BSc.(Information Technology)

(Semester VI)

2018-19

Security in Computing

(USIT 602 Core)

University Paper Solution

By

Ms. Geeta Sahu

Question 1

Q1a. What are the importance of Information Protection? Explain with example.

The Importance of Information Protection: Information is an important asset. Information can be classified into different categories. This is typically done in order to control access to the information in different ways, depending on its importance, its sensitivity, and its vulnerability to theft or misuse.

For e.g. :U.S. government, uses a five-level classification system that progresses from Unclassified information (which everyone can see) to Top Secret information (to which only the most trusted people have access).

- **Organizations** classify information in different ways in order to differently manage aspects of its handling, such as labeling (whether headers, footers, and watermarks specify how it should be handled), distribution (who gets to see it), duplication (how copies are made and handled), release (how it is provided to outsiders), storage (where it is kept), encryption (if required), disposal (whether it is shredded or strongly wiped), and methods of transmission (such as e-mail, fax, print, and mail).

- **Companies** may have confidential information, such as research and development plans, manufacturing processes, strategic corporate information, product roadmaps, process descriptions, customer lists and contact information, financial forecasts, and earnings announcements, that is intended for internal use on a need-to-know basis. Loss or theft of confidential information could violate the privacy of individuals

- **Specialized information** or secret information may include trade secrets, such as formulas, production details, and other intellectual property, proprietary methodologies and practices that describe how services are provided, research plans, electronic codes, passwords, and encryption keys. If disclosed, this type of information may severely damage the company's competitive advantage.

- A Case Study : **Egghead Software** was a well-known software retailer who discovered in 2000 that Internet attackers might have stolen as many as 3.7 million credit card numbers from its web site, housed offsite at an e-commerce service provider that lacked good security. This information quickly made the news. The media coverage cleaned out the company's reputation. Egghead's stock price dropped dramatically, along with its sales.

Q1b. Explain various components used to build a security program?

There are many components that go into the building of a security program:

Authority:

A security program charter defines the purpose, scope, and responsibilities of the security organization and gives formal authority for the program. Usually, the security organization is responsible for information protection, risk management, monitoring, and response.

Framework:

The security policy provides a framework for the security effort. The policy describes the intent of executive management with respect to what must be done to comply with the business requirements.

Assessment:

A risk analysis provides a perspective on current risks to the organization's assets. This analysis is used to prioritize work efforts and budget allocation, so that the greater risks can receive a greater share of attention and resources. A risk analysis results in a well-defined set of risks that the organization is concerned about. These risks can be mitigated, transferred, or accepted.

Planning:

A roadmap is a plan of action for how to implement the security remediation plans. It describes when, where, and what is planned. The roadmap is useful for managers who need the information to plan activities and to target specific implementation dates and the order of actions.

It is also useful for implementers who will be responsible for putting everything together. The roadmap is a relatively high-level document that contains information about major activities and milestones coming up in the next defined period of time.

Action:

This describe how processes are performed by people on an ongoing basis to produce the desired outcomes of the security program in a repeatable, reliable fashion. Maintenance and support are part of maintaining the ongoing operations of the security program and its associated technologies, as part of a normal lifecycle of planning, updating, reviewing, and improving. The actions that should be taken when a security event occurs are defined in the incident response plan.

Maintenance:

Policy enforcement is necessary to ensure that the intentions of management are carried out by the various people responsible for the behavior and actions defined in the security policies.

Q 1c. What are the three recognized variants of malicious mobile code? Explain.

Malicious Mobile Code

There are three generally recognized variants of *malicious mobile code*: viruses, worms, and Trojans.

Computer Viruses

A virus is a self-replicating program that uses other host files or code to replicate. Most viruses infect files so that every time the host file is executed, the virus is executed too.

A virus infection is simply another way of saying the virus made a copy of itself (replicated) and placed its code in the host in such a way that it will always be executed when the host is executed. Viruses can infect program files, boot sectors, hard drive partition tables, data files, memory, macro routines, and scripting files.

Computer Worms

A computer worm uses its own coding to replicate, although it may rely on the existence of other related code. The key to a worm is that it does not directly modify other host code to replicate. A worm may travel the Internet trying one or more exploits to compromise a computer, and if successful, it then writes itself to the computer and begins replicating again.

It adds itself into the Windows start up group so it gets executed each time Windows starts. Bugbear looks for and attempts to gain access to weakly password-protected network shares and terminates antivirus programs.

E-Mail Worms

E-mail worms are the intersection of social engineering. They appear in people's inboxes as messages and file attachments from friends, strangers, and companies. They pose as cute games, official patches from Microsoft, or unofficial applications found in the digital marketplace.

Trojans

Trojan horse programs, or *Trojans*, work by posing as legitimate programs that are activated by an unsuspecting user. After execution, the Trojan may attempt to continue to pose as the other legitimate program (such as a screensaver) while doing its malicious actions in the background.

Q1d. Write a short note on Network-Layer Attack.

Network-Layer Attacks

Many attacker attacks are directed at the lower six layers of the Open Systems Interconnection (OSI) network protocol model. Network-layer attacks include packet-sniffing and protocol-anomaly exploits.

Packet Sniffing

Sniffing occurs when an unauthorized third party captures network packets destined for computers other than their own. Packet sniffing allows the attacker to look at transmitted content and may reveal passwords and confidential data.

Specialized packet driver software, must be connected to the network segment they want to sniff, and must use sniffer software. By default, a network interface card (NIC) in a computer will usually drop any traffic not destined for it. By putting the NIC in promiscuous mode, it will read any packet going by it on the network wire. Packet-sniffing attacks are more common in areas where many computer hosts share the same collision domain.

Protocol-Anomaly Attacks

Network-layer attacks usually require that the attacker create malformed traffic, which can be created by tools called *packet injectors* or *traffic generators*. Packet injectors are used by legitimate sources to test the throughput of network devices or to test the security defense of firewalls and IDSs.

There are dozens of commercial and open source packet generators that allow a fair amount of flexibility in generating TCP/IP traffic, permitting different protocols (TCP, UDP, and ICMP), packet sizes, payload contents, packet flow rates, flag settings, and customized header options. Attackers can even manually create the malformed traffic as a text file and then send it using a *traffic replay* tool.

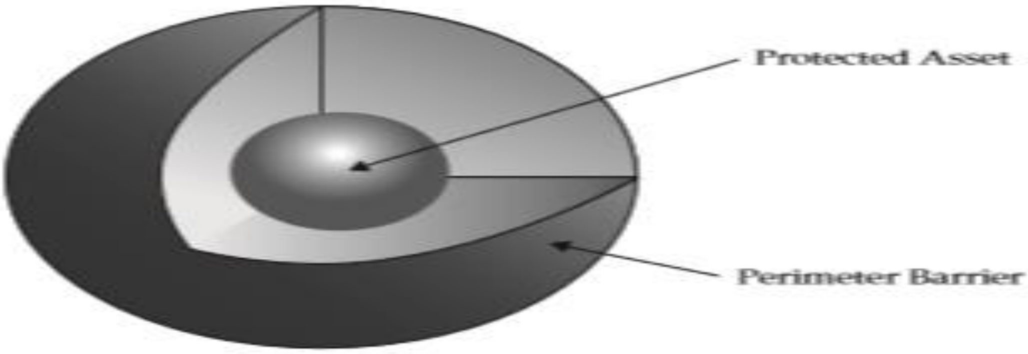
Q1e. Explain the two most common approaches of security.

1.The Lollipop Model

The most common form of defense, known as perimeter security, involves building a virtual (or physical) wall around objects of value. Perimeter security is like a lollipop with a hard, crunchy shell on the outside and a soft, chewy center on the inside.

Consider the example of a house—it has walls, doors, and windows to protect what's inside (a perimeter). But does that make it impenetrable? No, because a determined attacker can find a way in—either by breaking through the perimeter, or exploiting some weakness in it, or convincing someone inside to let them in.

By comparison, in network security, a firewall is like the house—it is a perimeter that can’t keep out all attackers. the firewall is the most common choice for controlling outside access to the internal network, creating a virtual perimeter around the internal network.

