B.Sc.(Information Technology)

(Semester VI ATKT)

04th December 2019

Security in Computing

(USIT 602 Core)

University Paper Solution

By

Ms. Geeta Sahu

Question 1

Q1a. Explain three D's of Security.

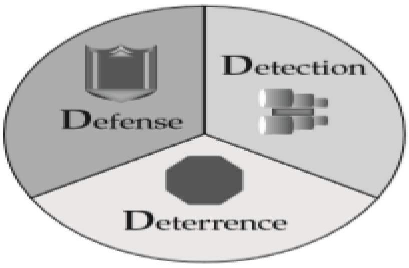
Ans: **Three Ds of security:** Defense, Detection, and Deterrence.

Defensive controls on the network can include access control devices such as stateful firewalls, network access control, spam and malware filtering, web content filtering, and change control processes. These controls provide protection from software vulnerabilities, bugs, attack scripts, ethical and policy violations, accidental data damage, and the like.

Detective controls include video surveillance cameras in local stores, motion sensors, and house or car alarm systems that alert passers-by of an attempted violation of a security perimeter. Detective controls on the network include audit trails and log files, system and network intrusion detection and prevention systems and security information and event management (SIEM) alerts, reports, and dashboards.

Deterrence is another aspect of security. It is considered to be an effective method of reducing the frequency of security compromises, and thereby the total loss due to security incidents. Many companies implement deterrent controls for their own employees, using threats of discipline and termination for violations of policy.

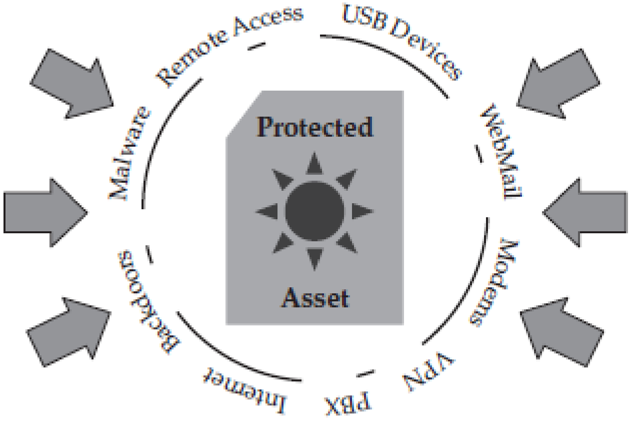
These deterrent controls include communication programs to employees about acceptable usage and security policies, monitoring of web browsing behavior, training programs to acquaint employees with acceptable usage of company computer systems.



Q1b. Explain the statement that "Achieving 100 percent protection against all conceivable attacks is an impossible job.".

Ans: **The Impossible Job**

- The job of the attacker is always easier than the job of the defender.
- The attacker needs only to find one weakness, while the defender must try to cover all possible vulnerabilities.
- The attacker has no rules—the attacker can follow unusual paths, abuse the trust of the system, or resort to destructive practices.
- The defender must try to keep their assets intact, minimize damage, and keep costs down.
- Eg : Homeowners who want to protect their property must try to anticipate every attack that is likely to happen, while attackers can simply use, bend, break, or mutilate the house's defenses.
- In an extreme example, the attacker can cut through the exterior, break the windows, knock down the walls, or set the house on fire. Homeowners have the more difficult job, trying to protect their assets against all types of attack.
- Every defender performs a risk assessment by choosing which threats to defend against, which to insure against, and which to ignore.
- *Mitigation* is the process of defense, *transference* is the process of insurance, and *acceptance* is deciding that the risk does not require any action.



Q 1c. Write a note on Threat Vector.
Ans: Threat Vectors

A *threat vector* is a term used to describe where a threat originates and the path it takes to reach a target. An example of a threat vector is an e-mail message sent from outside the organization to an inside employee, containing an irresistible subject line along with an executable attachment that happens to be a Trojan program, which will compromise the recipient's computer if opened.

- **Trojan** programs are installed pieces of software that perform functions with the privileges of authorized users, but unknown to those users.
- Common functions of Trojans include stealing data and passwords, providing remote access and/or monitoring to someone outside the trusted network, or performing specific functions such as spamming.
- Trojans can be exploited over the Internet, through the firewall, or across the internal network by users who are not authorized to have access. Trojans are dangerous because they can hide themselves in authorized communication channels such as web browsing.
- **Viruses** typically arrive in documents, executable files, and e-mail. They may include Trojan components that allow direct outside access, or they may automatically send private information, such as IP addresses, personal information, and system configurations, to a receiver on the Internet. These viruses usually capture and send password keystrokes as well.
- A further example is the ***girlfriend exploit***. It refers to a Trojan program planted by an unsuspecting employee who runs a program provided by a trusted friend from a storage device like a disk or USB stick, that plants a *back door* (also known as *trap door*) inside the network.

