Essay on network security monitoring

Law, Security

Security process

Security itself is not a technology rather it is a process that has to be applied (Wadlow, 2000). This is because new threats are developed every day, which require new forms of protection (Nordquist, 2002). The security process involves the analysis of a problem followed by the development of a solution based on the analysis and then evaluating the solution.

- Analysis
- This involves learning all concepts that concern the nature of the threat attack.
- Synthesis
- This involves developing a solution based on the outcome of the analysis.
- Evaluation
- This involves cross checking whether the solution applied is effective in handling the security threat. Further, in cases where the solution is inadequate, new solutions are then developed.

Security Processes

- Security processes include assessment, protection and response
- Assessment: involves ascertaining the level of security and policies and procedures required for the network security (Bejtlich, 2004).
- Protection: involves the applications of controls to prevent the security threat (Bejtlich, 2004).
- Detection: involves identification of the security threats (Bejtlich, 2004).
- Response: involves the reaction to the effects of a security threat or attack (Bejtlich, 2004).

- Security

Security involves protecting physical locations, hardware, and software from threats. This has developed from the need to feel safe. According to Bejtlich (2004), security involves maintaining a perceived level of risk.

- Risk

This deals with the likelihood of a loss occurring (Bejtlich, 2004). Risk is high when security level is low.

- Security Principles

These are aimed at providing a guideline to having a security system. They include integrity, confidentiality, and availability.

- Integrity

- This implies that the information or network being secured does not allow the data or information to be altered (Nordquist, 2002).

- Confidentiality

- Authorized personnel only should access information being protected (Nordquist, 2002).

- Availability

- The security level being applied should not prevent access to the information when it is required for use (Nordquist, 2002).

- Effectiveness

- Controls implemented in securing a system or a network must be effective (Nordquist, 2002).

- Adequate Protection

- The level of security needs to be directly related to the value of information or hardware that is being protected (Nordquist, 2002).

- Easiest Penetration

- This principle is based on the notion that an intruder will apply all possible means of penetrating a system or a network (Nordquist, 2002).

- Characteristics of the Intruder

- Intruders are unpredictable. This implies that the design of the security should address the worst-case scenario (Bejtlich, 2004).

- Intruders are intelligent. Most of the intruders are skilled individuals (Bejtlich, 2004).

Security Principles

- Phases of Compromise

- Reconnaissance: involves certifying connectivity and vulnerability assessment of the system. (Bejtlich, 2004). This assists in planning of structured threats and most cases ensures efficiency of the attack.

- Exploitation: involves using stolen passwords and usernames to access a system (Bejtlich, 2004). Additionally, it may involve using programs to perform differently than their initial intended use.

- Reinforcement: attackers use more approaches and tools to exploit the system further. Mostly used are back doors (Bejtlich, 2004).

- Consolidation: This phase involves the attacker using the back door to access the server or the system (Bejtlich, 2004).

- Pillage: During this phase, the intruder is able to execute his intended plan such as stealing information or transferring valuable records (Bejtlich, 2004).

Security Principles

- Defensible Networks

- Defensible networks can be watched: it is easy for analysts to observe traffic pass through the network (Bejtlich, 2004). This makes it possible to account for the services, applications, and operating systems in the network.

- Defensible networks limit the movement of the Intruder: the intruder is not provided with opportunities to move free across the network and cannot easily access the internal IP addresses (Bejtlich, 2004). Further, the freedom of the intruder is limited by reducing or limiting the number of protocols that are passed through the firewalls (Bejtlich, 2004).

- Defensible networks provide few numbers of services. The less the number of services in a network reduces the opportunities for the intruder (Bejtlich, 2004).

- Defensible Networks are updated regularly. This means that new patches and updates can be applied to reduce the vulnerabilities of the network

This involves examining the network traffic and activities across the network to be able to detect any form of intrusion (Ciampa, 2012). According to Bejtlich (2004), network monitoring allows the detection and response to threats to a network.

- Why IDS Deployments Often Fail

IDS are normally deployed to detect intrusion for the firewall to block. However, not all attacks can be blocked by the firewall without human supervision (Bejtlich, 2004). Individuals assuming that all attacks detected by the IDS will be blocked by the firewall reduce the effectiveness of the IDS.

- Security Principles Limitations

These limitations related to network security monitoring include increased traffic data, problems of real time analysis and increased cost.

- Increased Traffic data: the more the data the more time will be required to analysis the traffic activities

- Real Time Analysis: real time analysis uses techniques that may give the intruder more time to modify their attacks (Bejtlich, 2004).

- Increase Cost: the more the traffic activities the more resources that will be required, and this means extra cost (Bejtlich, 2004).

- What NSM is not

- NSM is not Security Event management:

- NSM is not Device Management: network monitoring does not translate to efficient use of devices.

- NSM is not Intrusion Prevention: Network security monitoring detects the intrusion for the analyst to block using firewalls or other approaches.

- NSM is not Network Based Forensics: forensics involves more of a legal process, which network security monitoring does not perform (Bejtlich, 2004).

- NSM in Action

- This entails the use of the analysis information to develop solutions that may prevent security attacks to a network. Further, network security principles have to be applied (Bejtlich, 2004).

References

Bejtlich, R. (2004). The Tao of network security monitoring: beyond intrusion detection. Boston:

Addison-Wesley.

Ciampa, M. (2012). Security+ guide to network security fundamentals (4th Ed.). Boston, MA:

Nordquist, M. (2002). Towards improved security management practice: designing an

Organizational model procedure for the implementation of information security management in heterogeneous information management environments. USA: Dissertation. com.

Wadlow, T. A. (2000). The process of network security: designing and managing a safe network.

Reading, Mass.: Addison Wesley.