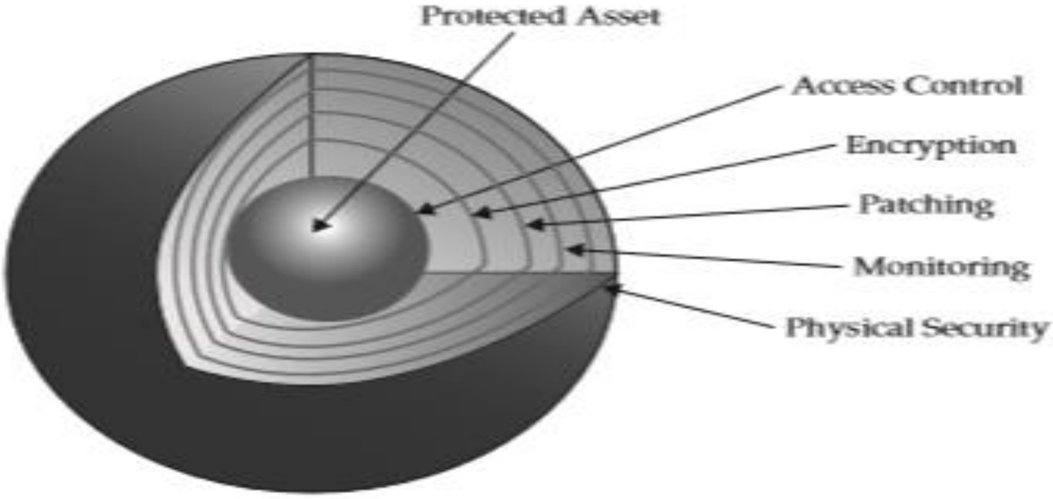


The lollipop model of defense

2.The Onion Model

It is a layered strategy, often referred to as defense in depth. This model addresses the contingency of a perimeter security breach occurring. It includes the strong wall of the lollipop. A layered security architecture, like an onion, must be peeled away by the attacker, layer by layer, with plenty of crying. The more layers of controls that exist, the better the protection against a failure of any one of those layers.

The layered security approach can be applied at any level where security controls are placed, not only to increase the amount of work required for an attacker to break down the defenses, but also to reduce the risk of unintended failure of any single technology.



The onion model of defense

Q1f. Explain the best practices for network defense.

Best Practices for Network Defense

- There are many countermeasures you can implement to minimize the risk of a successful attack, such as securing the physical environment, hardening the operating systems, keeping patches updated, using an antivirus scanner, using a firewall, securing network share permissions, using encryptions, securing applications, backing up the system, creating a computer security defense plan, and implementing ARP poisoning defenses.

Secure the Physical Environment

Regular PCs need physical protection. Depending on environment, PCs and laptops might need to be physically secured to their desks. There are several different kinds of lockdown devices, If anyone leaves their laptop on their desk overnight, it should be secured. There are also other steps that need to be taken on every PC in your environment.

Password Protect Booting

Consider requiring a boot-up password before the operating system will load. This can usually be set in the CMOS/BIOS and is called a user or boot password. This is especially important for portable computers, such as laptops and tablets and smartphones.

Password Protect CMOS

The CMOS/BIOS settings of a computer contain many potential security settings, such as boot order, remote wake-up, and antivirus boot-sector protection. It is important to ensure that unauthorized users do not have access to the CMOS/BIOS settings.

Harden the Operating System

Reduce the *attack surface* of the operating system by removing unnecessary software, disabling unneeded services, and locking down access: Reduce the attack surface of systems by turning off unneeded services. Install secure software.

Question 2

Q2a. Define authentication. Explain two parts of authentication.

Authentication

- Authentication is the process by which people prove who they are. It's composed of two parts: a public statement of identity (usually in the form of a *username*) combined with a private response to a challenge (such as a *password*).

- A password by itself, which is a means of identifying yourself through something you should know, is an example of *single-factor authentication*. Multifactor authentication refers to using two or more methods of checking identity.These methods includes :

   a. Something you know (a password or PIN code)

   b. Something you have (such as a card or token)

   c. Something you are (a unique physical characteristic)

CHAP and MS-CHAP

- One solution to the problem of securing authentication credentials across the network so they are not easily intercepted and replayed is to use the challenge and response authentication algorithms **Challenge Handshake Authentication Protocol (CHAP) and the Microsoft version, MS-CHAP**.

- These protocols use the Message Digest version 5 (MD5). The server that receives the request for access issues a challenge code and the requestor responds with an MD5 hash of the code and password. The server then compares that hash to its own hash made from the same code and password. If they are the same, the user is authenticated.

- Version 2 of MS-CHAP requires mutual authentication—the user must authenticate to the server, and the server must also prove its identity.

To do so, the server encrypts a challenge sent by the client. Since the server uses the client's password to do so, and only a server that holds the account database in which the client has a password could do so, the client is also assured that it is talking to a valid remote access server.

Q2b. Explain the authorization systems.

Authorization determines what they're allowed to do. This should always be done in accordance with the principle of least privilege—giving each person only the amount of access they require to be effective in their job function. There are a variety of types of authorization systems, including user rights, role-based authorization, access control lists, and rule-based authorization.

User Rights

Privileges or *user rights* are different from permissions. User rights provide the authorization to do things that affect the entire system. The ability to create groups, assign users to groups, log in to a system etc.Other user rights are implicit and are rights that are granted to default groups—groups that are created by the operating system instead of by administrators. These rights cannot be removed.

Role-Based Authorization (RBAC)

Each job within a company has a role to play. Each employee requires privileges (the right to do something) and permissions (the right to access particular resources and do specified things with them) if they are to do their job.

Access Control Lists (ACLs)

Attendance at some social events is limited to invitees only. To ensure that only invited guests are welcomed to the party, a list of authorized individuals may be provided to those who permit the guests in. If you arrive, the name you provide is checked against this list, and entry is granted or denied.

Information systems may also use ACLs to determine whether the requested service or resource is authorized. Access to files on a server is often controlled by information that is maintained on each file.

ACLs for Network Devices-ACLs are used by network devices to control access to networks and to

Rule-Based Authorization

Rule-based authorization requires the development of rules that stipulate what a specific user can do on a system. These rules might provide information such as "User A can access resource *Z* but cannot access resource *D*."

Q2c. Explain public key cryptography.

Public Key Cryptography

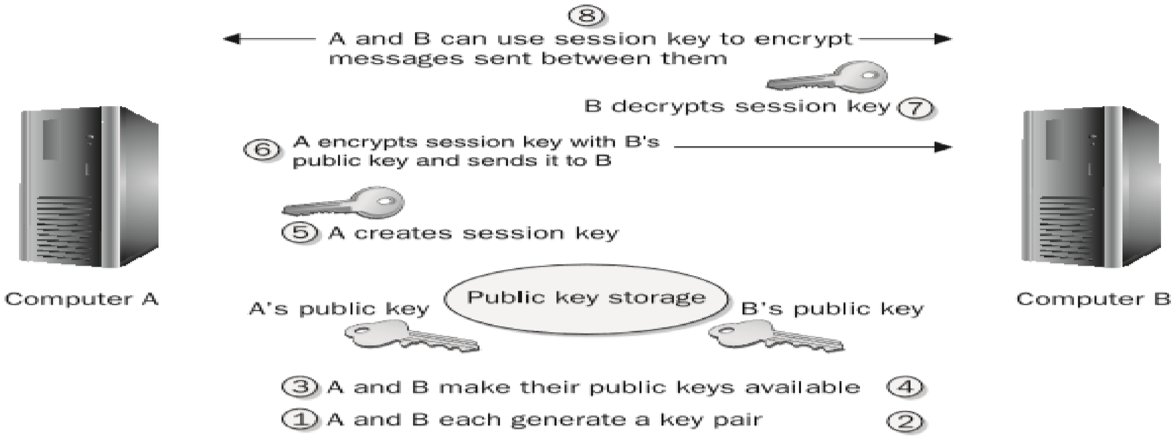
- This algorithm is asymmetric—it uses a set of related keys. If one key is used to encrypt the message, the other is used to decrypt it, and vice versa. This means that if each party holds one of the keys.

- Session key can be securely exchanged. Each party has their own set of these asymmetric keys. One of the key pairs is known as the private key and the other as the public key. Public keys are exchanged and private keys are kept secret.

- Public key is meant to be shared openly. It is used to create digital signatures. These algorithms traditionally use very large keys, and while you could use public key cryptography to encrypt whole messages or blocks of data on a disk, the process is remarkably slow compared to symmetric-key cryptography.