Q1d. What are Application Layer Attacks? Explain the following Application Layer attacks i) Buffer Overflows ii) Password cracking

Ans: **Application-Layer Attacks**: Application-layer attacks include any exploit directed at the applications running on top of the OSI protocol stack. Application-layer attacks include exploits directed at application programs, as well as against operating systems. Application-layer attacks include content attacks, buffer overflows, and password-cracking attempts.

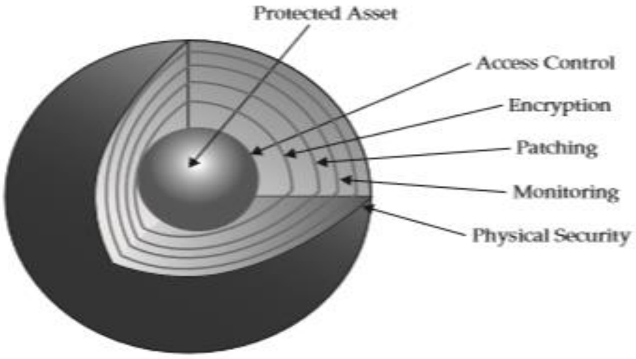
Buffer Overflows
Buffer overflows occur when a program expecting input does not do input validation
Password Cracking Password crackers either try to guess passwords or they use brute-force tools. *Brute-force* tools attempt to guess a password by trying all the character combinations listed in an accompanying *dictionary*. The dictionary may start off blindly guessing passwords using a simple incremental algorithm. (for example, trying aaaaa, aaaab, aaaac, and so on) or it may use passwords known to be common on the host (such as password, blank, michael, and so on).

Q1e. Explain the Onion model.

Ans: **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. List and explain the steps to create a Security Defence Plan.

Ans: **These are the steps to creating a plan:**

1. Inventory the assets you have to protect.

2. Decide the value of each asset and its chance of being exploited in order to come up with a quantifiable exposure risk.

3Develop a plan to tighten the security on your protected assets. Assets with the highest exposure risk should be given the most protection, but make sure all assets get some baseline level of security.

4. Develop and document security baseline tools and methods. For example, develop an acceptable security template for end-user workstations. Document a method for

applying security templates to those workstations (probably a group policy), and put policies and procedures in force to make sure each workstation gets configured with a security template.

5. Use vulnerability testing tools to confirm assets have been appropriately configured.

6. Do periodic testing to make sure security settings stay implemented.

7. Change and update the plan as dictated by new security events and risks.

Question 2

Q2a. Explain certificate based authentication in details.

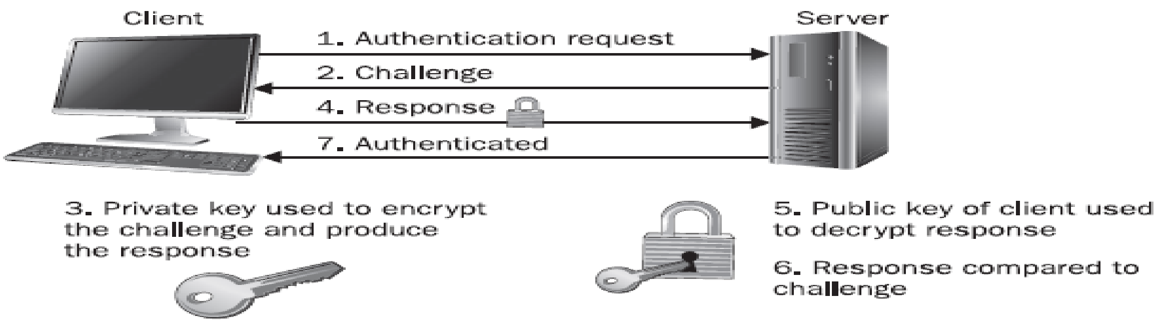
Ans: Certificate-Based Authentication

- *A certificate is a collection of information that binds an identity (user, computer, service, or device) to the public key of a public/private key pair. The typical certificate includes information about the identity and specifies the purposes for which the certificate may be used, a serial number, and a location.*
- *The certificate is digitally signed by the issuing authority, the certificate authority (CA). The infrastructure used to support certificates in an organization is called the Public Key Infrastructure (PKI).*
- *Certificate can be exchanged in e-mail, distributed as part of some application's initialization, or stored in a central database where those who need a copy can retrieve one. Each certificate's public key has its associated private key, which is kept secret.*
- *It uses public/private key algorithms use two keys: one key is used to encrypt, the other to decrypt. If the public key encrypts, only the related private key can decrypt. If the private key encrypts, only the related public key can decrypt.*
- *When certificates are used for authentication, the private key is used to encrypt or digitally sign some request. The related public key (available from the certificate) can be used by the server to decrypt the request.*

If the result matches, then proof of identity is obtained.

The Ce**rtificate-Based Authentication steps are as follows:**

1. The client issues an authentication request.
2. A challenge is issued by the server.
3. The client/workstation uses its private key to encrypt the challenge.
4. The response is returned to the server.
5. Since the server has a copy of the certificate, it can use the public key to decrypt the response.
6. The result is compared to the challenge.
7. If there is a match, the client is authenticated.


