International Digital Organization for Scientific Research ISSN: 2579-0781
IDOSR JOURNAL OF EXPERIMENTAL SCIENCES 6(1) 111-117, 2021.

Security issues and its Management in Network

Chika Lilian Okafor, Uchenna Paulinus Onwuka and O.R Okonkwor
Department of Computer Science, Nnamdi Azikiwe University Awka

ABSTRACT

Secure Network has now become a need of any organization. The security threats are increasing day by day and making high speed wired/wireless network and internet services, insecure and unreliable. Now a day's security measures works more importantly towards fulfilling the cutting edge demands of today's growing industries. The need is also induced in to the areas like defense, where secure and authenticated access of resources are the key issues related to information security. This Paper reviews different Security Threats in Network, and security measures, methods and how to manage security issues in a Network.
Keywords; Network Security, Threats; Security Measures and Security management

Background of the study

Network security can be defined as protection of networks and their services from unauthorized alteration, destruction, or disclosure, and provision of assurance that the network performs in critical situations and have no harmful effects for neither user nor for employee [1,2]. It also includes provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access [3]. [5], defined the core practical networking aspects of security including computer intrusion detection, traffic analysis, and network monitoring aspects of network security. [6], has presented a new approach for the implementation of distributed security solution in a controlled collaborative manner, called grid of security, in which community of devices ensures that a device is trustworthy and communications between devices can be performed under control of the system policies. [7], has defined information security in three parts - data security, network system security and network business security, and the network business security model. A theoretical basis for security defense for enterprise automatic production system has also been established. A Public Key Infrastructure (PKI)-based security framework for wireless network has been defined by [8]. In this paper various tools and treatment related to cryptography and network security has been defined [9,10]. The latest issues related to network security technology and their practical applications like Advance Encryption Standard (AES). In addition, various security threats and their detection and measures and methods are also discussed in a very efficient way. Nowadays, transfer of information in a safer and secure way over a network has become a major challenge in our society and the world at large [11,12]. The attacks and the network security measures define that how using the network security tools, a better, healthy and safe network can be designed and maintained for an organization/industry [13,14]. This research focuses on the issues through which network security can be managed and maintained more efficiently in an organization.

AIM

To review the security Issues, measures and Management in a Network

SECURITY THREATS

A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information. Cyber

threats can originate from various actors, including corporate spies, hacktivists, terrorist groups, hostile nation-states, criminal organizations, lone hackers and disgruntled employees. In recent years, numerous high-profile cyber attacks have resulted in sensitive data being exposed. For example, the 2017 Equifax breach compromised the personal data of roughly 143 million consumers, including birth dates, addresses and Social Security numbers. In 2018, Marriott International disclosed that hackers accessed its servers and stole the data of roughly 500 million customers. In both instances, the cyber security threat was enabled by the organization's failure to implement, test and retest technical safeguards, such as encryption, authentication and firewalls. Cyber attackers can use an individual's or a company's sensitive data to steal information or gain access to their financial accounts, among other potentially damaging actions, which is why cyber security professionals are essential for keeping private data protected.

Types of Security Threats in Network

Security Attacks Security attacks can be classified under the following categories:

a. Passive Attacks

b. Active Attacks

Passive Attacks: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted[14].

Attributes of Passive attacks are as following:

Interception (Man in the middle attacks): A man in the middle attack involves attackers intercepting traffic, either between your network and external sites or within your network. If communication protocols are not secured or attackers find a way to circumvent that security, they can steal data that is being transmitted, obtain user credentials and hijack their sessions.Traffic Analysis: attacks confidentiality, or anonymity. It can include trace back on a network. Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message. The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Active attack

An active attack could be a network exploit during which the attackers will modify or alter the content and impact the system resource. It'll cause damages to the victims. The attackers can perform passive attacks to gather info before they begin playacting a vigorous attack. The attackers attempt to disrupt and forced the lock of the system. The victims can get informed concerning the active attack. This sort of attack can threaten their integrity and accessibility. A vigorous attack is tougher to perform compared to a passive attack.

