTP, SQL or telnet), email text, files in transfer etc. Protocols vulnerable to sniffing include telnet, HTTP, FTP, POP, NNTP, SMTP and IMAP. Sniffing can be passive (sniffing through a hub, this is difficult to detect) or active (sniffing through a switch). (Gandhi & Srivatsa, 2010).

7. Viruses and worms: a virus is a self-replicating malicious program that replicates its own code by attaching copies of itself into other executable codes and operates without the knowledge of the computer user posing serious threat to both business and personnel. It resides in the memory and replicates itself while the program where it is attached is running. It can transform itself by changing codes to appear different. Viruses hide themselves from detection by encrypting themselves into the cryptic symbols, altering the disk directory data to compensate the additional virus bytes or using stealth algorithms to redirect disk data. Worms on the other hand are distinguished from viruses by the fact that a virus requires some form of human intervention to infect a computer whereas a worm does not. A worm can also be said to be a special type of virus that has the ability to replicate itself and use memory, but cannot attach itself to other programs. A worm spreads through the infected network automatically but a virus does not. Some indications of virus threat include:
   a. Programs take longer to load than normal
   b. Computer's hard drive constantly run out of disk space
   c. Files have strange names which are not recognizable
   d. Programs act erratically
   e. Resources are used up easily.

8. Trojan: this is a malicious application that is unable to spread of its own accord. Historically, the term has been used to refer to applications that appear legitimate and useful, but perform malicious and illicit activities on an affected computer. Trojan types include security software disablers, data-sending Trojans, remote access Trojans, destructive Trojans, proxy Trojans, FTP Trojans, denial-of-service Trojans. In general, Trojans can gain access into a system through physical access, instant messenger applications, attachments, browser and email software bugs, fake programs, untrusted sites and freeware software, downloading files, games and screensavers from the internet, legitimate shrink-wrapped software package by a disgruntled employee etc. Most times they reside deep in the system and make registry changes that allow it to meet its purpose as a remote administration tool. With the Trojan, a whole lot of protocols and ports come under severe attacks. Popular Trojans include back orifice and netbus (Microsoft Malware Protection Centre, 2011). Some manifestations of Trojan attack include:

a. CD-ROM drive opens and closes by itself.
b. Computer screen flips upside down or inverts.
c. Wallpaper or background settings change by themselves.
d. Documents or messages print from the printer themselves.
e. Screensaver settings change by themselves.
f. Computer browser goes to a strange or unknown web page by itself.
g. Windows colour settings change by themselves.
h. Right and left mouse buttons reverse their functions.
i. Windows start button disappears.
j. Mouse pointer disappears.
k. Mouse pointer moves and functions by itself.
l. Strange chat boxes appear on the victim's computer.
m. The ISP complains to the victim that his/her computer is IP scanning.

9. Spamming: this involves populating the inbox of a target group with junk or unsolicited emails. Spammers get access to the email ID's when the user registers to any email service, forum, or blogs by hacking the information, or registers as genuine users. Spam emails sometimes contain malicious computer programs such as viruses and Trojans which cause change in the computer system or serves as a tracking tool on the system. Some techniques used to effect spamming include spoofing the domain, social engineering, directory harvesting, phishing, sending virus attached files, database poisoning etc. however, spamming has legitimate use as is the case in advertising (Bradley, 2009).

10. Buffer overflows: this takes place when a buffer that has been assigned a specified storage space, has more data passed on to it than it can accommodate. As a way of exploiting buffer overflow to gain access in order to gain or escalate privileges, the offender creates the data to be fed to the application; this is because random data will generate a segmentation fault or bus error, never a remote shell or the execution of a command (Kramer David, 2001).
    In July 2000, a vulnerability to buffer overflow attack was discovered in Microsoft Outlook and Outlook Express. A programming flaw made it possible for an attacker to compromise the integrity of the target computer by simply sending an e-mail message. Unlike the typical e-mail virus, users could not protect themselves by not opening attached files; in fact, the user did not even have to open the message to enable the attack. The programs' message header mechanisms had a defect that made it possible for senders to overflow the area with extraneous data, which allowed them to execute whatever type of code they desired on the recipient's computers. Because the process was activated as soon as the recipient downloaded the message from the server, this type of buffer overflow attack is very difficult to defend. Microsoft has since created a patch to eliminate the vulnerability (Kramer David, 2001).