Client
Server
1. Authentication request
2. Challenge
4. Response
7. Authenticated
3. Private key used to encrypt the challenge and produce the response
5. Public key of client used to decrypt response
6. Response compared to challenge

Certificate authentication uses public and private keys.

Q2b. Write a note on Role-based Authorization (RBAC)

Ans: **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.

File-Access Permissions

- Both Windows and Unix systems use file permissions to manage access to files. It is only when you require interoperability that problems arise in ensuring that proper authorization is maintained across platforms.

Windows File-Access Permissions

- The Windows file system maintains an ACL for each file and folder. The ACL is composed of a list of access control entries (ACEs). Each ACE includes a security identifier (SID) and the permission(s) granted to that SID.
- Permissions may be either *access* or *deny*, and SIDs may represent user accounts, computer accounts, or groups.
- Part of the login process is the determination of the privileges and group memberships for the specific user or computer. A list is composed that includes the user's SID, the SIDs of the groups of which the user is a member, and the privileges the user has.
- When a connection to a computer is made, an access token is created for the user and attached to any running processes the user may start on that system.

ACLs for Network Devices

- ACLs are used by network devices to control access to networks and to control the type of access granted. Specifically, routers and firewalls may have lists of access controls that specify which ports on which computers can be accessed by incoming communications, or which types of traffic can be accepted by the device and routed to an alternative network.

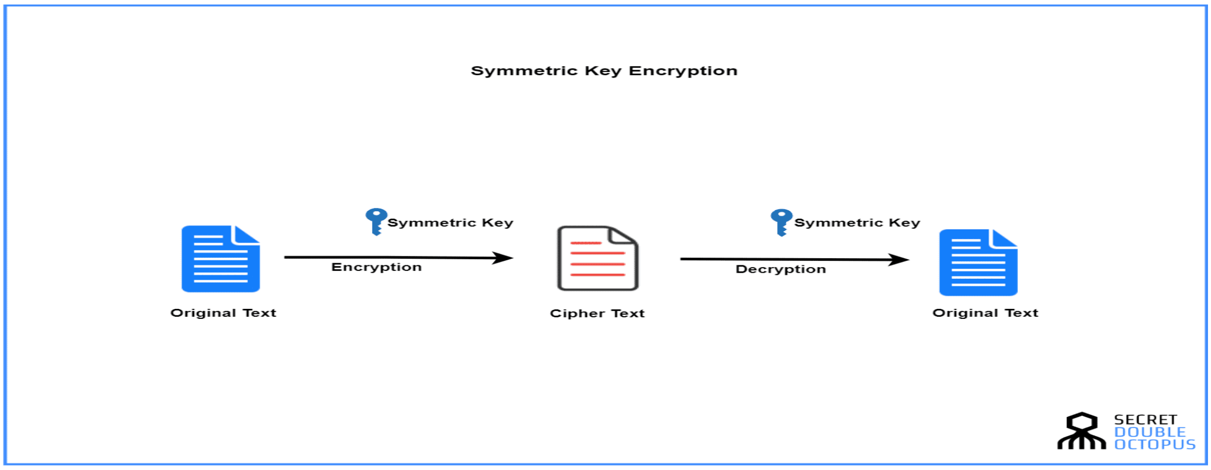
Q2c. Write a note on symmetric key cryptography.

Ans: Symmetric key cryptography is any cryptographic algorithm that is based on a shared key that is used to encrypt or decrypt text/cypher text, in contract to asymmetric key cryptography, where the encryption and decryption keys are different.

Symmetric encryption is generally more efficient than asymmetric encryption and therefore preferred when large amounts of data need to be exchanged.

Establishing the shared key is difficult using only symmetric encryption algorithms, so in many cases, an asymmetric encryption is used to establish the shared key between two parties.

Examples for symmetric key cryptography include AES, DES, and 3DES. Key exchange protocols used to establish a shared encryption key include Diffie-Hellman (DH), elliptic curve (EC) and RSA.



Symmetric-key encryption can use either stream ciphers or block ciphers.[5]

- Stream ciphers encrypt the digits (typically bytes), or letters (in substitution ciphers) of a message one at a time. An example is the Vigenere Cipher.
- Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size. Blocks of 64 bits were commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001, and the GCM block cipher mode of operation use 128-bit blocks.

Q2d. *Explain any two confidentiality risks.*

Ans: Confidentiality Risks

- Confidentiality risks are associated with vulnerabilities and threats pertaining to the privacy and control of information, given that we want to make the information available in a controlled fashion to those who need it, without exposing it to unauthorized parties.

1.Data Leakage, Theft, Exposure, Forwarding

- Data leakage is the risk of loss of information, such as confidential data and intellectual property.
- There are four major threat vectors for data leakage: theft by outsiders, malicious sabotage by insiders (including unauthorized data printing, copying, or forwarding), misuse by authorized users, and mistakes created by unclear policies.

