What do you mean by Confinement problem?

The confinement problem is the problem of preventing a server from leaking information that the user of the service considers confidential.

Write short notes on Ring-based Access Control.

The Ring-Based concept does not allow servers to be directly accessible over a WAN such as the Internet without initially interacting with the network infrastructure. This is done by using the concept of scope where a server acts only within a given scope.

Define policy and standards.

A policy is a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters. Standards, on the other hand, are more detailed statements of what must be done to comply with policy. The organizational rules for acceptable/unacceptable behavior.

- Penalties for violations
- Appeals process

Mention the Drawbacks of ISO 17799/BS 7799.

Several countries have not adopted 17799 claiming there are fundamental problems:

- The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799
- 17799 lack "the necessary measurement precision of a technical standard".
- There is no reason to believe that 17799 is more useful than any other approach currently available
- 17799 is not as complete as other frameworks available
- 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls
- There is no reason to believe that 17799 is more useful than any other approach currently available
- 17799 is not as complete as other frameworks available
- 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls

What is firewall? How does it differ from gateway?

Firewall is a device that selectively discriminates against information flowing into or out of the organization. A Firewall can be a single device or a firewall subnet, which consists of multiple firewalls creating a buffer between the outside and inside networks. Firewalls are usually placed on the security perimeter, just behind or as part of a gateway router.

What are the resources available in web to assist an organization in developing best practices as part of security framework?

Web resources that can assist in identifying risk limits and the categorization of web applications into risk pools are considered best practices when creating a security framework. Other steps that a business should take include the generation of risk reports and a database that tracks applications being used and its risk factors.

What are the advantages and disadvantages of using honey pot or padded cell approach?

Advantages:

- Attackers can be diverted to targets that they cannot damage
- Administrators have time to decide how to respond to an attacker
- Attacker's action can be easily and extensively monitored
- Honey pots may be effective at catching insiders who are snooping around a network

Disadvantages:

- The legal implications of using such devices are not well defined
- Honey pots and Padded cells have not yet been shown to be generally useful security technologies
- An expert attacker, once diverted into a decoy system, may become angry and launch a hostile attack against an organization's systems
- Security managers will need a high level of expertise to use these systems

Distinguish between symmetric and asymmetric encryption.

Symmetric	Asymmetric
Uses the same secret (private) key to encrypt and decrypt its data	Uses both a public and private key.
Requires that the secret key be known by the party encrypting the data and the party decrypting the data.	Asymmetric allows for distribution of your public key to anyone with which they can encrypt the data they want to send securely and then it can only be Decoded by the person having the private key.
Fast	1000 times slower than symmetric

What are the seven major sources of physical loss?

- Temperature extremes
- Gases
- Liquids
- Living organisms

- ♦ Projectiles
- ♦ Movement
- ♦ Energy anomalies

What are Criteria for selecting information security personnel?

- General requirements
- Criminal History
- Education
- Citizenship
- Fingerprints
- Photographs
- Personal Information
- Drug Screening
- Social Security Number

What are the different types of Access Controls?

- Discretionary Access Controls (DAC)
- Mandatory Access Controls (MACs)
- Nondiscretionary Controls
- Role-Based Controls
- Task-Based Controls

Lattice-based Control

What are the stages in the Business Impact Analysis?

The stages in the business impact analysis step are as follows:

1. Threat attack identification
2. Business unit analysis
3. Attack success scenarios
4. Potential damage assessment
5. Subordinate plan classification

Write short notes on Honeypot.

A honeypot is a security mechanism that creates a virtual trap to lure attackers. An intentionally compromised computer system allows attackers to exploit vulnerabilities so you can study them to improve your security policies.

What is content filter?

A content filter is software filter-technically not a firewall-that allows administrators to restrict access to content from within a network. Content filtering (also known as information filtering) is the use of a program to screen and exclude from access or availability Web pages or e-mail that is deemed objectionable.

Content filtering is used by corporations as part of Internet firewall computers and also by home computer owners.