Key Exchange

- Public/private key pairs can be used to exchange session keys. The public keys are either exchanged among the parties or kept in a database. The private keys are kept secret. When it is necessary to exchange a key, one party can encrypt it using the public key of the other. The encrypted key is then transmitted to the other party. Since only the intended recipient holds the private key that is related to the public key used to encrypt the session key, only that party can decrypt the session key.


⑧
A and B can use session key to encrypt messages sent between them
B decrypts session key ⑦
⑥ A encrypts session key with B's public key and sends it to B
⑤ A creates session key
Computer A
Computer B
A's public key
Public key storage
B's public key
③ A and B make their public keys available ④
① A and B each generate a key pair ②

Using public key cryptography for key exchange

Q2d. What are the three categories of storage infrastructure in modern storage security?

In securing these components, there are three primary categories:

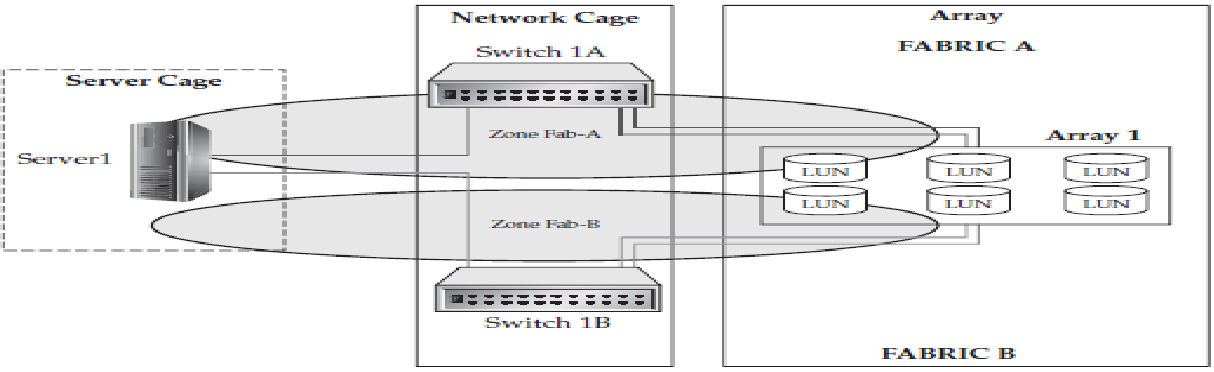
Storage networks

Arrays

Servers

Storage Networks

A Logical Unit Number (LUN) is the mechanism an array uses to present its storage to a host operating system. Someone may connect a server to the environment and configure it, LUNs are applied so that the server cannot gain access to restricted LUNs. Isolating data traffic between LUNs via the switch is accomplished through the use of *zoning*. Zoning creates a protected zone where only identified devices within that zone are allowed to communicate with each other.



Security areas of zoning

Zoning protects against a faulty hardware device affecting other servers through excessive chatter. Zoning also provides the opportunity for redundancy.

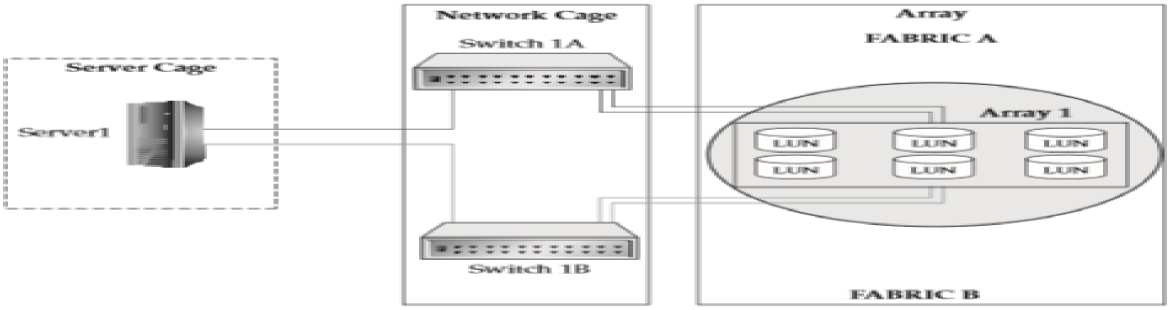
Port Zoning The characteristic of port zoning is that the accessibility of the host to the LUNs is defined by the switch port. The advantage to zoning is that an intruder cannot connect a host to the switch, enable spoofing of a good WWN, and access LUNs of another host. The disadvantage of port zoning is that management requires extra work.

WWN Zoning -The zones are created relative to the ports the servers are connected to on the switch, which defines the individual zone based on the WWN ID of the host bus adapter (HBA). The WWN is very much like the MAC address of a network card. It is a 16-digit hexadecimal number that uniquely identifies the HBA within the SAN fabric.

Arrays

When LUNs are created, it is necessary for the array to provide a screen to prevent the data that resides on the array from being accessed by other hosts that are able to connect to the array.

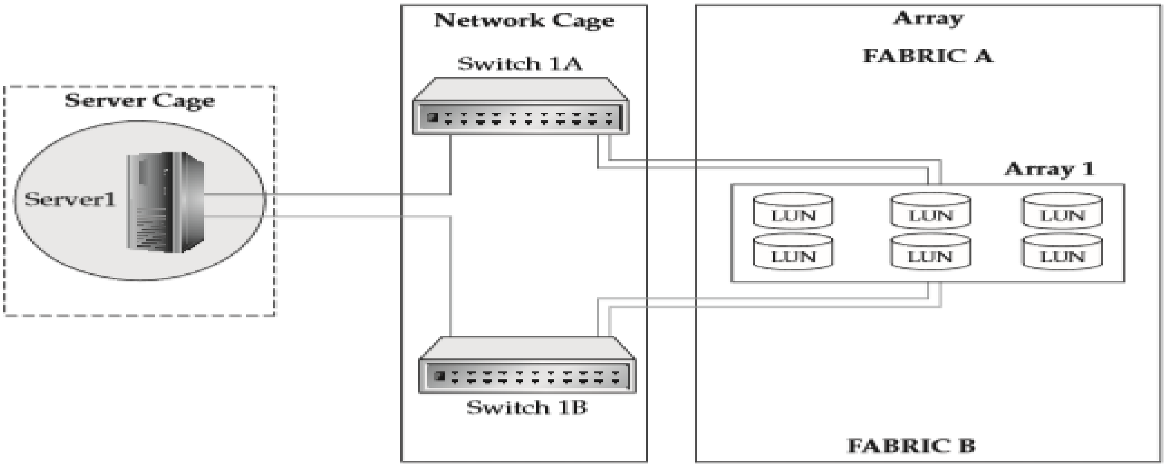
Storage arrays are therefore equipped with a mechanism that provides protection known as LUN masking. This allows multiple hosts to communicate with the array and only access LUNs that are assigned through the application that provides the LUN-masking protection.Once the data is put on the server, the potential still exists for that data to be accessed by other hosts on other networks. LUN masking adds a layer of protection to the data once that data resides on the storage array.



Security areas of arrays

Servers

As long as the data “rests” on the server, the potential to access that data exists. Many options are available to protect that data while it is at rest on the server. The concern of the storage administrator is what happens if someone is able to access the data either locally or remotely.



Security areas of servers

Q2e. Write a short note on Integrity risks.

Integrity Risks

Integrity risks affect both the validity of information and the assurance that the information is correct. If information can be changed without warning, authorization, or an audit trail, its integrity cannot be guaranteed.

Malfunctions

Computer and storage failures that corrupt data damage the integrity of that data.

Defense

Make sure the storage infrastructure which is selected has appropriate RAID redundancy built in and that archives of important data are part of the service.

Detection Employ integrity verification software that uses checksums or other means of data verification.

Deterrence

Due to the nature of data, because there is no human element involved, there isn't much that can be done.

Residual risk

Technology failures that damage data may result in operational risk.

Q2f. Explain Database Level Security.

Database Roles and Permissions

The general process begins with specifying to which database(s) a login may connect. Then, permissions must be assigned within the database. Database administrators will create "groups" or "roles," and each of these will contain users. Specific permissions are assigned to the roles. Some relational database platforms allow groups to be nested, thereby allowing you to create a hierarchy of permissions in a specific table.