Defense

- Employ software controls to block inappropriate data access using a data loss prevention (DLP) solution or an information rights management (IRM) solution,

Detection

- Use watermarking and data classification labelling along with monitoring software to track data flow.

Deterrence

- Establish security policies that assign serious consequences to employees who leak data, and include clear language in contracts with service providers specifying how data privacy is to be protected and maintained, and what the penalties are for failure to protect and maintain it.

Residual risks

- Data persistence within the storage environment can expose data long after it is no longer needed, especially if the storage is hosted on a vendor provided service that dynamically moves data around in an untraceable manner.

2.Espionage, Packet Sniffing, Packet Replay

- *Espionage* refers to the unauthorized interception of network traffic for the purpose of gaining information intentionally using tools to capture network packets is called *packet sniffing*, and using tools to reproduce traffic and data that was previously sent on a network is called *packet replay*.
- **Defense**

Encrypt data at rest as well as in transit through the use of modern, robust encryption technologies for file encryption, as well as network encryption between servers and over the Internet.

- **Detection**

An information rights management (IRM) solution can keep track of data access, which can provide the ability to detect inappropriate access attempts.

- **Deterrence**

In storage environments that are hosted by a third party, employ contract language that makes the service provider liable for damages resulting from unauthorized access.

- **Residual risk**

Data can be stolen from the network through tools that take advantage of network topologies, network weaknesses, compromised servers and network equipment, and direct access to network devices.

Q2e. ***Write a note on object-level security.***

Ans: 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.

- 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.

Using Other Database Objects for Security

- The three commonly used database objects and how they can be used to better manage security settings are:
- **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.

- For example, you can create a view that shows basic information about employees but excludes sensitive data like their salaries and Social Security numbers.
- Once a view has been defined, we can assign object-level permissions to the view. Users of the database can then use the view to access whatever information they require.
- **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.
- **Triggers -**Triggers are designed to automatically be "fired" whenever specification actions take place within a database. For example, you might create a trigger on the SalesOrder table that will automatically create a corresponding row in the Invoice table.
- Triggers can be used in different ways. It can use triggers to perform detailed auditing. For example, whenever a change is made to certain information in an EmployeeSalary table, you might want to notify a high-level manager, or you might write a row logging this action to another table.

Q2 f. Explain different types of database backups.

Ans: **Database Backup and Recovery**

- Systems administrators perform backups to protect information in the case of server hardware failures. Data can be lost due to accidental human errors, faulty application logic, defects in the database or operating system platform and malicious users who are able to avoid security measures.

Types of Database Backups

The following types of backups are possible on most systems:

- **Full backups** This type of backup consists of making a complete copy of all of the data in a database. The process can be performed while a database is up and running.
- Database administrators test the performance impact of backups before implementing an overall schedule.
- Disk space it is recommended to perform full backups frequently.
- **Differential backups** This type of backup consists of copying all the data that has changed since the last full backup. Since differential backups contain only changes, the recovery process involves first restoring the latest full backup and then restoring the latest differential backup. The use of differential backups can greatly reduce the amount of disk storage space and backup time required to protect large databases.

Transaction log backups

- Relational database systems are designed to support multiple concurrent updates to data.
- To ensure that all users see data that is consistent to a specific point in time, data modifications are first written to a transaction log file.
- Periodically, the transactions that have been logged are then committed to the actual database
- Database administrators can choose to perform transaction log backups frequently, since they only contain information about transactions that have occurred since the last backup.

Question 3

Q3a: Write a note on outbound filtering.

Ans: **Outbound Filtering**

- Failure to restrict outbound access creates a number of risks to the corporation and its infrastructure.
- Failure to filter traffic leaving the corporate network may allow an attacker to use the network to launch attacks on other networks.
- There is a liability for organizations that don't properly control their outbound network traffic.

Outbound Port Filtering

- To filter outbound traffic is to ensure that only authorized traffic traverses controlled links.
- To restrict outbound access, it is necessary to implement outbound filters on perimeter firewalls. As with inbound access, restrictive filters will limit which services can be used by default.
- This will also require security administrators to relax filters as new applications are deployed and business requirements demand access to new services.
- By limiting outbound traffic to authorized applications, outbound filtering will prevent users from using applications that are dangerous in the corporate environment.
- It can also reduce the chance that the organization network can be used to launch an attack against another network—such an attack could damage or cause loss for its victim.
- It is expensive and time consuming to build a defense, and it can focus negative publicity on the organization's security practices. It is necessary to block unneeded access at the corporate perimeter.

Q3b. Explain the role of hubs and switches in network.

Ans: **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.
- 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.
- As more devices are attached to the same hub, and more hubs are interconnected, the chance that two nodes transmit at the same time increases, and collisions became more frequent.
- In addition, as the size of the network increases, the distance and time a packet is in transit over the network also increases, making collisions even more likely. Thus, it is necessary to keep the size of such networks very small to achieve acceptable levels of performance.

