Network Proposal Vulnerability Assessment

Posted on May 13, 2020

Network security is a significant factor considered when determining the effectiveness of a communication infrastructure or a computer network. The morale and productivity of any institution are determined by the institution's ability to provide a secure operating environment. An institution like a university requires effective networking to facilitate communication between different sectors such as finance, dean of students, administration, and library. To achieve an efficient working network system, a clear understanding of the operations carried out by the system is necessary. A vulnerability assessment is performed on the system to ensure its efficiency in achieving the institution's aim. Vulnerability assessment, also known as vulnerability analysis, is the process that identifies, classifies and defines security holes in a network. The estimates also show any possible threats that may affect the system in the future. Vulnerability scanning can be performed internally by searching for missing vendor patches or externally by scanning for vulnerabilities such as Heartbleed (Vongpanitlerd, 2013). Heartbleed is a security hole in the OpenSSL cryptography library that is widely implemented in the Transport Layer Security protocol. Some of the vulnerability scanning tools include Nessus, SAINT, OpenVAS, and Nikto. These are software frameworks that provide several services related to vulnerability scanning and management. The main difference between these scanning tools is that some are free while others are purchased. For instance, some free vulnerability scanners offer a command line tool to perform the scan, while paid vulnerability scanners provide a Graphical-User-Interface that allows a point-and-click solution.

Personally, I suggest a free vulnerability scanner to be initially used, after which a second assessment can be performed with a different scanning tool, this time a purchased one. OpenVAS is a freely available vulnerability scanning tool that can be used to implement the initial vulnerability scanning. The Open Vulnerability Assessment System was developed by Greenbone Networks in 2017. This software is recommendable since it is free, fast, accurate and easy to use (Vongpanitlerd, 2013). Also, most of the components used in OpenVAS are licensed under the General Public License.

Network Security Policy

A network security policy is a document written by a committee of networking experts that provides the guidelines that determine how security policies are enforced. It's a complicated document that is meant to give details of how data is accessed and manipulated in a network. It dictates hierarchically the step by step access procedures that allow network users to navigate through a network safely (Batagelj, 2011).

A network policy document requires some elements that are used to control access and authorization in the network. These elements include identification/authentication, access control/authorization,

privacy/confidentiality, data integrity and non-repudiation. Authentication is a policy used to identify a user who wants to access the network accurately. This is done through the use of passwords and biometric scans. Access control/authorization is used to regulate authenticated users by controlling the resources they can access. This is achieved through the use of mechanisms such as usernames. Data integrity assures the network operators that data resources in the network cannot be manipulated without the proper procedures being followed.

I would recommend a security policy to adopt an identification/authentication method to ensure the network is safe. There are different types of authentication, such as password-based authentication, which requires the user to provide a password and a username. Another method of authentication is device-based authentication. In this method, a user is provided with a portable device that is similar to a credit card intermesh of size and appearance. The invention holds user data that is used to identify him. Biometric authentication uses unique body features that are unique such as fingerprints, facial recognition, and retina scans, to identify a user.

The advantage of user authentication is that it provides several ways by which a user can be identified, as illustrated above. It is also a cost-effective way to ensure that unauthenticated users do not access the network. Another advantage of authentication is that it is easily understood by all the network operators.

Risk Management

Every institution aims to maximize capital and reduce losses as much as possible. Any threat to its wealth and earnings is a significant drawback, and this is the reason why most institutions come up with risk management bodies. Risk management is the process of assessing and identifying threats ranging from financial uncertainty, management errors, and IT security holes to natural disasters. Digitalized institutions such as universities prioritize data and network-related risk management strategies. Several organizations developed risk management standards that were designed to help identify vulnerabilities, assess threats, determine the value of their risk and come up with ways to reduce the effect of these risks. National Institute Of Standards And Technology and ISO are some of the bodies that developed these standards (Batagelj, 2011).

ISO standards recommend that the risk management process should address any uncertainty, should be structured and systematic, should be based on valid available information, and should also be transparent. ISO insists that a risk management process should take into account potential errors and human factors.

After my research, I can confidently recommend the use of ISO standards in developing a risk management procedure. ISO provides a framework that can be used by companies, regardless of the business’s size. The ISO is also designed to improve the likelihood of achieving opportunities and threats and efficiently use resources for risk treatment.

Business Continuity Plan

Institutions come up with strategies that are meant to ensure that they can be able to function normally in case of a disaster. A business continuity plan is used to visualize the process of mitigating risks and implementing safeguards used to ensure the smooth flow of operation of an institution. In networking, there are several methods used to achieve a business continuity plan. Some of these methods include backing up user data and client files in satellite offices and external hard drives, operational risk, crisis management and catastrophe loss index. Another method is accepting risk, which is used when an institution appreciates the fact that the loss to be incurred is not significant enough to warrant spending money to avoid it.

