Information Security

SAQs

1. List Security Policies.

1. Security Program Policy. 2. Enterprise information security policy (EISP). 3. Issue-Specific Security Policy (ISSP). 4. Systems-Specific Policy (SysSP).

2. Define IDS.

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. An IDS works like a burglar alarm in that it detects a violation (some system activity analogous to an opened or broken window) and activates an alarm. This alarm can be audible and/or visual (producing noise and lights, respectively), or it can be silent (an e-mail message or pager alert).

3. List cryptographic tools.

1. Security token/Authentication token. 2. Key-Based Authentication. 3. Docker. 4. Java Cryptography Architecture (JCA). 5. CertMgr.exe 6. SignTool.exe.

4. Define VPN.

VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time. A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

5. List Maintenance models.

1. External monitoring. 2. Internal monitoring. 3. Planning and risk assessment.
4. Vulnerability assessment and remediation. 5. Readiness and review.

6. Differentiate between DoS and DDoS.

Parameter	DOS	DDOS
Full Form	Denial Of Service	Distributed Denial Of Service
Source of attack	DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource	DDoS attack uses multiple computers and Internet connections to flood the targeted resource.
Protection	System can be stopped/protected easily	Difficult to protect system against DDOS attack
Threat Level	Low threat level	Medium to high threat level, as these can be used to do some serious damage to networks and end systems.
Malware involvement	No malware involved	A botnet is usually made up of thousands of infected pc's.
Cost and management	Easier to operate and manage	Not easy to manage and operate

7. Define firewall.

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out. A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

8. What is information security Blueprint?

-> Basis for design, selection, and implementation of all security policies, education and training programs, and technological controls. -> More detailed version of security framework (outline of overall information security strategy for organization). -> Should specify tasks to be accomplished and the order in which they are to be realized. -> Should also serve as a scalable, upgradeable, and comprehensive plan for information security needs for coming years.

LAQs

5A. What are the different protocols used for secure communication?

SSL Protocol: SSL Protocol stands for Secure Sockets Layer protocol, which is an encryption-based Internet security protocol that protects confidentiality and integrity of data.

SSL is used to ensure the privacy and authenticity of data over the internet.

SSL is located between the application and transport layers.

At first, SSL contained security flaws and was quickly replaced by the first version of TLS; that's why SSL is the predecessor of modern TLS encryption.

TLS Protocol : Same as SSL, TLS which stands for Transport Layer Security is widely used for the privacy and security of data over the internet.

TLS uses a pseudo-random algorithm to generate the master secret which is a key used for the encryption between the protocol client and protocol server.

TLS is basically used for encrypting communication between online servers like a web browser loading a web page in the online server.

S-HTTP : S-HTTP stands for Secure HyperText Transfer Protocol, which is a collection of security measures like Establishing strong passwords, setting up a firewall, thinking of antivirus protection, and so on designed to secure internet communication.

S-HTTP's services are quite comparable to those of the SSL protocol.

Secure HyperText Transfer Protocol works at the application layer (that defines the shared communications protocols and interface methods used by hosts in a network) and is thus closely linked with HTTP.

Set Protocol : Secure Electronic Transaction (SET) is a method that assures the security and integrity of electronic transactions made using credit cards.

SET is not a payment system; rather, it is a secure transaction protocol that is used via the internet.

The SET protocol includes the following participants:

1. Cardholder 2. Merchant 3. Issuer 4. Acquire. 5. Payment Gateway. 6. Certification Authority.

PEM Protocol : PEM Protocol stands for privacy-enhanced mail and is used for email security over the internet.

RFC 1421, RFC 1422, RFC 1423, and RFC 1424 are the four particular papers that explain the Privacy Enhanced Mail protocol.

It is capable of performing cryptographic operations such as encryption, nonrepudiation, and message integrity.

PGP Protocol : PGP Protocol stands for Pretty Good Privacy, and it is simple to use and free, including its source code documentation.

It also meets the fundamental criteria of cryptography.

5B. Explain various attacks on Cryptography systems.

Attempts to gain unauthorized access to secure communications have used brute force attacks. Attackers may alternatively conduct known-plaintext attacks or selected-plaintext attack schemes.

Man-in-the-Middle Attack: Designed to intercept transmission of public key or insert known key structure in place of requested public key. From the victim's perspective, encrypted communication appears to be occurring normally, but in fact the attacker receives each encrypted message, decodes, encrypts, and sends to the originally intended recipient. Establishment of public keys with digital signatures can prevent traditional man-in the-middle attack.

Correlation Attacks: Correlation attacks are a collection of brute-force methods that attempt to deduce statistical relationships between the structure of the unknown key and the ciphertext that is the output of the cryptosystem. The only defense against this kind of attack is the selection of strong cryptosystems that have stood the test of time, thorough key management, and strict adherence to the best practices of cryptography in the frequency of changing keys.

Dictionary Attacks: In a dictionary attack, the attacker encrypts every word in a dictionary using the same cryptosystem as used by the target. Dictionary attacks can be successful when the ciphertext consists of relatively few characters, as for example files that contain encrypted usernames and passwords. After a match is located, the attacker has essentially identified a potential valid password for the system under attack,

Timing Attacks: In a timing attack, the attacker eavesdrops during the victim's session and uses statistical analysis of the user's typing patterns and inter-keystroke timings to discern sensitive session information. While timing analysis may not directly result in the decryption of sensitive data, it can be used to gain information about the encryption key and perhaps the cryptosystem in use. Once the attacker has successfully broken an encryption, he or she may launch a replay attack, which is an attempt to resubmit a recording of the deciphered authentication to gain entry into a secure source.