Prevention/Containment Measures

Vulnerabilities can be successfully contained when certain measures are put in place such as asking the right questions and anticipating every step and potential threat. Such questions include ascertaining what the intruder can see on a target system, what the intruder can do with the information and if there are ways of substantiating the footprints after a potential breach. The ability to substantiate a security breach becomes handy for legal measures. It is incumbent on any network administrator to be adept with the design weaknesses that exposes an operating system and its corresponding applications to attack hence; a thorough understanding of products and technologies is paramount. Also, he gathers information about viruses and worms, identifies and correct network vulnerabilities, gets information that helps to prevent security problems and in the event of an eventual successful attack – a way to recover from such, in good time.

1. To prevent SQL injection,
   a. Lessen the privileges of database connections.
   b. Disable verbose error messages.
   c. Safeguard the system account.
   d. Audit the source codes
   e. Never trust user input instead, confirm by means of authentication, all textbox entries using validation controls, regular expressions, code and so on.
   f. Never use dynamic SQL rather, use parameterized SQL or stored procedures.
   g. Never connect to a database using an admin-level account rather, use a limited access account to connect to the database.
2. To prevent password cracking:
   a. Choose passwords that have at not less than eight characters.
   b. Passwords should have a combination of lower and upper case letters, numbers, special characters etc. This makes it difficult to crack.
   c. Do not use words that can be easily found in the dictionary as passwords.
   d. Do not use public information, such as social security number, credit card number and ATM card number as passwords.
   e. Never use personal information as passwords.
   f. Usernames and passwords should be different.
   g. Managers and administrators can enhance the security of their networks by setting strong passwords policies. This can be further enhanced by ensuring that password requirements are built into organisational security policies.
   h. When installing new systems, make sure default passwords are immediately changed. (Shimonski, 2002).
3. One good way of preventing phishing, is through the deployment of anti-phishing software. This software is known to detect phishing attacks within the website or in the customer's email. The software displays the real website domain that the customer is visiting by residing at the web browsers and email servers, as an integral tool. It is noteworthy that phishing attacks can be prevented at the server side and also the client side. Examples of these tools include: PhishTank Site Checker, Nercraft, GFI MailEssentials and SpoofGuard.
4. To prevent or curtail social engineering as a mode of attack is cumbersome. This is because it is very difficult to detect since there is no method that ensures complete security from a potential attack. There is no specific software or hardware for defending against a social engineering attack. However this menace can be minimized through:
   a. Trainings which should consist of all security policies methods to increase awareness on social engineering.
   b. Password policies: there should be periodic change in passwords, use of lengthy and complex passwords.
   c. Ensuring the security of sensitive information and authorised use of resources.
   d. Physical security policies such as identification of employees using biometrics, escorting of visitors, area restrictions and demilitarized zones (DMZs), proper shredding of useless documents and employing security personnel.
   e. Information should be classified into categories such as top secret, proprietary, for internal use only, for public use, and so on.
5. To prevent/contain the excesses of sniffers:
   a. Check which machines are running in promiscuous mode.
   b. Restriction of physical access to network media ensures that a packet sniffer cannot be installed.

c. Encryption: this is the best security measure against sniffers. It would not prevent a sniffer from functioning but will ensure that what a sniffer reads is not important.
d. Apply the latest patches or other lockdown techniques to the system.
e. Permanently add the MAC address of the gateway to the ARP cache.
f. Change the protocol used to facilitate remote login from telnet to SSH.
g. For small networks, use static IP addresses and static ARP tables while for large networks, enable port security features.
h. Deploy anti-sniffing tools such as ARP Watch and Prodetect.

