CSIT988 Security, Ethics and Professionalism

Workshop 9 for Week 10

1. What is the difference between authentication and authorization? Can a system permit authorization without authentication? Why or why not?

Authentication is confirming the identity of the person who is accessing a logical or physical area, whereas authorization is determining what actions the person can perform in a particular physical or logical area. A system cannot permit authorization without authentication because it needs to know the person's identity in order to know what authorization level the person possesses.

2. How is an application layer firewall different from a packet filtering firewall? Why is an application layer firewall sometimes called a proxy server?

An application layer firewall is a dedicated computer distinct from the first filtering router; it is commonly used in conjunction with a second or internal filtering router. Such firewalls are sometimes called proxy servers because they serve as proxies for external service requests for internal services. A packet filtering firewall is a simple network device that filters packets by examining every packet header, accepting or rejecting packets as needed.

3. How does a network-based IDPS differ from a host-based IDPS?

A network-based IDPS monitors network traffic in order to provide early warning of potential network threats (such as DoS attacks). A host-based IDPS monitors the access or altering of files on multiple systems. A host-based IDPS is much easier to set up and administer than a network-based IDPS because of the more specific rules and restrictions it can be set to enforce.

4. What are the main components of cryptology?

Cryptology has two components: cryptography and cryptanalysis.
Cryptology— from the Greek words kryptos, meaning " hidden," and graphein, meaning "to write"—describes the processes involved in encoding and decoding messages so that others cannot understand them.

Cryptanalysis—from analyein, meaning " to break up" —is the process of deciphering the original message (or plaintext) from an encrypted message (or ciphertext) without knowing the algorithms and keys used to perform the encryption.

5. Explain the key differences between symmetric and asymmetric encryption. Which can the computer process faster? Which lowers the costs associated with key management?

Asymmetric encryption uses a public key system with a private key, whereas symmetric encryption uses a private key only. Symmetric encryption systems are almost always more efficient when viewed only in terms of computing efficiency; however, asymmetric systems offer a lower total cost of ownership because key management is easier. Advanced PKI systems can make such hybrid systems vastly easier to use