**NATIONAL INSTITUTE OF TECHNOLOGY DELHI**

A blue and white logo

Description automatically generated

**Department of Computer Science & Engineering**

**CSB451 – Network Security & Cryptography**

***Assignment – 11***

**Submitted By:**

**Himanshu Verma**

**201210023**

**Submitted To: Dr. Karan Verma**

1. **Define the following terminologies……….relate to each other.**
   1. **Policy:**

A network security policy is a formal document that outlines strategies for ensuring the confidentiality, integrity, and availability of network-based data and resources.

The main goals of a network security policy are to

define the acceptable use of network assets, to outline standardized security procedures and establish optimal measures for protecting resources against network threats. A typical network security policy is a collection of multiple documents, each focused on a specific aspect of security (e.g., data encryption, password rules, patch management, etc.).

There is typically some overlap between these documents, which isn't a cause for concern if guidelines are consistent among all policies.

* 1. **Standard:**

A cybersecurity standard is a set of guidelines or best practices that organizations can use to improve their cybersecurity posture.

Organizations can use cybersecurity standards to help them identify and implement appropriate measures to protect their systems and data from cyber threats. Standards can also provide guidance on how to respond to and recover from cybersecurity incidents.

* 1. **Practices, procedures and guidelines:**

**Practices:** Network Security Practices protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.

Some of the best Network Security Practices which are widely implemented are:

1. Adopt a formal information security governance framework
2. Implement data loss prevention
3. Perform regular data backups
4. Watch out for social engineering attacks
5. Educate your employees
6. Onboard new employees and third-party users
7. Keep your software up to date
8. Build an incident response plan
9. Perform regular network audits
10. Implement PCAP

**Procedures:** Procedures are detailed step-by-step instructions to achieve a given goal or mandate. They are typically intended for internal departments and should adhere to strict change control processes. Procedures can be developed as you go. If this is the route your organization chooses to take it’s necessary to have comprehensive and consistent documentation of the procedures that you are developing.

**Guidelines:** Guidelines are recommendations to users when specific standards do not apply. Guidelines are designed to streamline certain processes according to what the best practices are. Guidelines, by nature, should open to interpretation and do not need to be followed to the letter. They are more general as compared to specific rules and provides flexibility for unforeseen circumstances. However, they should not be confused with formal policy statements.

1. **Describe how the following systems work,………. Secure Shell.**
   1. **Pretty Good Privacy (PGP):** 
      1. **Functionality**: PGP is a data encryption and decryption program used for email and data file encryption and decryption. It provides cryptographic privacy and authentication for data communication.
      2. **Security** **Dimensions**:
         1. **Confidentiality**: PGP uses symmetric-key cryptography for efficient encryption of data. It also employs asymmetric-key cryptography (public-key cryptography) for secure key exchange and digital signatures. This ensures that only the intended recipient can decrypt the message.
         2. **Integrity**: PGP uses digital signatures to ensure message integrity. The sender signs the message with their private key, and the recipient verifies the signature using the sender's public key. Any tampering with the message would result in the signature failing to verify.
         3. **Authentication**: PGP provides authentication through digital signatures. Recipients can verify that the message is indeed from the claimed sender by verifying the digital signature.
      3. **Special Features/Capabilities:**
         1. **Web** **of** **Trust**: PGP supports a decentralized trust model called the "web of trust," where users can vouch for the authenticity of each other's public keys. This enhances the trustworthiness of public keys used for encryption and digital signatures.
         2. **Key** **Revocation**: PGP allows users to revoke their public keys if they are compromised or no longer valid. This ensures that outdated or compromised keys are not used for encryption or verification.
   2. **IPSec (Internet Protocol Security):**
      1. **Functionality**: IPSec is a suite of protocols used for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a communication session.
      2. **Security** **Dimensions**:
         1. **Confidentiality**: IPSec provides confidentiality by encrypting IP packets using encryption algorithms like AES (Advanced Encryption Standard) or 3DES (Triple Data Encryption Standard).
         2. **Integrity**: IPSec ensures message integrity by using cryptographic hash functions like SHA-1 or SHA-256 to generate message authentication codes (MACs) for each packet. This allows the recipient to detect any tampering with the packet during transmission.
         3. **Authentication**: IPSec provides authentication through cryptographic mechanisms like digital signatures or pre-shared keys. This ensures that both communicating parties can verify each other's identity.
      3. **Special Features/Capabilities:**
         1. **Tunnel Mode and Transport Mode:** IPSec supports two modes of operation: tunnel mode and transport mode. Tunnel mode encrypts the entire IP packet, including the original IP header, while transport mode only encrypts the payload of the IP packet.
         2. **Perfect Forward Secrecy (PFS):** Some implementations of IPSec support PFS, which ensures that even if the long-term secret keys are compromised, past communications remain secure. This is achieved by using ephemeral key exchange protocols like Diffie-Hellman for session key generation.
         3. **Network Address Translation (NAT) Traversal:** IPSec includes mechanisms for traversing NAT devices, which are commonly used in network environments. This ensures that IPSec-protected communications can pass through NAT devices without compromising security.
   3. **Secure Shell (SSH):**
      1. **Functionality:** SSH is a network protocol that allows secure remote access to systems over an unsecured network. It provides encrypted communication sessions between clients and servers.
      2. **Security Dimensions:**
         1. **Confidentiality:** SSH encrypts data exchanged between the client and server, including user credentials, commands, and responses, using symmetric-key encryption algorithms like AES or 3DES.
         2. **Integrity:** SSH ensures message integrity through the use of message authentication codes (MACs), which are generated using cryptographic hash functions like SHA-1 or SHA-256. This allows the recipient to verify that the data has not been tampered with during transmission.
         3. **Authentication:** SSH provides various authentication methods, including password-based authentication, public-key authentication, and host-based authentication. Public-key authentication is widely used for stronger security.
      3. **Special Features/Capabilities:**
         1. **Port Forwarding:** SSH supports port forwarding, allowing users to securely tunnel arbitrary network connections over the SSH connection. This feature is useful for accessing services securely over an untrusted network.
         2. **X11 Forwarding:** SSH can forward X11 graphical sessions securely over the network, allowing users to run graphical applications on a remote system and display them locally.
         3. **SSH Keys Management:** SSH supports the use of public-key cryptography for authentication. Users can generate SSH key pairs (public and private keys) and securely manage them for authentication purposes. Additionally, SSH allows users to set passphrase protection for their private keys, enhancing security.
2. **Explain the two main modes of IPsec: Transport mode and Tunnel mode.**
   1. Internet Protocol Security (IPsec) is a protocol and tactic used for securing IP communications through statistics authentication and encryption.