6. Viruses and worms are largely put on check by the installation of up-to-date anti-virus softwares that scan the system routinely at scheduled times. Integrity checking and interception are other virus detection methods.

7. To detect Trojans:
   a. Routinely scan for questionable network activities using tools like Ethereal.
   b. Routinely scan for questionable registry entries using tools such as MS Config.
   c. Routinely scan for questionable open ports using tools such as Netstat, Fport and TCPView.
   d. Routinely run Trojan scanner to detect Trojans.
   e. Routinely check for running processes.
   f. Delete suspicious and unaccountable device drivers.
   g. Install anti-Trojan software programs.

8. To contain spamming, anti-spam tools such as AEVITA and Spam Bully should be installed.

9. To prevent buffer overflows:
   a. Implement manual auditing of codes.
   b. Disable stack execution.
   c. Implement safer C library support.
   d. Adopt efficient and robust techniques.

Other measures include:

1. Patch management: this is the process of ensuring that appropriate patches are installed on a system. It involves:
   a. Choosing, verifying, testing and applying patches.
   b. Updating previously applied patches with current patches.
   c. Listing patches applied previously to the current software.
   d. Recording repositories or depots of patches for easy selection.
   e. Assigning and deploying applied patches. (Mell, Bergeron & Henning, 2005)

2. Security convergence: this is the process of reusing and blending various technologies to create new and improved capabilities and products. This includes integration of security functions and information into a common IP network. This measure can leverage technology to improve the performance of the security function both physically and logically. Summarily, it is a three-pronged approach composed of technologies, security processes and people (EC-Council).

3. Firewall technologies: these are programs or hardware devices that protect the resources of a private network from users of other networks. Firewalls are responsible for incoming traffic to be allowed to pass, block or refuse and they also work with proxy servers. They help in the protection of private networks from intruders (EC-Council).

4. Creating security policies: security policies are documents that describe the security controls that will be implemented in a company at a high level without which the company cannot be protected from possible lawsuits, lost revenue, bad publicity and basic security attacks. These policies set the objectives and rules of behaviour for users and administrators and also suggest the safety measures to be followed in an organisation. Policies achieve three goals, namely:
   a. They reduce or eliminate legal liability to employees and third parties.
   b. They protect confidential, proprietary information from theft, misuse, unauthorised disclosure or modification.
   c. They prevent waste of company computing resources (EC-Council).
5. Penetration testing: this is a technique used to assess the security model of an organisation in general, and consequently revealing possible outcomes of a real attacker breaching the network security. When this test is not sufficiently and professionally carried out, it can result in the loss of services and disruption of business activities as well as continuity.
6. Physical security: this describes the mechanisms put in place to protect personnel, critical assets and systems against intentional and accidental threats. This is to prevent unauthorised access to computer systems, prevent pilfering and tampering of data from computer systems, prevent the loss of data/damage to systems against any natural disaster or fire outbreak and protect the trustworthiness of the data stored in the computer. These measures can be:
   a. Physical – to secure assets e.g. deploying security personnel.
   b. Technical – to secure services and elements that support information technology e.g. security for server rooms and expensive gadgetry.
   c. Operational – measures taken before performing an operation such as analysing threats of an activity and taking appropriate countermeasures.
7. Cryptography – this is the science of encoding text in formats that are impossible to understand. Plain texts are encrypted into unreadable formats called cipher text which is based on mathematical algorithms that use secret keys for secure transformation back to clear text. (Barr, 2001)
8. Intrusion Detection Systems (IDSs): these are mechanisms that are used to monitor network traffic, check for suspicious activities and notifies the network administrator or the system. In some instances, the IDS might also react to malicious or anomalous traffic and will take action such as barring the user or perhaps the IP address source from accessing the system. (http://www.intrusiondetectionsystem.org)