Switches

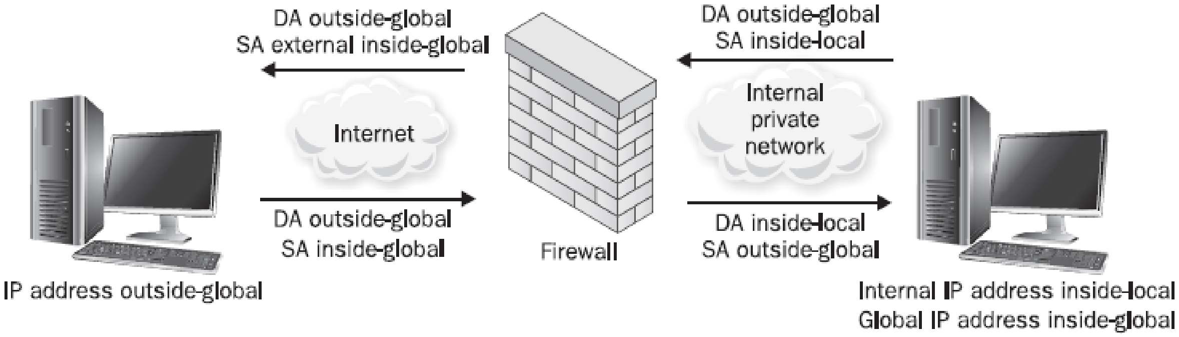
- Switches are layer two devices and routers are layer three devices. They are more intelligent devices that learn the various MAC addresses of connected devices and transmit packets only to the devices they are specifically addressed to.
- Since each packet is not rebroadcast to every connected device, 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*.
- ARP poisoning works by forging replies to ARP broadcasts. For example, suppose malicious workstation Attacker wishes to monitor the traffic of workstation Victim, another host on the local switched network segment. To accomplish this, Attacker would broadcast an ARP packet onto the network containing Victim's IP address but Attacker's MAC address.

Q3c. Explain in detail Network Address Translation (NAT).

Ans: **Network Address Translation (NAT)**

- In order to conserve IPv4 addresses, specified blocks of addresses will never be used on the Internet. These network are referred to as "private" networks.
- This allows organizations to use these blocks for their own corporate networks. when these networks are connected to the Internet, they must translate their private IP network addresses into public IP addresses (NAT) in order to be routable.
- By doing this, a large number of hosts behind a firewall can take turns or share a few public addresses when accessing the Internet.
- NAT is usually implemented in a firewall separately from the policy or rule set. NAT has been defined to translate addresses between one host and another, it does not mean those hosts will be able to communicate. This is controlled by the policy defined in the firewall rule set.
- When hosts have both public and private IP addresses, the IP information contained within a packet header will change depending on where the packet is viewed. the addresses when viewed on the trusted side of the firewall will be referred to as *local addresses*.
- Once the packet crosses the firewall and is translated, the addresses will be called the host's *global addresses*. DA" and "SA" refer to "destination address" and "source address" respectively.



Static NAT

- A static NAT configuration always results in the same address translation. The host is defined with one local address and a corresponding global address in a 1:1 relationship, and they don't change.
- The static NAT translation rewrites the source and destination IP addresses as required for each packet as it travels through the firewall. No other part of the packet is affected.

Dynamic NAT

- Dynamic NAT is used to map a group of inside local addresses to one or more global addresses. The global address set is usually smaller than the number of inside local addresses, and the conservation of addresses is accomplished by overlapping this address space.

Q3d. Explain strengths and weakness of a firewall.

Ans: Firewall Strengths

- *Firewalls are excellent at enforcing security policies. They should be configured to restrict communications to what management has determined and agreed with the business to be acceptable.*
- *Firewalls are used to restrict access to specific services.*
- *Firewalls are transparent on the network—no software is needed on end-user workstations.*
- *Firewalls can provide auditing. Given plenty of disk space or remote logging capabilities, they can log interesting traffic that passes through them.*
- *Firewalls can alert appropriate people of specified events.*

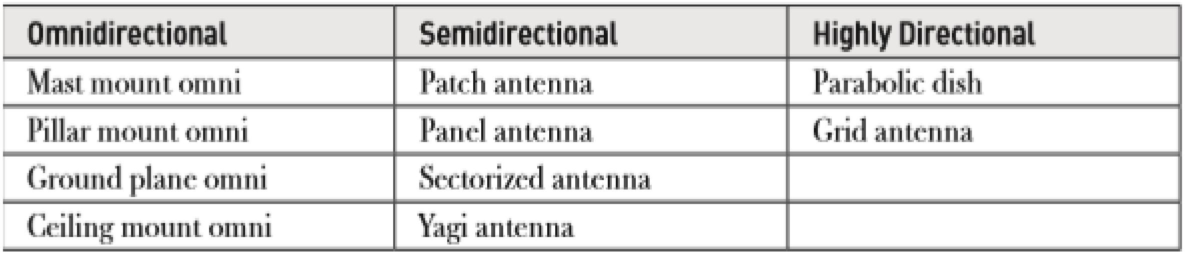
Firewall Weaknesses

- *Firewalls are only as effective as the rules they are configured to enforce. An overly permissive rule set will diminish the effectiveness of the firewall.*
- *Firewalls cannot stop social engineering attacks or an authorized user intentionally using their access for malicious purposes.*
- *Firewalls cannot enforce security policies that are absent or undefined.*
- *Firewalls cannot stop attacks if the traffic does not pass through them.*

Q3e. Explain the importance of antenna choice and positioning.