Users of this role might also be able to call certain stored procedures, views, and other database objects.

Object-Level Security: Relational databases support many different types of objects. Tables. Each table is generally designed to refer to some type of entity Permissions are granted to execute one or more of the most commonly used SQL commands.

These commands are SELECT Retrieves information from databases. SELECT statements can obtain and combine data from many different tables, and can also be used for performing complex aggregate calculations. .

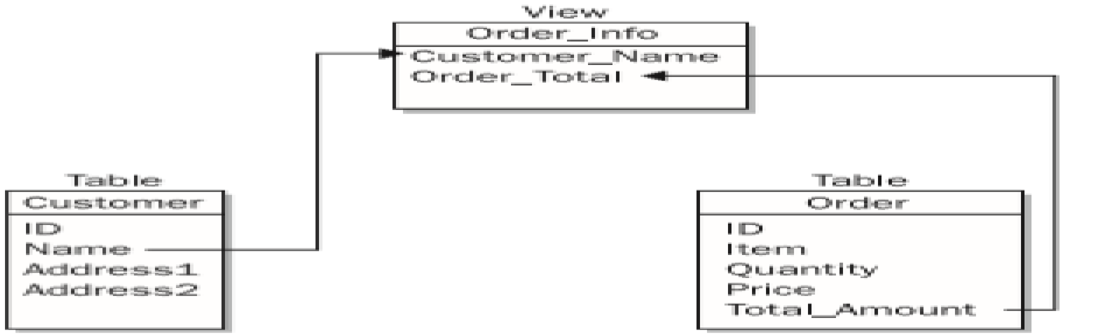
INSERT adds a new row to a table. UPDATE Changes the values in an existing row or rows. DELETE Deletes rows from a table. GRANT specifies that a particular user or role will have access to perform a specific action. REVOKE removes any current permissions settings for the specified users or roles. DENY prevents a user or role from performing a specific action.

Views A view is a logical relational database object that actually refers to one or more underlying database tables. Views are generally defined simply as the result of a SELECT query. This query, in turn, can pull information from many different tables and can also perform common calculations on the data.

Views can query other views, thereby creating a chain of objects based on business rules. When portions of the logic change, only some of the views may be affected. Views are generally used to return sets of data to users. Database developers can allow users to modify data through the use of views.

Stored Procedures - Databases offer developers the ability to create and reuse SQL code through the use of objects called stored procedures. Stored procedures can be used to perform any function that is possible through the use of standard SQL commands.

A stored procedure might be used to automatically perform common operations on a set of customer-related database tables. When a customer record changes, corresponding changes can be easily made by calling the stored procedure.



A conceptual diagram of a database view

Triggers -Triggers are designed to automatically be "fired" whenever specification actions take place within a database. Triggers can be used in different ways. It can use triggers to perform detailed auditing. Another use of triggers is to enforce complex database-related rules. If your marketing staff is only allowed to add information to a table in a specific format, or if you want to ensure that a series of actions is always taken when data changes are made, you can write the appropriate trigger to do so.

Question 3

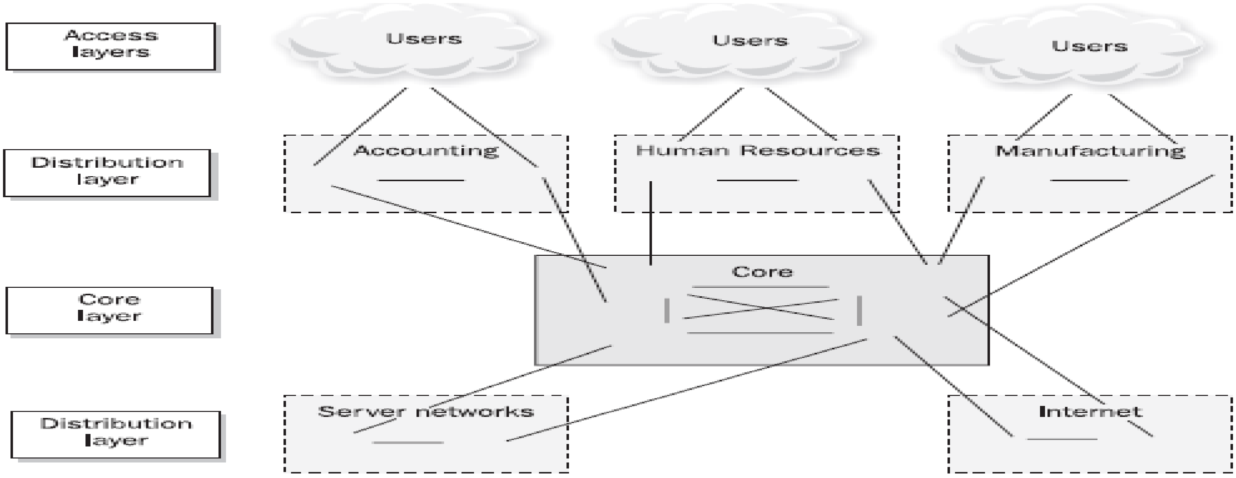
Q3a. Explain the Cisco Hierarchical Internetworking model.

The Cisco Hierarchical Internetworking model, depicted in Figure, uses three main layers - core, distribution, and access layers.

Core layer Forms the network backbone and is focused on moving data as fast as possible between distribution layers. it should not be used to perform CPU-intensive operations such as filtering, compressing, encrypting, or translating network addresses for traffic.

Distribution layer Sits between the core and the access layer. This layer is used to aggregate access-layer traffic for transmission into and out of the core.

Access layer Composed of the user networking connections.



The Cisco Hierarchical Internetworking model

Filtering, compressing, encrypting, and address-translating operations should be performed at the access and distribution layers. The Cisco model is highly scalable. As the network grows, additional distribution and access layers can be added. This model assists in higher levels of availability by allowing implementation of redundant hardware at the distribution and core layers.

The following are two-tier network fundamentals:

Core The core of the two-tier network is a highly available, horizontally scalable element used for transit and moving data between different areas or zones in the network. The difference is the core in a two-tier network doesn’t see 100 percent of the traffic.

Distribution The distribution layer in some collapsed networks either is eliminated completely or is combined with the access layer as part of the fabric. it does not logically exist, as it is part of the same switch fabric or switching cluster as the access switching.

Access The access layer is collapsed into the distribution layer, so while physically separate devices may provide the aggregation and access function; both can be part of the same layer-two domain. These combined layers offer active/active connectivity across multiple switches via clustering for high availability and performance.

Q3b. Explain network availability and security.

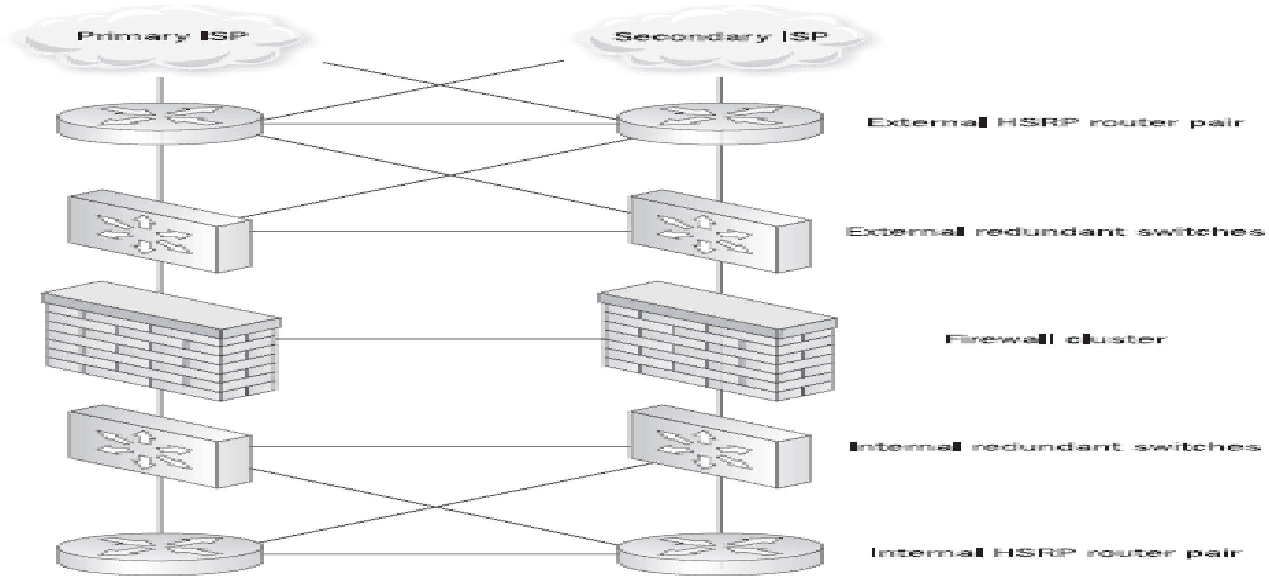
Availability

Network availability requires that systems are appropriately resilient and available to users on a timely basis. The opposite of availability is denial of service, which is when users cannot access the resources they need on a timely basis.