Assessing Network Vulnerabilities

A properly executed network security evaluation involves three main stages. These phases are:

1. Planning – in this stage, an official agreement is signed between concerned parties. This document is meant to contain both legal and non-disclosure clauses that serve to protect the ethical hacker against possible law suit during this stage.
2. Conduct – this stage involves the evaluation of technical reports prepared based on testing potential vulnerabilities.
3. Inference – in this stage, the results of the evaluation are communicated to the organisation or sponsors and corrective action is taken if needed.

Approaches to proactively secure a network and prevent unwarranted intrusion from destructive elements include:

1. Attempting to simulate oneself as an intruder trying to attack ones network from a remote location through the internet.
2. Attempting to simulate oneself as an intruder trying to attack ones network by launching attacks against the client's modem pools.
3. Probing within a local network to see if a user within the network is able to gain unauthorized access to another location on the network.
4. Attempting to steal crucial data or information resource from an employee to ascertain the level of awareness that members of staff have toward social engineering as a threat to system security.
5. Attempting to physically compromise the ICT infrastructure of the organisation to determine the level and efficiency of physical security.

Any Network Vulnerability Assessment exercise consists of the following steps:

1. Finding all the hosts on the network.
2. Fingerprinting their Operating systems.
3. Detecting open ports on the system.
4. Mapping the ports to various network services.
5. Detecting the version of the services running.
6. Mapping the service version to various discovered security vulnerabilities.
7. Verifying if the service on the host is actually vulnerable to an attack or if it has been patched.

Disadvantages/Effects on Business

1. Loss of credibility and trust of customers
2. Loss of privacy and damage to goodwill
3. According to experts, businesses most at risk are those handling online financial transactions.
4. Economic loss
5. Temporary or permanent closure
6. Exposure to wanton lawsuits and arbitrations
7. Making headlines for all the bad reasons

Limitations

1. Designing software to be invulnerable against attacks is like building a house where every square inch is fortified with steel and sensors that detect intrusions.
2. Patching an existing operating system written by hundreds of programmers who were not particular about the issue of security when they wrote the code is a tedious job.

Recommendations

1. Administrators should deploy simple configurations that work and are easy to maintain.
2. In order to effect proper and efficient system configuration, emphasis should be laid on the removal/disabling of unnecessary services and applications.
3. More ethical hackers – security professionals who apply their hacking skills for defensive purposes. People who fall within this category strive for excellence in programming and networking, understanding of system vulnerabilities as well as a mastery of different hacking techniques.
4. Prompt patch releases from vendors as soon as vulnerabilities are detected and reported.

5. A network administrator should routinely access vulnerability sites to keep updated with current trends in the security spheres.
6. Victims of computer crimes should endeavour to report to law enforcement agencies for necessary (legal) actions.
7. More laws such as the Cyber Security Enhancement Act of 2002 (in the US-statutes 1029 & 1030) should be enacted all around the world as a way of discouraging involvement by potential miscreants.
8. Despite having the best firewall, intrusion detection systems, antivirus systems, one can still get hit with security breaches as a result of having disgruntled employees. Hence efforts should be made by employers to meet the average needs of their employees and where there is enough reason to fire an employee, it should be done properly.
9. Implementation of good and efficient security policies and procedures. Trainings to sensitive employees should be routinely carried out and if possible, the employees should sign an agreement stating their resolve to implement the guidelines in the security policy. The guidelines should cover areas such as account setup, virus and worm control, modems, privacy issues, paper documents, violations, password change, help desk procedures, physical access restrictions, employee identification and so on
10. There should be thorough background check on employees because insiders with criminal background or tendency can pose severe security risks to an organisations network. Where necessary, such personnel should be relieved of their duties.
11. Proper incidence response system in the case of successful security breach from intruders.
12. Beware of activities and information shared on social networking sites such as facebook, myspace, twitter, orkut and so on.
13. Antidotes to new virus releases should be promptly made available by stakeholder companies.
14. Password changes should be made as soon as an employee's appointment is terminated. This will prevent the kind of scenario highlighted in the introduction about the disgruntled ex-employee.
15. Designing a deployment plan to distribute patch on a timely basis.
16. Administrators should be knowledgeable in Computer forensic and incident handling.