Defending From Attacks: No matter how sophisticated encryption and cryptosystems have become, however, they have retained the same flaw that the first systems contained thousands of years ago: if you discover the key, you can determine the message. Thus, key management is not so much the management of technology but rather the management of people.

6B. Explain firewalls and VPNs in detail.

Firewall: A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out. A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

Types of Firewalls

- **Packet filtering**: A small amount of data is analyzed and distributed according to the filter's standards.
- **Proxy service:** Network security system that protects while filtering messages at the application layer.
- **Stateful inspection**: Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.
- **Next Generation Firewall (NGFW)**: Deep packet inspection Firewall with application-level inspection.

Firewalls, focus on blocking malware and application-layer attacks. Along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls are able to react quickly and seamlessly to detect and combat attacks across the whole network. Firewalls can act on previously set policies to better protect your network and can carry out quick assessments to detect invasive or suspicious activity, such as malware, and shut it down. By leveraging a firewall for your security infrastructure, you're setting up your network with specific policies to allow or block incoming and outgoing traffic.

VPN: VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual "private network" i.e. a user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection. VPN also ensures security by providing an encrypted tunnel between client and VPN server. VPN is used to bypass many blocked sites. VPN facilitates Anonymous browsing by hiding your ip address. Also, most appropriate Search engine optimization(SEO) is done by analyzing the data from VPN providers which provide

country-wise stats of browsing a particular product. This method of SEO is used widely by many internet marketing managers to form new strategies.

VPN and its legality: Using VPN is legal in most of the countries. The legality of using a VPN service depends on the country and its geopolitical relations with another country as well. A reliable and secure VPN is always legal if you are not intended to use it for any illegal activities like committing fraud online, cyber theft, or in some countries downloading copyrighted content.

Set-2

5B. Explain in detail about information detection and prevention systems.

An intrusion detection and prevention system (IDPS) is defined as a system that monitors a network and scans it for possible threats to alert the administrator and prevent potential attacks. An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an information system, almost always with the intent to do harm. Even when such attacks are self-propagating, as in the case of viruses and distributed denial-of-service attacks. Intrusion prevention consists of activities that deter an intrusion.

Intrusion detection: consists of procedures and systems that identify system intrusions.

Intrusion reaction: encompasses the actions an organization takes when an intrusion is detected. These actions seek to limit the loss from an intrusion and return operations to a normal state as rapidly as possible.

Intrusion correction: activities finalize the restoration of operations to a normal state and seek to identify the source and method of the intrusion in order to ensure that the same type of attack cannot occur again—thus reinitiating intrusion prevention.

When a system has been attacked or is under attack, IDPS alerts and alarms take the form of audible signals, e-mail messages, pager notifications, or pop-up windows.

Basic functions of IDPS:

1. Guards technology infrastructure and sensitive data. 2. Reviews existing user and security policies. 3. Gathers information about network resources 4. Helps meet compliance regulations.

Types of IDPSs: 1. Network-Based, which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest.

2. Wireless, which monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves. It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring. **3.**

Network Behavior Analysis (NBA), which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems). **4. Host-Based,** which monitors the characteristics of a single host and the events occurring within that host for suspicious activity.

6B. Illustrate about Information Security Management?

Information security management describes the set of policies and procedural controls that IT and business organizations implement to secure their information assets against threats and vulnerabilities. Many organizations develop a formal, documented process for managing Infosec, called an Information Security Management System (ISMS).

ISM developed in response to increasing enterprise data collection over the past decade, along with the increasing threat of cyber attacks and data breaches.

Three objectives of Information Security Management: Information security at the organizational level is centered around the triad of confidentiality, integrity and availability (CIA).

Confidentiality - When it comes to InfoSec, confidentiality and privacy are essentially the same thing. Preserving the confidentiality of information means ensuring that only authorized persons can access or modify the data. Information security management teams may classify or categorize data based on the perceived risk and anticipated impact that would result if the data were compromised. Additional privacy controls can be implemented for higher-risk data.

Integrity - Information security management deals with data integrity by implementing controls that ensure the consistency and accuracy of stored data throughout its entire life cycle. For data to be considered secure, the IT organization must ensure that it is properly stored and cannot be modified or deleted without the appropriate permissions. Measures such as version control, user access controls and check-sums can be implemented to help maintain data integrity.

Availability - Information security management deals with data availability by implementing processes and procedures that ensure important information is available to authorized users when needed. Typical activities include hardware maintenance and repairs, installing patches and upgrades, and implementing incident response and disaster recovery processes to prevent data loss in the event of a cyber attack.

-> Once you have identified and quantified all of the known risks, the next step is determining what to do about it. There are several methods for dealing with risk in information security:

Avoidance - Sometimes risk can be avoided by changing business activities to eliminate the source of the vulnerability.
Acceptance - Some risks are not very likely and even if they manifested would not cause significant harm to the business. In these cases, we may be able to simply accept the risk.
Control - Move forward with the business activities, but implement controls to either lessen the potential impact of the threat or reduce the probability of the threat being realized.
Transfer - In some cases, your organization may be able to transfer risk to someone else and avoid responsibility.