Attributes of Active attack are as follows:

Denial of Service

A denial of service (DoS) is a type of cyber attack that floods a computer or network so it can't respond to requests. A distributed DoS (DDoS) does the same thing, but the attack originates from a computer network. Cyber attackers often use a flood attack to disrupt the "handshake" process and carry out a DoS. Several other techniques may be used, and some cyber attackers use the time that a network is disabled to launch other attacks. Phishing: Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

SECURITY MEASURES IN NEWORK

(1). Virus Defense Technology

Virus defense technology is an important precautionary measure for computer network security at present. The power of virus has also been mentioned above. The damage caused by the virus to humans is simply incalculable. Some viruses can be isolated from our computers through our effective defense, but some of the more severe viruses cannot be completely eliminated through several protective nets. Computer technology is constantly updated and developed, but hackers and outlaws are also constantly learning, so we must not stop studying computer network security technology. Our protective technology must be faster than the speed at which they study viruses, otherwise our computer network security will not be guaranteed.

(2). Data Encryption Technology

As mentioned earlier, information leakage is one of the most frequently mentioned problems in computer network security. We can use data encryption technology, so that users' information is not so easy to steal. Data encryption technology refers to the use of special data processing technology to hide or specialize data, through which other users may not understand the information. Data encryption can be divided into two forms: public key encryption and private key encryption. Public-key encryption is more secure than private-key encryption, and it develops relatively late. Private key encryption can be divided into two processes: encryption and decryption. The encryption and decryption process correspond to each other, which has a certain protective effect on the security of information. Private key encryption is not restricted by users, anyone can set up and use it. In terms of decryption speed, private key encryption is faster than public key encryption and easier to implement in life. Comparing the characteristics of public key cryptography and private key cryptography, we find that they have their own merits. Personally, if public key encryption and private-key encryption are used together, the effect of data encryption should be higher. I hope this idea can be realized as soon as possible.

(3).Access Control

The most important feature of access control is to verify the identity of the users who access computer resources. It requires auditing, authorization verification, and password, key and other authentication methods to protect user information and computer security. Simply put, the core idea of access control funds is that information is only open to those who really need it, and that users who enter illegally are intercepted. Access control is an important means to protect computer network security. It has great research value. It has a good effect on hacker intrusion. It is hoped that there will be significant development in the future.

(4). Firewall Technology Firewall

On the surface, is a security barrier to protect computer security and prevent computer failure. It is also the most common type of computer security measures used by ordinary people. Firewalls can be hardware, software, or between two or more computers. Firewall can play a more substantive role in protecting computers, because after all, all data streams need to be filtered through the firewall [4]. Generally speaking, firewalls have the following functions: first, firewalls can prevent other unrelated people from entering the user's own private computer; second, even if someone from outside enters our system, firewalls can prevent him from approaching your defense facilities; third, firewalls can prevent me from visiting special sites; and finally, firewalls can prevent us from visiting special sites. Computers provide security monitoring.

SECURITY METHODS

Cryptography

The most widely used tool for securing information and services according to [8]. Cryptography relies on ciphers, which is nothing but mathematical functions used for encryption and decryption of a message.

Authentication

Authentication is the process of recognizing or identifying a user's identity whether it is true, real, or not. It's simply a verification of claim whether you are who you say you are or not. There are many authentication methods available nowadays like password authentication that includes using a password, physical authentication that includes the scannable card or smart card or digital certificate, biometric authentication that includes signatures and fingerprints, or visual identification, and many more.

Authorization

Authorization means to ensure whether you have permission to access on network or not. It's simply a verification of permission either user has access or not. Some authorization methods are ACLs (Access Control Lists), Secure objects and methods, Access control for URL's, etc.

Biometric

A Biometric system is one of the most secure systems as it provides high security to the computer network. This system verifies the user's identity based on some important characteristics that are physiological and behavioral features. Physiological features include face, eyes, fingerprints, hand. Behavioral features include voice, signature, etc.

Firewall

A firewall is a method of network security that prevents the computer network from users that are not authorized to have access to a network. Firewalls can either be hardware or software or both. It acts as a barrier between unauthorized Internet users and private computer networks connected to the Internet. It blocks the message, viruses, and hackers if they do not have authorized access and do not meet the security criteria as per requirement. Any message entering or leaving private computer networks connected to the Internet especially Intranet passes through the firewall. Firewall than checks each message and block if found unauthorized.