The most effective tool used in a business continuity plan is risk financing. Risk financing is the process of determining how an organization will pay for the loss events most effectively and economically. This method provides an assured way to ensure that a business will continue running no matter what(Faust, 1994).

Access Control Techniques

For any institution, access control systems are one of the most crucial elements to consider. Access control techniques allow the management to regulate who can access what and the operations that can be performed on the obtained resources. To achieve this, the administration needs to identify the users in the network, identify the elements to be accessed, and the encryption procedures to be used. Several techniques are applied to facilitate how access control is managed. Mandatory Access Control (MAC) is one of the methods used. The MAC system classifies all users and entities and provides mechanisms to pass them through the security gains. Role-Based Access Control Technology (RBAC) is one of the most successful technologies applied in access control mechanisms. Discretionary Access Control (DAC) is the most popular control method used in many operating systems, including Windows. An excellent example of DAC is the Access Control Lists (ACLs) (Faust, 1994). This system works by holding owners responsible for deciding what people to access network resources.

RBAC is the most efficient method of access control. It is the most popular technology among households, and it provides stringent based access according to the role of the business. For example, employees are given access limitations according to their job responsibilities.

Physical Security Requirements

To ensure a safe working environment institutions are required to put in place measures to enforce physical security keenly. Physical security is the process of protecting employed personnel, hardware and software resources, data and the entire communication infrastructure from real events that may cause harm and damage to them. This entails protection from natural disasters, fire, theft, and

vandalism. In most instances, physical security is overlooked, and the results usually are devastating.

Detection of possible physical insecurities is mostly done through observation. The location of hardware resources such as computers is determined and investigated whether it can cause harm to the personnel using it. Using notifications such as smoke detectors, heat sensors, and intrusion detection sensors also helps to detect physical insecurities.

There are three essential components to ensuring physical security. These components are access control, surveillance, and testing. Hardening measures such as locking, fencing, and biometric access should be used. Secondly, surveillance cameras should be employed to monitor physical locations.

Disaster recovery techniques, policies, and procedures should be regularly tested to improve the time an institution recovers from human-made or natural disasters. Some of the recovery techniques applied may include tracking signals and the use of tamper-proof locks.

Mobile Device Security

Hackers are using viruses and worms patched in mobile devices to breach the security of a network. Due to the advancements made in mobile devices technology, traditional desktop antivirus, and other endpoint controls cannot be used to provide protection services. With the current trends of increase in the number of individuals using laptops, tablets, iPhones and other Android devices, security managers are redirecting their energy to come up with ways of ensuring that these devices are secure.

Mobile authentication is one of the security measures taken. Authentication using password and username is done to ensure that only the legitimate user can access the network resources using the mobile device. To prevent the use of malware and spyware in mobile devices, two layers of antivirus and antispyware can be handled. To add to this protection mechanism, antimalware can be attached to the endpoint point device and at or near the gateway. This is the most recommendable form of providing mobile device security, and it works by ensuring all the security holes that an attacker can use are addressed (Scott, 2017).

Perimeter Defense Requirement.

Numerous corporate enterprises use perimeter security technologies like firewalls, virtual private network servers (VPN) and intrusion detection systems (IDS). A perimeter defense technology is configured to permit only those activities that are required. By so doing, they detect attacks and prevent them from causing damage to back-end systems. IDS works by alerting the security team in charge in case of an attack. VPN technology authenticates and provides a safe tunnel for communication to legitimate network users.

Firewall technology or application proxy is the most recommendable perimeter defense mechanism. A firewall filters all the information getting into a computer from the internet and blocks all the harmful from getting through. It uses several techniques to achieve this, such as packet filtering, application gateway, circuit-level gateway and proxy server. In practice, a firewall uses more than one technology, especially when protecting private information.

Network Defense Requirements.

A networks day to day operations is intercepted by disruptions, degradation and service denial. Installing protective measures to monitor, analyze and defend the network against network infiltrations is the method used to provide network defense. The critical objective of network defense is to ensure that no illegal, malicious traffic or unauthorized users get into the IT environment. A computer network defense system(CND) uses the following tools to achieve its purpose: intrusion detection system, mobile device management, anti-malware, network access control, firewalls, authorization, and authentication (Scott, 2017).

Host Defense Requirements

Network devices such as computers can easily be used by attackers despite the security measures provided to them. Protecting the host is the last line of defense used to protect a network. Defence-in-depth is the phrase used to refer to the multi-layered security measures taken in host defense. Host defense entails all the steps put in place to detect, analyze and eliminate any threat that can cause damage to the normal operation of the network. The first tool used to implement this protection is the host Intrusion Prevention System (IPS)/ intrusion defense system (IDS). This technology relies upon patterns and signatures to accurately detect and identify a virus or any other form of attack targeting the host. Route ACLs are another defense requirement required to be provided for efficient host security. In modern-day networks, inspection technologies such as Cisco ISR routers are used in host defense (Cramer, 2013).