The best practice for ensuring availability is to avoid single points of failure within the architecture. This can require redundant and/or failover capabilities at the hardware, network, and application functions.

The switch becomes a single point of failure, and any interruption in its normal operation would take firewalls off the network, if there is only a single router between the firewalls and the rest of the network, the failure of that router would also cause an outage.

Figure shows a full high-availability network segment without a single hardware point of failure. this example uses Cisco’s Hot Standby Router Protocol, which is a built-in protocol for switching routes if a router or interface goes down).


Primary ISP
Secondary ISP
External HSRP router pair
External redundant switches
Firewall cluster
Internal redundant switches
Internal HSRP router pair

A full high-availability network design

A true high-availability design will incorporate redundant hardware components at the switch, network, firewall, and application levels. When eliminating failure points, be sure to consider all possible components.

Designers can and should consider maintaining multiple Internet links to different Internet service providers to insulate an organization from problems at any one provider. Load balancers also play an important role in maintaining the availability and performance of network-based services.

Security

When designing and implementing security in network, it is helpful to identify critical security controls and understand the consequences of a failure in those controls.

For example, firewalls protect hosts by limiting what services users can connect to on a given system. Firewalls can allow different sets of users selective access to different services, such as allowing system administrators to access administrative services while preventing non-administrative users from accessing those same services.

By denying a non-administrative user the ability to connect to the administrative service, that user is prevented from growing an attack directly on that service without avoiding the firewall. Application-layer gateways firewalls can help protect segmented networks by ensuring that traffic being sent as a particular service over a particular port is in traffic for that service.

Q3c. Write short note on hubs and switches.

Hubs

Hubs were dumb devices used to solve the most basic connectivity issue: how to connect more than two devices together. They transmitted packets between devices connected to them, and they functioned by retransmitting each and every packet received on one port out through all of its other ports without storing or remembering any information about the hosts connected to them.

This created scalability problems for legacy half-duplex Ethernet networks, because as the number of connected devices and volume of network communications increased, collisions became more frequent, degrading performance. A collision occurs when two devices transmit a packet onto the network at almost the exact same moment, causing them to overlap and thus mangling them. When this happens, each device must detect the collision and then retransmit their packet in its entirety.

Switches

Switches are layer two devices and routers are layer three devices. They are more intelligent devices that learn the various MAC addresses of connected devices and transmit packets only to the devices they are specifically addressed to.

Since each packet is not rebroadcast to every connected device, the likelihood two packets will collide is reduced. In addition, switches provide a security benefit by reducing the ability to monitor or “sniff” another workstation’s traffic.

With a hub, every workstation would see all traffic on that hub; with a switch, every workstation sees only its own traffic. A switched network cannot absolutely eliminate the ability to sniff traffic. An attacker can trick a local network segment into sending it another device’s traffic with an attack known as *ARP poisoning*.

Any workstation that receives this broadcast would update its ARP tables and thereafter would send all of Victim’s traffic to Attacker. This ARP packet is commonly called a *gratuitous ARP* and is used to announce a new workstation attaching to the network.

Q3d. Explain the features of firewall.
Firewall Features

Application Awareness

The firewall must be able to process and interpret traffic from OSI layers three through seven. At layer three, it should be able to filter IP address; at layer four by port; at layer five by network sessions; at layer six by data type, and, at layer seven to properly manage the communications between applications.

Accurate Application Fingerprinting

The firewall should be able to correctly identify applications, Correct application identification is necessary to ensure that all applications are properly covered by the firewall policy configuration.

Granular Application Control

In addition to allowing or denying the communication among applications, the firewall also needs to be able to identify and characterize the features of applications so they can be managed appropriately. File transfer, desktop sharing, voice and video, and in-application games are examples of potentially unwanted features that the firewall should be able to control.

Bandwidth Management (QoS)

The Quality of Service (QoS) of preferred applications, which might include Voice over IP (VoIP) can be managed through the firewall based on real-time network bandwidth availability. If a sporting event is broadcast live via streaming video on a popular web site, firewall should be able to proactively limit or block access so all those people who want to watch it don’t bring down your network.

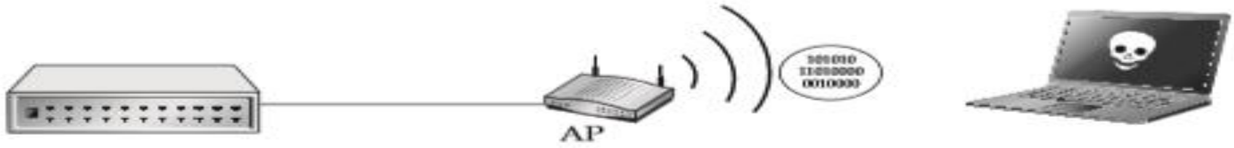
Q3e. Explain the five different types of wireless attacks.
Five types of wireless attacks:

1. Rogue (harmful) Access Points (AP) - Rogue AP is an unsanctioned wireless access point connected to the physical network. It involves a user who brings a consumer-grade access point like a Linksys router into the office. Many organizations attempt to detect rogue APs through wireless assessments. it is important to validate if they are connected to the physical network.

2. Wired Side Leakage

On wireless networks, investigation involves promiscuously listening for wireless packets using a wireless sniffer so the attacker can begin to develop a footprint of the wireless network. If the attacker were associated to an access point, then he or she could sniff layer three and above.

Most access points and wireless switches allow this traffic to leak into the airspace without being blocked. Figure illustrates this concept with a network device that is connected to an AP via a wired network, leaking internal protocol communications onto the airwaves. This traffic may reveal network topology, device types, usernames, and even passwords.



Network device traffic can leak onto the wireless airspace.

3. Misconfigured Access Points

Human error coupled with different administrators installing the access points and switches can lead to a variety of misconfigurations. For example, an unsaved configuration change can allow a device to return to its factory default setting the device reboots during a power outage. These devices must be monitored for configurations that are in line with policies.

4. Wireless Phishing

Users may unknowingly connect to a wireless network that they believe is the legitimate access point. But that has, in fact, been set up as a honeypot or open network specifically to attract unsuspecting victims. For example, they may have a network at home called “Linksys.” As a result, their laptop may automatically connect to any other network known as “Linksys.”

5. Client Isolation

Most users connect to the access point to obtain Internet access or access to the corporate network, but they can also fall victim to a malicious user of that same wireless network. In addition to eavesdropping, a malicious user can also directly target other users as long as they’re associated to the same access point. once a user authenticates and associates to the access point, he or she obtains an IP address and, therefore, layer three access.

Q3f. What are the countermeasures against the possible abuse of wireless LAN?