***Ans:* Importance of Antenna Choice and Positioning**

- A radio frequency signal is a high-frequency alternating current (AC) passed along the conductor and radiated into the air via an antenna. The emitted waves propagate away from the antenna in a straight line and form RF beams or lobes, which are dependent on antenna horizontal and vertical beam-width values. There are three generic types of antennas, which can be further divided into subtypes:



Omnidirectional	Semidirectional	Highly Directional
Mast mount omni	Patch antenna	Parabolic dish
Pillar mount omni	Panel antenna	Grid antenna
Ground plane omni	Sectorized antenna	
Ceiling mount omni	Yagi antenna	

- Antennas can increase the range of your wireless signal, and capture higher volumes of data.
- When choosing necessary antennas, consider antenna irradiation patterns. Get it right, and the coverage is exactly where you need it.
- Omni directional antennas are typically used in point-to-multipoint wireless network topologies, semi directional antennas.
- Yagi antennas, are directional antennas composed of a dipole and reflector.
- Yagis form a narrower "extended bubble" with side and back lobes. Highly directional antennas irradiate a narrowing cone beam, which can reach as far as the visible horizon. Horizontal and vertical planes of semi- and highly directional antennas are often similar in shape but have different beam widths.

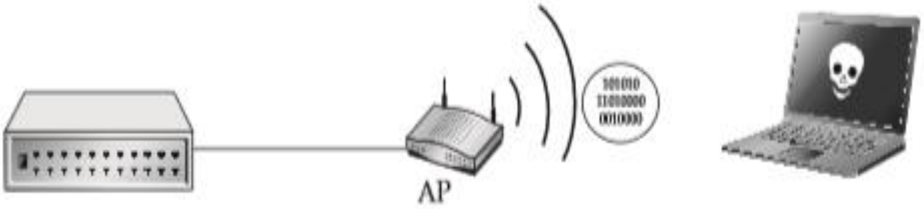
Q3f. Explain any two types of wireless attacks.

Ans: Two types of wireless attacks are:

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.

Question 4

Q4a. Explain network-based intrusion detection system in detail.

Ans: **Network-Based IDS (NIDS)** -are the most popular IDSs, and they work by capturing and analysing 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.
- NIDSs must have promiscuous network cards with packet-level drivers, and they must be installed on each monitored network segment. Network taps, a dedicated appliance used to mirror a port and Switch Port Analysis (SPAN), are the two most common methods for setting up monitoring on a switched network.
- **Packet-Level Drivers** Network packets are captured using a packet-level software driver bound to a network interface card.

Promiscuous Mode

- For a NIDS to sniff packets, the packets have to be given to the packet-level driver by the network interface card. most network cards are not promiscuous, meaning they only read packets that are intended for them.

- This typically includes unicast packets, meant for one particular workstation, broadcast packets, meant for every computer that can listen to them, and multicast traffic, meant for two or more previously defined hosts.
- Most networks contain unicast and broadcast traffic. Multicast traffic isn't as common, but it is gaining in popularity for web-streaming applications. a network card in normal mode drops traffic destined for other computers and packets with transmission anomalies.

Q4b. List and explain steps to a successful IPS Deployment Plan.

Ans: **IPS Deployment Plan** the steps to a successful IPS deployment are:
1. Document your environment's security policy.
2. Define human roles.
3. Decide the physical location of the IPS and sensors.
4. Configure the IPS sensors and management console to support your security policy.
5. Plan and configure device management (including the update policy).
6. Review and customize your detection mechanisms.
7. Plan and configure any prevention mechanisms.
8. Plan and configure your logging, alerting, and reporting.
9. Deploy the sensors and console (do not encrypt communication between sensors
and links to lessen troubleshooting).
10. Test the deployment using IPS testing tools (initially use very broad rules to make
sure the sensors are working).
11. Encrypt communications between the sensors and console.
12. Test the IPS setup with actual rules.
13. Analyze the results and troubleshoot any deficiencies.
14. Fine-tune the sensors, console, logging, alerting, and reporting.
15. Implement the IPS system in the live environment in monitor-only mode.
16. Validate alerts generated from the IPS.
17. One at a time, set blocking rules for known reliable alerts that are important in
your environment.
18. Continue adding blocking rules over time as your confidence in each rule increases.
19. Define continuing education plans for the IPS administrator.
20. Repeat these steps as necessary over the life of the IPS.