There are three basic types of firewalls:

I) Application Gateways: This is the first firewall and is sometimes also known as proxy gateways. These are made up of bastion hosts so they do act as a proxy server. This software runs at the Application Layer of the ISO/OSI Reference Model. Clients behind the firewall must be categorized & prioritized in order to avail the Internet services. This is been the most secure, because it doesn't allow anything to pass by default, but it also need to have the programs written and turned on in order to start the traffic passing. Packet Filtering: Packet filtering is a technique whereby routers have ACLs (Access Control Lists) turned on. By default, a router will pass all traffic sent through it, without any restrictions. ACL's is a method to define what sorts of access is allowed for the outside world to have to access internal network, and vice versa. This is less complex than an application gateway, because the feature of access control is performed at a lower ISO/OSI layer. Due to low complexity and the fact that packet filtering is done with routers, which are specialized computers optimized for tasks related to networking, a packet filtering gateway is often much faster than its application layer cousins. Working at a lower level, supporting new applications either comes automatically, or is a simple matter of allowing a specific packet type to pass through the gateway. There are problems with this method; thought TCP/IP has absolutely no means of guaranteeing that the source address is really what it claims to be. As a result, use layers of packet filters are must in order to localize the traffic. It

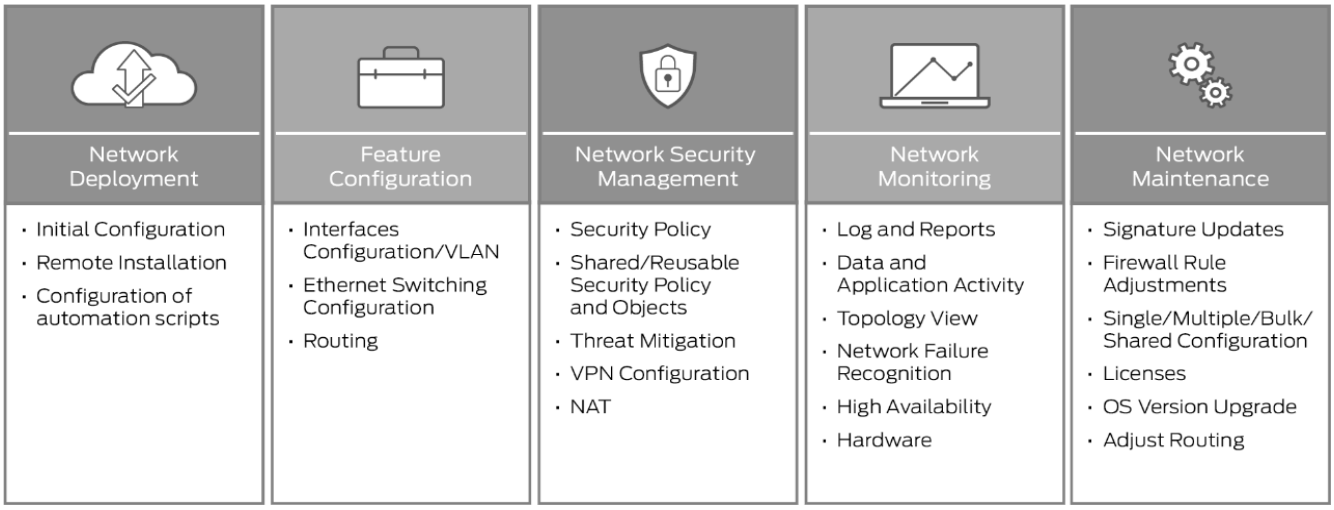
can differentiate between a packet that came from the Internet and one that came from our internal network. Also It can be identified which network the packet came from with certainty, but it can't get more specific than that.

II)Hybrid Systems: In an attempt to combine the security feature of the application layer gateways with the flexibility and speed of packet filtering, some developers have created systems that use the principles of both. In some of these systems, new connections must be authenticated and approved at the application layer. Once this has been done, the remainder of the connection is passed down to the session layer, where packet filters watch the connection to ensure that only packets that are part of an ongoing (already authenticated and approved) conversation are being passed. Uses of packet filtering and application layer proxies are the other possible ways. The benefits here include providing a measure of protection against your machines that provide services to the Internet (such as a public web server), as well as provide the security of an application layer gateway to the internal network. Additionally, using this method, an attacker, in order to get to services on the internal network, will have to break through the access router, the bastion host, and the choke route.

SECURITY MANAGEMENT IN NETWORK

What is network security management?Network security management allows an administrator to manage a network consisting of physical and virtual firewalls from one central location. Administrators need network security management solutions to get a high level of visibility into network behavior, automate device configuration, enforce global policies, view firewall traffic, generate reports, and provide a single management interface for physical and virtual systems. Problems Network Security Management Address. In today's complex network architecture and constantly changing threat environment, it is challenging for IT staff to maintain an effective security posture. Security administrative tasks include supporting an ever-expanding matrix of users, devices, locations, and applications; adhering to compliance; enabling new services; optimizing performance; ensuring access controls and security mechanisms; and troubleshooting on demand. Any misconfiguration can make the network vulnerable to sophisticated threats and regulatory noncompliance. To confront these challenges, network administrators need to consistently deploy security policies across their network. However, the network infrastructure might have thousands of firewall policies that have accumulated over the years. Often these rules are cluttered, duplicated, outdated, or conflict with new rules, inadvertently affecting a network's performance and security.