Summary

System vulnerability is a flaw in the design or implementation of an information system that could be intentionally or unintentionally exploited to adversely affect an organization's operations or assets through a loss of confidentiality, integrity or availability. System vulnerabilities are predicated on either application/software loopholes or human related limitations. This fact goes to show that no system can possibly attain the status of absolute immunity from potential security breaches. It is often said that if a hacker wants to get inside your system or network as the case may be, there is nothing one can do about it. Perhaps, what can be done is to exhaust all avenues at making it extremely harder for the hacker to breach the system's security. This paper discussed some of the means through which networks are exposed to malicious attacks and suggests measures to curtail or contain such eventualities. In the future we intend to probe into the vulnerabilities associated with cloud and distributed computing.

Reference

Anderson, R. (2002). Security in open versus closed systems - The dance of Boltzmann, Coase, and Moore. *Conference on Open Source Software: Economics, Law and Policy*; 2002. p. 1-15

Barr, T. H. (2001). *An invitation to cryptography*.

Berg, R. (2007). *The path to a secure application: A source code security review checklist* – An OUNCE LABS Security Topics White Paper 2007. Doc.# 20070205-1.0. Retrieved: March 2, 2012 from http://hosteddocs.ittoolbox.com/OunceLabs092707.pdf

Bradley, D. (2009). *Spam or ham?* Sciencetext 2009-05-13. Retrieved: March 3, 2012 from http://www.sciencetext.com/spam-or-ham.html

Chen, M. T. & Davis, C. (2006). An *Overview of Electronic Attacks*. Retrieved: March 3, 2012 from http://lyle.smu.edu/~tchen/papers/dig-forensics06.pdf

Curry, S., Hartman, B., Hunter P. D., Martin, D., Moreau, R. D., Oprea, A., Rivner, U., & Wolf, D. E. (2011). *Mobilizing intelligent security operations for advanced persistent threats* – RSA Security Brief, February, 2011, EMC Corporation. APT BRF 0211. Retrieved: March 4, 2012 from http://www.rsa.com/innovation/docs/11313_APT_BRF_0211.pdf

Dahse, J. (2010). *RIPS - A static source code analyser for vulnerabilities in PHP scripts*. Retrieved: February 28, 2012 from http://www.nds.rub.de/media/nds/attachments/files/2010/09/rips-paper.pdf

EC-Council – Ethical Hacking and Countermeasures version 6. Module 49 – Creating Security Policies

EC-Council – Ethical Hacking and Countermeasures version 6. Module 60 – Firewall Technologies

EC-Council – Ethical Hacking and Countermeasures version 6. Module 66 – Security Convergence

Gandhi, M., & Srivatsa, S. K. (2010). Detecting and preventing attacks using network intrusion detection systems. *International Journal of Computer Science and Security (IJCSS), 2*(1).

Hamid, R., Shahriari, M., Sadegh, M., Marjan, S., Rasool, J., & Ali, M. (2010). Vulnerability analysis of networks to detect multiphase attacks using the actor-based language Rebeca. *Journal for Computers and Electrical Engineering, 36,* 874-885.