|  |  |
| --- | --- |
| **IPsec Tunnel Mode** | IPsec Transport Mode |
| Full Header and Payload Encryption: In Tunnel Mode, the complete original IP packet (header and payload) is encrypted after which it is encapsulated inside a new IP packet. This new packet has a different IP header, normally with exclusive source and destination spotted on its IP addresses. | Payload encryption simplest: In shipping mode, preferably the payload (information) of a valid IP packet is encrypted, while the valid IP header stays intact. This mode is usually used to pause communication between hosts or gadgets. |
| Used for Site-to-Site VPNs: Tunnel Mode is normally utilized in site-to-web page VPNs (Virtual Private Networks) in which entire networks or subnets need to talk securely over an untrusted network, including the Internet.  Protects | Used for host-to-host communication: The host-to-host communication mode is generally used to guard communication among hosts or devices in preference to the whole network. |
| Protects Network-to-Network Communication: Network to network Communication secures communication between all the networks, for encryption and protection from attacks. | Less overhead: Since the original IP header no longer trades, new headers may have less overhead in keeping with the sentence compared to Tunnel Mode. |

1. **Describe the components of IPsec,………………….. limitations of implementing IPsec in a network environment.**
   1. **Components of IPsec:**
      1. **Security Association (SA):** An SA is a set of security parameters, including encryption and authentication algorithms, keys, and other attributes, negotiated between two IPsec endpoints (usually hosts or gateways) to secure their communications. Each SA is identified by a unique Security Parameters Index (SPI).
      2. **Authentication Header (AH):**
         1. **Functionality:** AH provides data integrity, authentication, and protection against replay attacks for IP packets. It calculates a message authentication code (MAC) using a cryptographic hash function (e.g., HMAC-SHA1) over the entire IP packet (excluding mutable fields like the Time-to-Live (TTL) field) and appends it to the packet. AH ensures the integrity and authenticity of the entire IP packet, including both the IP header and payload. It protects against both passive and active attacks on the packet.
      3. **Encapsulating Security Payload (ESP):**
         1. ESP provides confidentiality, data integrity, authentication, and anti-replay protection for IP packets. It encapsulates the original IP packet within a new ESP packet, encrypts the payload, and optionally authenticates the encrypted payload and other parts of the packet.
         2. ESP ensures confidentiality by encrypting the packet payload, protecting sensitive information from eavesdropping. It also provides data integrity, authentication, and anti-replay protection, enhancing the overall security of the communication.

**Benefits of Implementing IPsec:**

1. **Security:** IPsec provides strong security mechanisms, including data encryption, data integrity, authentication, and anti-replay protection, ensuring the confidentiality, integrity, and authenticity of network communications.
2. **Flexibility:** IPsec offers flexibility in terms of security policies and configurations. Administrators can define different security policies for different traffic flows, allowing for granular control over security requirements.
3. **Interoperability:** IPsec is a widely adopted standard supported by many networking devices and operating systems, ensuring interoperability across different vendors' products.
4. **Remote Access and Site-to-Site VPNs:** IPsec can be used to establish secure remote access connections for remote users and site-to-site VPN tunnels for connecting remote offices over the internet securely.

**Limitations of Implementing IPsec:**

1. **Complexity:** IPsec can be complex to configure and manage, especially in large-scale networks with multiple endpoints and security policies. Proper planning and expertise are required for successful implementation.
2. **Performance Overhead:** IPsec introduces additional overhead, including encryption and authentication processing, which can impact network performance, especially on low-powered devices or high-throughput networks.
3. **Key Management:** IPsec requires robust key management mechanisms to securely generate, distribute, and update encryption keys and security associations. Poor key management practices can compromise the security of IPsec implementations.
4. **End-to-End Security:** IPsec protects communications between IPsec endpoints, but it does not provide end-to-end security. Other security measures, such as transport layer security (TLS), may be needed to ensure end-to-end security, especially in multi-hop network environments.