These countermeasures include:

a. Secure replacements for WEP
b. Proper wireless user authentication
c. Intrusion detection and anomaly tracking on wireless LANs

Temporal Key Integrity Protocol and Counter Mode with CBC-MAC Protocol

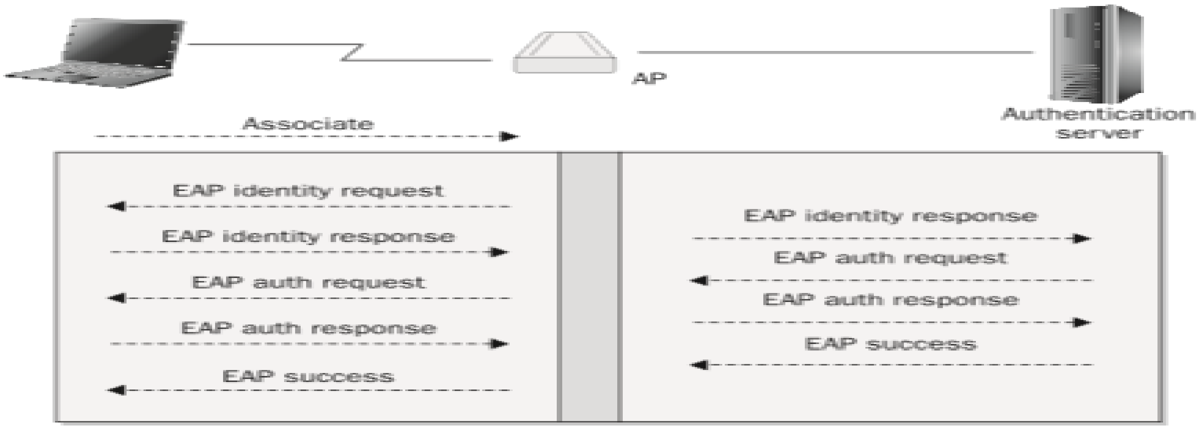
The Temporal Key Integrity Protocol (TKIP) and the Counter Mode with CBC-MAC Protocol (CCMP) are WPA2 encryption protocols on 802.11 LANs. TKIP encrypts each data packet with a unique encryption key. To increase key strength, TKIP includes four additional algorithms:

A cryptographic message integrity check to protect packets. An initialization-vector (IV) sequencing mechanism that includes hashing. A per-packet key-mixing function to increase cryptographic strength. A rekeying mechanism to provide key generation every 10,000 packets.

802.1x-Based Authentication and EAP Methods

802.1x can also be used for the dynamic distribution of WEP keys. An association between the wireless client and the access point is assumed to be a network access port. 802.1x, the wireless client is defined as a supplicant (or peer), and the access point, as an authenticator an authentication server is needed on the wired network segment to which the access point is connected.

This service is usually provided by a RADIUS server supplied with some form of user database, such as native RADIUS, LDAP, NDS, or Active Directory. Wireless gateways can implement the authentication server, as well as the authenticator functionality User authentication in 802.1x relies on the layer two Extensible Authentication Protocol. EAP frame exchange between the supplicant, authenticator, and authentication server is summarized in Figure



EAP authentication process

Wireless Intrusion Detection and Prevention

Wireless IPS identifies wireless attacks using wireless sensors. These wireless sensors typically use the same Wi-Fi radios that are found in access points,

Wireless IDS involves receiving packets only. Its coverage is, therefore, more physically broad compared to an access point, which transmits and receives. In a typical access point and sensor use, the rule of thumb is one sensor for every three access points.

Question 4

Q4a. Explain intrusion Defense System types and detection models.

IDS Types:

1. A host-based IDS (HIDS) -is installed on the host it is intended to monitor. The host can be a server, workstation, or any networked device (such as a printer, router, or gateway). A HIDS installs as a service or daemon, or it modifies the underlying operating system's kernel or application to gain first inspection authority.

A file-integrity HIDS (sometimes called a snapshot or checksum HIDS) takes a cryptographic hash of important files in a known clean state and then checks them again later for comparison. If any changes are noted, the HIDS alerts the administrator that there may be a change in integrity.

2. Network-Based IDS (NIDS) -are the most popular IDSs, and they work by capturing and analyzing network packets on the wire. NIDS is designed to protect more than one host. It can protect a group of computer hosts, or monitor an entire network. Captured traffic is compared against protocol specifications and normal traffic trends or the packet's payload data is examined for malicious content.

If a security threat is noted, the event is logged and an alert is generated. NIDS works by examining network packet traffic, including traffic not intended for the NIDS host on the network.

IDSs follows two detection models—anomaly (also called profile, behavior, heuristic, or statistical) detection or signature (knowledge-based) detection.

1. Anomaly-Detection (AD) Model

Some IDS vendors refer to AD systems as behavior-based since they look for deviating behaviors. If an IDS looks only at network packet headers for differences, it is called protocol anomaly detection.

The goal of AD is to be able to detect a wide range of malicious intrusions, including those for which no previous detection signature exists. AD system identifies and stores all the normal activities that occur on a system or network, it can alert to everything else that doesn't fit the normal profile.

2. Signature-Detection Model

Signature-detection or *misuse* IDSs work by using databases of known bad behaviors and patterns. Signature-detection engines can query any portion of a network packet or look for a specific series of data bytes. The defined patterns of code are called *signatures,* and are included as part of a governing *rule* when used within an IDS.A byte signature may contain a sample of virus code, a malicious combination of keystrokes used in a buffer overflow, or text that indicates the attacker is looking for the presence of a particular file in a particular directory.

Q4b. Write short note on Security Information and Event management.

Security Information and Event Management (SIEM)

Multiple security systems can report to a centralized *Security Information and Event Management (SIEM) system*, bringing together logs and alerts from several disparate sources. "Security Incident and Event Management" or "Security Incident and Event Monitoring."—a technology to collect, analyzes, and correlates events and alerts generated by monitoring systems.

SIEM platforms take the log files, find commonalities (such as attack types and threat origination), and summarize the results for a particular time period. For example, all logs and alerts from all IDSs, perimeter firewalls, personal firewalls, antivirus scanners, and operating systems can be tied together.

SIEM can significantly reduce false positives by verifying information based on other data. That data comes from many sources, including workstations, servers, computing infrastructure, databases, applications, network devices, and security systems. SIEM products need to be fast and effective, with a significant amount of storage and computing power.

SIEM can do the following:

1.Data Aggregation

SIEMs collect information from every available source that is relevant to a security event. These sources take the form of alerts, real-time data, logs, and supporting data. these provide the correlation engine of the SIEM with information it can use to make decisions about what to bring to the security administrator's attention.

2. Alerts

The SIEM's key function is to validate security alerts using many different sources of data to reduce false positives, so only the most reliable alerts get sent on to the security administrator.

3. Real-Time Data

Real-time data such as network flow data gives the SIEM additional information to correlate. Streaming this data into the SIEM provides important information about normal and abnormal traffic patterns that can be used in conjunction with alerts to determine whether an attack is in progress.

4.Logs

Logs are different from events, in that they are a normal part of system activity and meant for debugging purposes. Logs contain valuable information about what's happening on a system. For example, login failures that may otherwise go unnoticed by a system administrator especially if there are many login failures for a single account, if there are login failures on many different accounts.

5. Supporting Data

Data can be imported into the SIEM, and it will use that data to make comparative determinations. For example, asset management data containing names, IP addresses, operating systems, and software versions gives the SIEM valuable information it can use to determine whether an IDS alert makes sense within the context of the software environment.

Q4c. What are the components of Voice over IP.

VoIP Components

1. Call Control

The call control element (the "brains" of the operation) of a VoIP system can be either an appliance, a piece of software that runs on a specialized server operating system, or a piece of network hardware embedded into another networking component. There are special types of call control elements such as session border controllers (SBCs) and voice proxies that are designed to be exposed to or interface with systems under a different administrative domain.

2. Voice and Media Gateways and Gatekeepers

Gateways are configured to use *dial peers* (defined as "addressable endpoints") to originate and receive calls. Some gateways are directly managed by the call control elements via a control protocol (MGCP or H.248), whereas others operate in a more independent, stand-alone capacity (H.323 or SIP). Voice gateways can also run soft switches and perform primary (or survivable) call processing or "all-in-one" functions.

3. MCUs

The Conference Bridge, or multi-conference unit (MCU), a multiport bridging system for audio, video, and multimedia collaboration. Conferencing and collaboration is used extensively within and across all enterprises as part of the fundamental communications capability that connects all users to each other.

A problem with an MCU can affect a lot of users at once. Like gateways, MCUs are frequently exposed to the outside world, and are commonly used by everyone in the organization up through executive level. MCUs can connect different types of media; require those facilities to be secured.

An off-premise MCU provided by an experienced third party is often more easily secured than an internally hosted MCU that is exposed, as the service providers have had some practice at securing MCSs

4. Hardware Endpoints

The hardware phone or video codec, sitting quietly idle in the office but running 24/7, may, become an important tool for advanced corporate espionage, eavesdropping, or denial of service attacks. Video codec run all kinds of custom code required for video conferencing and content sharing and are sometimes directly exposed to the Internet.