Q4 c. Write a note on H.323 protocol that includes:

- ***i) Governing Standard***
- ***ii) Purpose***
- ***iii) Function***
- ***iv) Known Compromises and Vulnerabilities***
- ***v) Recommendations***

Ans: **Protocol: H.323**

Governing Standard

- It is a component of the "H-series" for Audio-visual and Multimedia Systems specifically addressing systems and terminal equipment for audio-visual services.

Purpose

- Standardized approach for terminals and other entities that provide multimedia communications services over packet-based networks that may not provide a guaranteed quality of service. Audio support is mandatory, but entities may support real-time video and/ or data communications as well. If video and data are supported, the ability to use a common mode of operation is required, so that all terminals supporting the media type can interact.
- H.323 has dozens of sub protocols, including a specific security sub protocol, H.235

Function

H.323 entities may be integrated into PCs or implemented in standalone devices and support many types of networks and internetworking, including point-to-point, multipoint, broadcast, or multi-access networks. B-ISDN, N-ISDN, guaranteed quality-of-service LANs, GSTN, and

Known Compromises and Vulnerabilitieswireless networks, and other specific types of terminals and networks through the use of vulnerabilities are -DoS, DDoS, flooding, Gateway compromises Remote code execution and arbitrary code execution.

Recommendations the capability to communicate via this protocol suite over your network is disabled by default. Many devices are shipped with these protocols enabled.

Q4d. What is Private Branch Exchange (PBX)? How will you secure PBX?

Ans: **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:
  1. Multiple extensions
  2. Voicemail
  3. Call forwarding
  4. Fax management
  5. Remote control (for support)

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.
- Disable all through-dialing features.
- If you require dial through, limit it to a set of predefined needed numbers.
- Block all international calls, or limit the number of users who can initiate them.
- Block international calls to places such as the Caribbean that fraudsters tend to call.
- Train your help desk staff to identify attempted PBX hacks, such as excessive hang-ups, wrong number calls, and locked-out mailboxes.
- Make sure your PBX model is immune to common DoS attacks.

Q4 e. Write a note on Access Control List (ACL)

Ans : Access Control Lists

- An access control list is defined as a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or an individual file.

- The list has an entry for each system user with access privileges. The common privileges include the ability to read a file, to write the file, and to execute the file.

- The user can also be a role name, such as *programmer* or *tester*. For each of these users, groups, or roles, the access privileges are stated in a string of bits called an *access mask*.

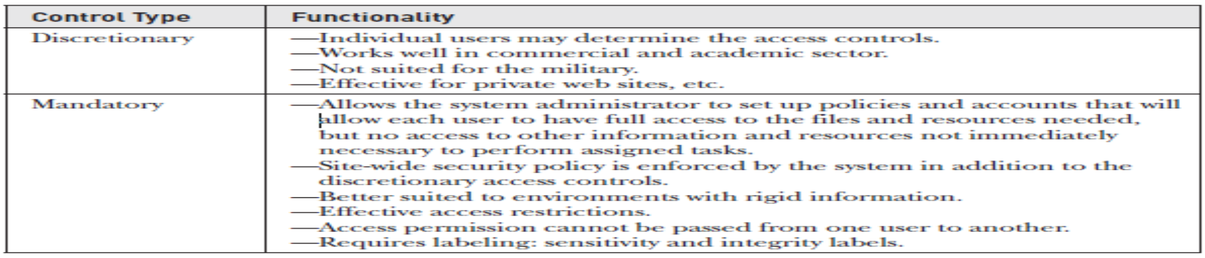
An object's security descriptor can contain two ACLs: A *discretionary* access control list (DACL) that identifies the users and groups who are allowed or denied access. A *system* access control list (SACL) that controls how access is audited.

MAC(Mandatory access control) vs. DAC (discretionary access control)

- DAC provides an entity or object with access privileges it can pass to other entities. Depending on the context in which they are used, these controls are also called rule-based access control (RBAC) and identity-based access control (IBAC). Solaris, Windows uses DAC.

- *Mandatory access control* requires that access control policy decisions beyond the control of the individual owners of an object. MAC is generally used in systems that require a very high level of security.

- With MAC, only the administrator and *not* the owner of the resource may make decisions derive from the security policy. Only a security administrator may change a resource's category, and no one may grant a right of access that is explicitly forbidden in the access control policy. MAC is always prohibitive and not permissive. MAC is implemented in TrustedBSD and Trusted Solaris.



Control Type	Functionality
Discretionary	—Individual users may determine the access controls. —Works well in commercial and academic sector. —Not suited for the military. —Effective for private web sites, etc.
Mandatory	—Allows the system administrator to set up policies and accounts that will allow each user to have full access to the files and resources needed, but no access to other information and resources not immediately necessary to perform assigned tasks. —Site-wide security policy is enforced by the system in addition to the discretionary access controls. —Better suited to environments with rigid information. —Effective access restrictions. —Access permission cannot be passed from one user to another. —Requires labeling: sensitivity and integrity labels.