Kellermann, T., & Nishiyama, Y. (2003). *The digital insider: Backdoor Trojans*. The World Bank Integrator Unit December 8, 2003. Retrieved: February 25, 2012 from http://www.thehackademy.net/madchat/vxdevl/library/The%20Digital%20Insider:%20Backdoor%20Trojans.pdf

Knapp, J. K., & Boulton, R. W. (2006). Cyber-warfare threatens corporations: Expansion into commercial environments. *Journal of Information Systems Management; ISM 77* (Spring). Retrieved: March 5, 2012 from http://www.infosectoday.com/Articles/cyberwarfare.pdf

Kraemera, S., Carayonb, P. & Clemc, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Journal of Computers & Security, 28,* 509 – 520.

Kramer, D. (2001). *Buffer overflow*. Retrieved: October 25, 2011 from http://searchsecurity.techtarget.com/definition/buffer-overflow

Kuhn, D. R., Walsh, J. T., & Fries, S. (2005). Security Considerations for Voice Over IP Systems (Jan. 2005); NIST Special Publication 800-58. Retrieved March 3, 2012 from http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

Lai, Y-P., & Hsia, P-L. (2007). Using the vulnerability information of computer systems to improve the network security. *Journal of Computer Communications, 30,* 2032–2047.

Mell, P., Bergeron, T., & Henning, D. (2005). *Creating a patch and vulnerability management program.* (NIST Special Publication 800-40 version 2.0) (Nov. 2010). Retrieved March 1, 2012 from http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

Menkus, B. (1990). Understanding data communication security vulnerabilities. *Journal for Computers and Security, 9*, 209-213.

Microsoft Malware Protection Centre. (2011). *Threat research and response*. Retrieved – October 25, 2011 from http://www.microsoft.com/security/portal/Threat/Encyclopedia/Glossary.aspx#t

Newson, A. (2005). Network threats and vulnerability scanners. Journal of Network Security, 2005(12), 13–15.

NIST (National Institute of Standards and Technology). (2010). *Guide for applying the risk management framework to federal information systems: A security life cycle approach*, (NIST Special Publication 800-37, rev. 1) (Feb. 2010). See also Comm. on Nat'l Security Sys., National Information Assurance Glossary 68 (Inst. No. 4009 (2006)) ("Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited."). Retrieved: October 11, 2011

Peltier, R. T. (2006). Social engineering: Concepts and solutions. *Journal of Information Systems Security (ISC), 15*(5), 13-21. Retrieved from http://www.informatik.uni-trier.de/~ley/db/journals/isjgp/isjgp15.html#Peltier06

Pfleeger, C. P., & Pfleeger, S. L (2003). *Security in computing* (3rd ed). Prentice Hall.

Shimonski, R. (2002). *Hacking techniques – Introduction to password cracking*. Retrieved: October 21, 2011 from http://www.ibm.com/developerworks/library/s-crack

Tan, K. Y. (2006). *Phishing and spamming via IM (SPIM).* Retrieved: October 5, 2011 from http://isc.sans.org/diary.php?storyid=1905. http://www.intrusiondetectionsystem.org.

Biographies

Awodele, Oludele holds a Ph.D. in Computer Science from the University of Agriculture, Abeokuta, Nigeria. He has several years experience of teaching computer science courses at the university level. He is currently a lecturer in the department of Computer Science, Babcock University, Nigeria. He is a full member of the Nigeria Computer Society (NCS) and the Computer Professional Registration Council of Nigeria. His areas of interest are Artificial Intelligence, Cloud Computing and Computer Architecture. He has published works in several journals of international repute.

Onuiri, Ernest Enyinnaya is a Graduate Assistant in the Computer Science Department of Babcock University. He is a graduate of Computer Science (Technology) from Babcock University. He is a Cisco Certified Network Professional [CCNP] and a Certified Security+ Professional. He is currently doing his M.Sc. in Computer Information Systems at Babcock University. His areas of interest include networking and security, cloud computing, intelligent computing and bioinformatics.

Dr. Okolie Samuel O. is a Senior Lecturer in Computer Science Department, Babcock University, Ilishan-Remo, Ogun State; Nigeria. His research interests are in the area of Computation and Data Structures.