5. Software Endpoints

This is a piece of software that runs on a PC or mobile device and acts like a hardware endpoint by registering to the call control element(s) as a device. Second, by running the soft client, you can extend your enterprise features to the mobile user, including functionality not available on mobile devices such as extension-based or URI dialing.

6. Call and Contact Center Components

Call centers are being used as a place to take orders and field complaints. Centers have morphed into “contact centers” and “centers of excellence.” Trusted to sustain 24/7/forever operation and provide all levels of support to customers across every industry imaginable, these highly complex distributed systems.

7. Voicemail Systems

VoIP-based telephony system is the voicemail system. Auto attendants, direct inward system access (DISA) features used for manual call forwarding, automatic call forwarding, and other voicemail features.

Anyone who has ever built a voicemail system knows the practice of initially setting everyone’s default password to their extension, or perhaps the last four digits of their direct inward dialing (DID) phone number, or some other easy-to figure- out formula. Some of a voicemail system’s convenience “features” need outside access in order to work properly.

Q4d. Write short note on Private Bank Exchange.
PBX

A Private Branch Exchange (PBX) is a computer-based switch that can be thought of as a local phone company. Following are some common PBX features:

Multiple extensions

Voicemail

Call forwarding

Fax management

Remote control (for support)

Hacking a PBX

Attackers hack PBXs for several reasons: To gain confidential information (espionage). To place outgoing calls that are charged to the organization’s account.To cause damages by crashing the PBX

Administrative Ports and Remote Access

Administrative ports are needed to control and diagnose the PBX. Vendors often require remote access via a modem to be able to support and upgrade the PBX.

This port is the hacker entry point. An attacker can connect to the PBX via the modem; or if the administrative port is shared with a voice port, the attacker can access the port from outside the PBX by calling and manipulating the PBX to reach the administrative port.

Voicemail

An attacker can gain information from voicemail or even make long-distance phone calls using a “through-dial” service. An attacker can discover a voicemail password by running an automated process that “guesses” easy passwords such as “1111,” , “1234,” and so on.

Denial of Service

A PBX can be brought down in a few ways: PBXs store their voicemail data on a hard drive. An attacker can leave a long message, full of random noises, in order to make compression less effective—whereby a PBX might have to store more data than it anticipated.

Securing a PBX. Here is a checklist for securing a PBX:

Connect administrative ports only when necessary.

Protect remote access with a third-party device or a dial-back.

Review the password strength of your users’ passwords.

Allow passwords to be different lengths, and require the # symbol to indicate the end of a password, rather than revealing the length of the password.

Q4e. Explain different classic security models.

Classic Security Models

Famous security models are Bell-LaPadula, Biba, and Clark-Wilson.

1.Bell-LaPadula

Bell-La Padula model was published in 1976. This model was one of the first attempts to celebrate an information security model. It was designed to keep secrets, not to protect data integrity. The model prevents users and processes from reading above their security level.

This is used within a data classification system—so a given classification cannot read data associated with a higher classification.—as it focuses on sensitivity of data.

This model prevents objects and processes with any given classification from writing data associated with a lower classification.

2. Biba

Biba is known as a reversed version of Bell-LaPadula, as it focuses on integrity labels, rather than sensitivity and data classification.

It covers integrity levels, which are similar to sensitivity levels in Bell-LaPadula, and the integrity levels cover inappropriate modification of data. It attempts to preserve the first goal of integrity, to prevent unauthorized users from modifying data.

3.Clark-Wilson

Clark-Wilson attempts to define a security model based on accepted business practices for transaction processing. It articulates the concept of *well-formed transactions* that Perform steps in order. Authenticate the individuals who perform the steps

TCSEC (*Trusted Systems Security Evaluation Criteria)*

The United States Department of Defense published a series of documents to classify the security of operating systems, known as the *Trusted Systems Security Evaluation Criteria* .

TCSEC was developed to meet three objectives:

To give users a yardstick for assessing how much they can trust computer systems for the secure processing of classified or other sensitive information

To guide manufacturers in what to build into their new, widely available commercial products to satisfy trust requirements for sensitive applications.

To provide a basis for specifying security requirements for software and hardware.

Q4f. Write short note on trustworthy computing.

Trustworthy Computing. The four goals of the Trustworthy Computing initiative are :

Security As a customer, you can expect to withstand attack. In addition, you can expect the data is protected to prevent availability problems and corruption.

Privacy You have the ability to control information about yourself and maintain privacy of data sent across the network.

Reliability When you need your system or data, they are available.

Business integrity The vendor of a product acts in a timely and responsible manner, releasing security updates when vulnerability is found.

Trustworthy Computing initiative, Microsoft created a framework to explain its objectives: its products be secure by design, secure by default, and secure in deployment, it provide communications (SD3+C).

Secure by design means all vulnerabilities are resolved prior to shipping the product. Secure by design requires three steps.

1. *Build a secure architecture.* Software needs to be designed with security and features.

2. *Add security features.* Feature sets need to be added to deal with new security vulnerabilities.

3. *Reduce the number of vulnerabilities in new and existing code.*

Question 5

Q5a. Define virtual machine. How is hypervisor responsible for managing all guest OS installation on a VM server?

In a *virtual machine* (VM), the OS (referred to as a "guest OS" when virtualized) and the software applications that it hosts run on *virtual hardware*.In a virtualized environment, everything is software—therefore, the risks are greater. Virtual machines carry their own security risks, unique from those of computer systems and local area networks.

Protecting Virtual Storage

Guest OS systems can utilize virtual or physical network attached storage (NAS) and storage area networks (SAN) allocated by the hypervisor to meet data storage requirements, as if these storage devices were directly attached to the system.

Protecting the Hypervisor

The hypervisor is responsible for managing all guest OS installations on a VM server, and the service console provides a centralized location for managing all the servers in a virtual environment.

Hypervisor and service console servers need to be properly patched and secured, as well as logically separated through the use of isolated networks with strict access controls.

Protecting the Guest OS

Hypervisor manages access to hardware resources so that each guest OS is able to access only its own allocated resources, such as CPU, memory, and storage, but not those resources allocated to other guest OSs. This characteristic is known as *partitioning* and is designed to protect each guest OS from other guest OS instances, so attacks and malware are unable to "cross over."

Partitioning also reduces the threat of *side-channel attacks* that take advantage of hardware usage characteristics to crack encryption algorithms or implementations. Partitioning, therefore, is considered an important security measure. If an attacker attempts to "break out" of a guest OS to access the hypervisor or neighboring guest OSs, this is referred to as an *escape*.

If an attacker were to escape his or her guest OS and access the hypervisor, the attacker could potentially take over the hypervisor's entire guest OSs. The hypervisor monitors and tracks the state of its guest OSs, which is a function commonly, referred to as *introspection*.

Introspection can be integrated with intrusion detection systems (IDS) or intrusion prevention systems (IPS) and security information and event management (SIEM).

Protecting Virtual Networks

The hypervisor can present the guest OS with either physical or virtual network interfaces. hypervisors provides three choices for network configurations:

Network bridging

The guest OS has directs access to the actual physical network interface cards (NIC) of the real server hardware.

Network Address Translation (NAT)

The guest OS has virtual access to a simulated physical NIC that is connected to a NAT emulator by the hypervisor. As in a traditional NAT, all outbound network traffic is sent through the virtual NIC to the underlying subsystem to get routed to the main network, or directly to other guest OSs.

Host-only networking

A guest OS has virtual access to a virtual NIC that does not actually route to any physical NIC. Network packets are translated by the hypervisor from one guest OS to another without any physical network connectivity.

Q5b. What is cloud computing? Explain the types of cloud services.

Cloud Computing

Cloud computing provides a way to increase capacity or add capabilities, training new personnel, or licensing new software cloud service providers have experienced full service outages, performance issues, and various types of security breaches

Cloud providers are well-suited for large file-size content, with lots of read access, such as digital content and streaming media, video, and music, as well as for long-term file storage, such as data backups and data archives.

Types of Cloud Services: The types of services /"cloud" associated :

Infrastructure-as-a-Service (IaaS) -This type of service allows consumers to provision processing, storage, and networking resources, allowing them to deploy and run their own operating systems or applications in their own cloud environment.

Software-as-a-Service (SaaS) - This type of cloud computing delivers a single application through the browser to customers using a multitenant architecture.