The following illustration depicts a scenario from a typical enterprise, where the IT department needs to address network security management:



Network security management helps reduce manual tasks and human errors by simplifying administration with security policy and workflow tools through a centralized management interface. Network security management can reduce risk across the network and protect data by leveraging the information on threats, network vulnerabilities and their criticality, evaluating potential options to block an attack, and providing intelligence for decision support. Policy administration is improved by unifying common policy tasks within a single interface, automating policy change workflow, including compliance audits and the management of multiple firewall vendors. This simplified and automated security policy management enables IT teams to save time, avoid manual errors, and reduce risk. How Does Network Security Management Work? Network security management provides complete visibility into the network and generates data for assets (asset groupings and classifications), firewalls, applications, ports, protocols, VPNs, NAT, and security policies and vendor devices. This information drills into the details for individual devices and is analyzed. The data is translated into intelligence that decrypts security transactions into manageable, actionable information in the form of policy creation. Updated policies are distributed to enforcement points (firewalls), ensuring network protection.

CONCLUSION

Security has become important issue for large computing organizations there are different definitions and ideas for the security and risk measures from the perspective of different persons. The security measures should be designed and provided, first a company should know its need of security on the different levels of the organization and then it should be implemented for different levels. Security policies should be designed first before its implementation in such a way, so that future alteration and adoption can be acceptable and easily manageable. The security system must be tight but must be flexible for the end-user.

In addition, the technological development of computer network security should keep up with it as soon as possible and suppress the illegal elements technically. There is still a long way to go for the future development of computer network security technology. Technical breakthroughs should be realized as soon as possible, and our security protection measures should be improved.

REFERENCES

1. Al-Akhras, M.A (2006). "Wireless Network Security Implementation in Universities" In Proc. of Information and Communication Technologies, ICTTA '06., Vol. 2, pp.3192 – 3197.
2. Brenton, C. &Hunt, C. (2002): Mastering Network Security, Second Edition, Wiley
3. Chaohan, (2005). Computer network security and data integrity technology [M]. Beijing: Electronic Industry Press, pg :11-13.
4. CISCO (2001) A beginner's guide to network security, CISCO Systems, Retrieved from http://www.cisco.com/warp/public/cc/so/neso/sqso/ beggu_pl.pdf
5. Curtin (1997), Introduction to Network security, retrieved from http://www.cs.cornell.edu/Courses/cs519/2003sp/slides/15_securitybasics.pdf,
6. Flauzac O, Nolot F, Rabat C, Stiffened L,(2009). "Grid of Security: A New Approach of the Network Security", In Proc. of Int. Conf. on Network and System Security,. NSS '09, pp. 67-72.
7. Hu Shichang(2010) .Analysis of hidden dangers of computer network security and discussion of preventivemeasures[J].Information and Computer (theoretical edition), 11 (10): 159-158.
8. Lin, Xianbo(2006). Brief discussion on computer network security technology [J]. Computer knowledge and technology, pg: 45-46.
9. Marin G.A. (2005), "Network security basics", In security & Privacy, IEEE, Issue 6, Vol. 3, pp. 68-72
10. McClure S, Scambray J, Kurtz G, (2009): Hacking Exposed: Network Security Secrets & Solutions, Sixth Edition, TMH.
11. Stallings W. (2006): Cryptography and Network Security, Fourth Edition, Prentice Hall.
12. Stallings W. (2007): Network security essentials: applications and standards, Third Edition, Prentice Hall.
13. Wu Kehe, Zhang Tong, Li Wei, Ma Gang,(2009) "Security Model Based on Network Business Security", In Proc. of Int. Conf. on Computer Technology and Development,. ICCTD '09, Vol. 1, pp. 577-580.
14. Wuzheng Tan, Maojiang Yang, Feng Ye, Wei Ren(2009) A security framework for wireless network based on public key infrastructure, In Proc. of Computing, Communication, Control, and Management. CCCM 2009, Vol. 2, pp. 567 – 570,