Corrected Text:

Worms, viruses, and bacteria are different. A worm is an independent program that can replicate itself and often spreads to different sites over a network. A virus is a type of malicious software program that spreads through computer files without the user's knowledge. It needs a host program to replicate and inserts copies of itself into other programs, executing when the host program runs. Unlike worms, viruses do not independently spread across networks. Bacteria, in this context, is irrelevant. Infected programs can harm the system and its files. Bacteria-like programs copy themselves, creating copies that replicate, resulting in exponential growth and consumption of all system resources.

Intrusion detection is the process of identifying unauthorized or unusual system activities using audit records.

A firewall monitors and controls data traffic between a private network and the internet, allowing or blocking connections based on its configuration.

Profiles define normal behavior between subjects and objects to detect and report abnormal activities. Logon and Session Activity: Audit records show the user (subject), logon location (object), and actions such as logon/logoff. Command or Program Execution: Audit records show the user (subject), program name (object), and execution action, including measures such as frequency, resource use, and denied executions. File Access Activity: Audit records show user actions (read, write, create, delete, append) on files. Security Concepts: 1. Identification: Users are identified to a computer or application through a user ID. 2. Authentication: The process used to verify the user's claimed identity. 3. Authorization: The process of assigning access rights to each user ID. 4. Access control: The process of enforcing access rights for network resources. 5. Confidentiality: The process used to protect secret information from unauthorized disclosure. 6. Data integrity: Allows detection of unauthorized data modification; it detects whether... The data was modified during transmission. 7. Non-repudiation: The capability to provide proof of data origin or delivery. 8. Denial-of-Service: An attack where the attacker takes over or consumes a resource, preventing others from using it. Authentication methods: ● Something unique to the user (e.g., fingerprints or voice patterns), verified by comparison with system data. ● Something the user possesses (e.g., keys or badges) used to verify identity. Something the user knows, like a secret password known only to the user and the system. Access control is the regulation of user access to resources based on a security policy, such as access to files, databases, or system settings. A capability list defines the access rights a subject has to specific objects, such as files or devices. Each subject has its own list. Access rights define how a subject can access an object. Access rights are specified. For each pair of subjects and objects. Audit Trail: Records important events for later review, such as repeated login attempts by an intruder. Audit Requirements: 1. Automatically collects information on all security-sensitive activities. 2. Stores information in a standard record format. 3. Creates and saves audit records automatically without administrator intervention. 4. Minimally impacts normal system operation and performance. 5. Protects audit logs under a robust security scheme. One-Time Passwords Using Token Cards: Single-use passwords, generated by token cards, become invalid after use. One-way hash function: Used to detect data transmission errors by generating a fixed-size checksum from data of any size. It is easily implemented in hardware and software. Requirements: 1. Applies to data blocks of any size. 2. Produces a fixed-size digest (usually 128 or 160 bits). 3. Is easily implemented in hardware and software. Client: A Server: Communicates with the server and analyzes data to present to the user. Server: Provides one or more services, such as databases or image processing; responds only to client requests; does not initiate communication on its own; and may communicate with other servers. Encrypted message: Used to protect the message content from unauthorized access. Digital signature: Verifies the sender's identity and ensures the message has not been altered. Decrypted signature: Uses the public key to verify the signature's Message

Digest: A short representation of message content used to detect modifications. ACL: An access control list (ACL) for a given object defines the access rights for each subject. Anomaly Records: Created when behavior deviates from the normal profile. Encryption: The process of converting data into an unreadable form that can only be recovered using decryption and a key. The original data is called plaintext; the encrypted data is called ciphertext. Asymmetric: Uses one key for encryption and a different but related key for decryption. Symmetric: Uses the same key for encryption and decryption. Private key: Every user has two keys; a private key (known only to the user). Public key: Each user's public key is published (known to everyone).