Utility computing - Companies that offer storage and virtual servers that IT can access on demand. Enterprise adopters use utility computing for supplemental, non-mission-critical needs.

Platform-as-a-Service (PaaS) - This form of cloud computing delivers development environments as a service. Build your own applications that run on the provider's infrastructure and are delivered to your users .

Web services in the Cloud - It offer APIs that enable developers to exploit functionality over the Internet, rather than delivering full-blown applications.

Managed service providers (MSP) - It is basically an application exposed to IT rather than to end users. Examples include virus scanning services, e-mail spam filtering services, application monitoring services, and managed security services.

Q5c. Explain the application security practices and decisions that appear in most secure development lifecycle.

Application Security Practices are :

1. Security Training

Security training program for development teams includes technical security awareness training for everyone and role-specific training for most individuals. Role-specific training about the security activities a particular individual participates in, and the technologies in use.

2.Secure Development Infrastructure

At the beginning of a new project, source code repositories, file shares, and build servers must be configured for team members' exclusive access, bug tracking software must be configured to disclose security bugs only according to organization policies, project contacts must be registered in case any application security issues occur, and licenses for secure development tools must be acquired.

3.Security Requirements

Security requirements may include access control matrices, security objectives, abuse cases, references to policies and standards, logging requirements, security bug bars, assignment of a security risk or impact level, and low-level security requirements such as key sizes or how specific error conditions should be handled.

4. Secure Design

Secure design activities usually revolve around secure design principles and patterns. They also frequently include adding information about security properties and responsibilities.

5. Threat Modeling

Threat modeling is a technique for reviewing the security properties of a design and identifying potential issues and fixes. Architects can perform it as a secure design activity, or independent design reviewers can perform it to verify architects' work. There is a variety of threat modelling methodologies to choose from.

6. Secure Coding

Secure coding includes using safe or approved versions of functions and libraries, eliminating unused code, following policies, handling data safely, managing resources correctly, handling events safely, and using security technology correctly.

Q5d. Explain the reasons for remote administration security. What are the advantages of web remote administration?

Reasons for Remote Administration. Remote administration is needed for various reasons:

Relocated servers

An administrator needs an interface to administer any relocated web servers

Outsourced services

Managing security products requires knowledge that some organizations don't possess, so they often outsource their entire security management to a firm specializing in that area.

Physical distance

An administrator may need to manage a large number of computers in the organization. Some organizations span several buildings (or cities), and physically attending the computers can be a tedious and time-consuming task. Additionally, physical access may be limited to the actual data centers.

Advantages of remote web administration:

Quick development time

Developing a web interface is faster than developing a GUI client, in terms of development, debugging, and deployment.

OS support

A web interface can be accessed from all the major OSs by using a browser

Accessibility

A web interface can be accessed from any location on the Internet.

User learning curve

An administrator knows how to use a browser, so the learning curve for the administrator will be shorter.

Accessibility

Because web administration is accessible from anywhere on the Internet, it's also accessible to an attacker who may try to hack it.

Browser control

Because a browser controls the interface, an attacker doesn't need to deploy a specific product control GUI .

Support

Web-based applications are typically easier to support and maintain.

Authenticating Web-Based Remote Administration

When connecting to the remote web administration interface, the first hurdle to clear is the authentication process. If the authentication is weak, an attacker can bypass it and take control of the application or computer.

HTTP Authentication Methods

it's important to go over the current methods available to authenticate HTTP connections:

Securing Web-Based Remote Administration

The best solution for securely logging in to a web-administered server is to use either SSL, which checks for client certificates, or encrypted basic authentication. (SSL can also authenticate the server against a third-party certificate authority to ensure it is the server you meant to connect to.)

Q5e. Explain the security considerations for choosing a secure site location.

Choosing Site Location for Security

When choosing a location for a data center or office site, survivability should be considered more important than cost.

Low-cost sites may have risks associated with them that outweigh their cost savings. If the site is in a flood zone, an area likely to be hit by a tornado or hurricane, an earthquake zone, or high-crime area, there is a significant risk that one of these events could cause a lot of expensive damage. A well-designed and well-maintained site will have a backup power generator, security guards, Security considerations for choosing a secure site location are :

1. Accessibility

Accessibility of the site is first consideration. If a site is located too remotely to be practical, usability and commutability are affected. Consider potential evacuation. For example, bomb threats, fires, terrorist attacks, are potential catalysts for evacuation.

2.Lighting

Proper lighting, especially for organizations with 24×7 operations, should be evaluated.

Mirrored windows or windows with highly reflective coatings should face north-south rather than east-west to avoid casting sun glare into trafficked areas. Lighting should be positioned in such a way that it never blinds those leaving the building at night.

Proximity to Other Buildings

Know who your neighbors are. For instance, sharing a building with a branch of law enforcement would be considered less of a risk than sharing a building with Unknown person." The closer the proximity to other buildings and companies, the higher the probability is for a physical security incident to occur.

Proximity to Law Enforcement and Emergency Response

If the area has a history of crime, you've chosen the site, consider the possibility that the incident may not get a response within a framework that you consider ideal. Similarly, if an emergency service unit were to be called to respond to an incident at this location, consider what the impact would be for any delay.

RF and Wireless Transmission Interception

As wireless networking becomes more dominant, wireless hacking and hijacking become more of a threat. "airborne" protocols that should be taken into consideration include radio frequency devices, cordless phones, cell phones, Mobile e-mail devices.

Utilities Reliability

Office buildings provide work space for employees who need to be productive and reliable in their work. Power outages can seriously interfere with productivity, as can phone service and network outages. UPS batteries only last for a short time, and generator fuel can be expensive and difficult to get in a serious emergency. For a data center, loss of power can have a serious impact.

Construction and Excavation

Construction and excavation can entire network and communications infrastructure down. Town or city records will usually provide the information regarding construction/excavation/ demolition, both past and present.

Q5f. Explain the different factors for securing the assets with physical security devices.
Securing Assets: Locks and Entry Controls

Many different factors you should consider when securing the assets with physical security devices. Lock Controls are:

1.Locks

Anything of value that is capable of "growing should have a lock or to be secured in a location that has a lock. smartphones, tablets, MP3 players, jewellery, keys, and other assorted items. Lock up the device or valuable and educate the asset owner on the importance of securing the item.

2.Doors and File Cabinets

Check for locked doors where applicable. Make sure the lock on the door functions correctly and can withstand sufficient force. File cabinets containing sensitive information or valuable equipment should be kept locked when not in use. The keys to these should also be kept out of common reach.

3.Data Centers and Network Rooms

Make sure these rooms are kept locked. If automatic entry-tracking mechanisms are not in use, ensure an access log is kept.

4.Laptops

Laptops at the office, when not in transport, should be physically locked to the desk. Cable locks are a relatively small price to pay to ensure the laptop (and confidential information) doesn't fall into the wrong hands. All personnel should be instructed to be worried when traveling with a laptop. Operating system security and software safeguards are only as good as the physical security protecting access to the device.

Entry Controls

Entry controls have their own security considerations that will vary with security plan and business needs. first consider the site in which the entry controls will be deployed.

1.Building Access Control Systems

Multitenant buildings typically have access control systems that control entrance into the building or entrance to a special parking lot that is common to the entire building.dealing with a multitenant building is to make sure that you never have to allow anyone from the unsecured side to pass into the secured side unless they are authorized to do so.

2.Mantraps

A *mantrap* is an area designed to allow only one authorized individual entrance at any given time.These are typically used as an *antitailgating* mechanism—to prevent an unauthorized person from closely following an authorized person through an open door.

3.Building an Employee IDs

One first things any organization does after hiring new employees is to provide them with ID badges. Building and/or employee identification should be displayed at all times, and anyone who lacks a visible ID should be challenged.

4.Biometrics

A *biometric device* is classified as any device that uses distinctive personally identifiable characteristics or unique physical traits to positively identify an individual. common devices use one or more of the following characteristics or traits to confirm identification: fingerprint, voice, face, retina, iris, handwriting, and hand geometry.

5. Security Guards

A security guard is employed by an organization, company, preserve, protect, support, and maintain the security and safety of personnel and property. Security guards detect, and report infractions of organizational rules, policies, and procedures.

-----------------------------x---------------------------