I would recommend host-based firewalls to be used to guarantee a full-proof barrier against unwanted activities in the network. These types of firewalls are vulnerability-free and are used to reduce the surface available to launch an attack. The firewall is also responsible for monitoring and configuring all the host defense components to ensure the effectiveness and trustworthiness of the system.

Public Key Infrastructure

Encryption, identity, and authorization management (IAM) applications are some of the key factors considered when setting up an institution’s layered security environment. An essential public infrastructure (PKI) supports IAM and public encryption keys enabling users in a network to exchange data via the communication channels available and identify the identity of the other party. The PKI is

made up of the following components. The first component is the certification authority (CA) which authenticates the integrity of all network entities in the network. Another tool is the Registration Authority (RA), which acts as a subordinate CA. It certifies uses permitted by the CA. The third component is the certificate database that is used to save or revoke certificates from RA or CA. The fourth tool is the certificate store that saves issued licenses and pending or rejected requests. The last device is the central archival server that serves to preserve encrypted keys in a certified database for disaster recovery (Cramer, 2013).

All the above components are required to build a PKI that can control access using 802.1x authentication, secure network IPSec and ensure authorization applications with code signing.

Secure Protocol Implementation

Security protocol defines the methodologies used to ensure that illegitimate attempts to extract and view data contents cannot succeed. Network security protocols provide data integrity and security as it is in transit. The protocols employ encryption and cryptography skills to encode data so that it can be decrypted using a particular kind of logic key, a mathematical formula or a particular algorithm. Among the commonly used security protocols are Secure File Transfer Protocol (SFTP), Secure Socket Layer (SSL) And Secure Hypertext Transfer Protocol (HTTPS).

HTTPS is the most used protocol communication protocol. This type of protocol is encrypted by its predecessor, SSL, or by Transport Layer Security (TLS). HTTPS eliminates man-in-the-middle attacks and assures privacy, integrity and communication can take place without a strike (Varhol, 2011).

File Encryption

Encryption is a kind of technology that works by changing data format so that it is unreadable by unintended parties. Once encrypted, the data in transit becomes a jumbled mess of characters, and the receiver is required to be equipped with a unique decryption technique to understand the information sent. File encryption comes in many technologies, such as Triple DES. Triple DES uses three individual keys of 56 bits each to encrypt data. RSA is another encryption technology that uses methods from PGP and GPG programs to encrypt data. RSA forms the standard public encryption format used over the internet. Other forms used to encrypt data used are AES, Twofish, and blowfish.

RSA is recommendable for use since it is the most common form of encryption, easy to understand and decode.

File Hashing

Hashing is an algorithm that aims to calculate a fixed-size bit value from a file. Hashing transforms data into a far shorter fixed-length value. A good hashing effect contains an effect called the avalanche effect that significantly changes the file properties and data structures within the file. Different hashing types include MD5, SHA1, and CRC32 (Varhol, 2011).

A hash is used to improve data retrieval speed and encrypt and decrypt digital signatures. Hashing is also used to compare two files for equity. The main drawback of hashing is that it is a unidirectional process, and once performed, it is impossible to get back the original data.

Backup And Recovery

A disaster recovery plan must include procedures for backup and restoration of vital information to prevent loss of data. All the data stored in electronic form should be backed up and kept safe in case of system failure, attacks or disasters. A copy of the backup and recovery files should be stored away from the primary site to prevent destruction. Backup dictates that files should be stored and saved onto magnetic tapes or some other offline mass storage media. Restoring is the process of feeding back destroyed data into the file servers for routine operations to continue smoothly (Varhol, 2011).

A good backup plan should be economical and meet all the business and regulatory requirements. It consists of the following data protection solution. First, it should resolve the malicious deletion of critical data and provide a quick means to restore these files. It should also restore data that is lost or corrupted by severe failures.

References

Borgatti, S. P., Everett, M. G., & Freeman, L. C. (2002). Ucinet for Windows: Software for social network analysis.

Wasserman, S., & Faust, K. (1994). Social network analysis: Methods and applications (Vol. 8). Cambridge University Press.

Scott, J. (2017). Social network analysis. Sage.

De Nooy, W., Mrvar, A., & Batagelj, V. (2011). Exploratory social network analysis with Pajek (Vol. 27). Cambridge University Press.

Anderson, B. D., & Vongpanitlerd, S. (2013). Network analysis and synthesis: a modern systems theory approach. Courier Corporation.

Borsboom, D., & Cramer, A. O. (2013). Network analysis: an integrative approach to the structure of psychopathology. Annual review of clinical psychology, 9, 91-121.

Gardy, J. L., Johnston, J. C., Sui, S. J. H., Cook, V. J., Shah, L., Brodkin, E., ... & Varhol, R. (2011). Whole-genome sequencing and social-network analysis of a tuberculosis outbreak. New England Journal of Medicine, 364(8), 730-739.