Q4f. Explain the reference monitor concept and windows security reference monitor.

Ans: Reference Monitor

- *The reference monitor concept as an object that maintains the access control policy. It does not actually change the access control information; it only provides information about the policy.*

- *The security reference monitor is a separable module that has access control decisions and security processes for the operating system. All security operations are routed through the reference monitor, which decides if the specific operation should be permitted or denied.*

- *The main elements of an effective reference monitor are:*

- *Always on Security must be implemented consistently and at all times for the entire system and for every file and object.*
- *Not subject to pre-emption Nothing should be able to pre-empt the reference monitor. If this were not the case, then it would be possible for an entity to bypass the mechanism and violate the policy that must be enforced.*
- *Tamperproof It must be impossible for an attacker to attack the access mediation mechanism such that the required access checks are not performed and authorizations not enforced.*

- *Lightweight It must be small enough to be subject to analysis and tests, proving its effectiveness.*

Question 5

Q5 a. Explain how to protect the Guest OS, Virtual Storage and Virtual Networks in Virtual machines.

Ans: 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 neighbouring 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 all of the hypervisor's guest OSs.*
- *The hypervisor monitors and tracks the state of its guest OSs, which is a function commonly referred to as introspection.*

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.*
- *This aspect of security for virtualization is focused on controlling access to the files on the virtual hard drive and the overall configuration of the storage network.*

Protecting Virtual Networks

- *The hypervisor can present the guest OS with either physical or virtual network interfaces. hypervisors provide three choices for network configurations:*
- *Network bridging- The guest OS has direct access to the actual physical network interface cards (NIC) of the real server hardware.*

Q5 b. State and explain the types of cloud services.

***Ans:* 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.
- **Service commerce platforms -** It is a service hub that users interact with, such as an expense management system, to order travel or secretarial services from a common platform that then coordinates the service delivery and pricing within the specifications set by the user.
- **Internet integration –**It is serving SaaS providers using in-the-cloud integration technology.

Q5c. Explain various Application Security Practices.

Ans: **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 modelling 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.

Q5d. Write a note on Custom Remote Administration.

Ans: Custom Remote Administration

- *Some applications are controlled remotely via a GUI or through console applications, such as SQL Server, Exchange Server, firewalls, and intrusion detection systems (IDSs).*

Advantages and Disadvantages

These are the advantages of custom remote administration:

- ***Complex graphics***

Sometimes the console needs to display complex graphics that can't be shown using a regular web administration interface.

- ***Authentication and encryption***

The application may use either a stronger authentication method or a stronger encryption method to secure the session

- ***Availability***

Since the application can only be controlled from a dedicated GUI, the attacker will need to install it at his computer.

- ***Specific OS***

Some vendors will require a specific OS to run the controlling GUI, and the administrator will have to install it if it isn't already installed.

- ***Session Security***

It's important that the session between the client and the application be secure. Otherwise, attackers may be able to gain information, steal credentials, or even conduct a replay attack. If the session is known to be insecure, the administrator can easily relay it through a VPN or a secure tunnel (SSH).

- ***Unavailability***

The application can be administered only from computers on which the GUI is installed, and if the administrator is not in the office, it may not be possible to administer it from other computers.

Q5e. Explain the classification of Corporate Physical Assets.

***Ans:* The classification of corporate physical assets under the categories are:**

- Computer equipment Servers, network-attached storage (NAS) and storage area networks (SANs), desktops, laptops, tablets, pads, etc.
- Communications equipment Routers, switches, firewalls, modems, private branch exchanges (PBXs), fax machines, etc.
- Technical equipment Power supplies, uninterruptable power supplies (UPSs), power
- conditioners, air conditioners, etc.
- Storage media storage media devices like magnetic tapes, DATs, CD-ROMs, and Zip drives. Use of hard drive arrays, solid-state drives or thumb drives, and the various types of memory cards such as Secure Digital (SD), microSD, Compact Flash, and Memory Stick.
- Furniture and fixtures Racks, etc.
- Assets with direct monetary value Cash, jewellery, bonds, stocks, credit cards, personal data, cell phones, etc.

Q5f. Explain Lock and Entry Controls that should be considered while securing assets with physical security devices.

Ans: 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 Centres 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.
- The elevator should also exit into this public space. This ensures that the public, andother tenants, will not have to enter to get to another part of the building

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 *ant tailgating* 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.
- An individual becomes friendly with the security guard and, eventually, the guard just waves them through without showing valid identification. This situation has many security implications associated with it.

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.
- For entry control, deployed biometric technologies are currently fingerprint and hand geometry devices. The latest fingerprint readers now read the corpuscles under the skin, so they can be used for everyone, even individuals who do not have strong fingerprint ridges.

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.
- Security guards help limit or prevent unauthorized activities.
- Background checks should be done for all security guards, and appropriate licenses and clearances obtained wherever applicable.

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