

Security+ cram notes (SY0-301)

1. Network Security
 - 1.1 Explain the security function and purpose of network devices and technologies
 - 1.2 Apply and implement secure network administration principles
 - 1.3 Distinguish and differentiate network design elements and compounds
 - 1.4 Implement and use common protocols
 - 1.5 Identify commonly used default network ports
 - 1.6 Implement wireless network in a secure manner

2. Compliance and Operational Security
 - 2.1 Explain risk related concepts
 - 2.2 Carry out appropriate risk mitigation strategies
 - 2.3 Execute appropriate incident response procedures
 - 2.4 Explain the importance of security related awareness and training
 - 2.5 Compare and contrast aspects of business continuity
 - 2.6 Explain the impact and proper use of environmental controls
 - 2.7 Execute disaster recovery plans and procedures
 - 2.8 Exemplify the concepts of confidentiality, integrity and availability (CIA)

3. Threats and Vulnerabilities
 - 3.1 Exemplify the concepts of confidentiality, integrity and availability (CIA)
 - 3.2 Analyze and differentiate among types of attacks
 - 3.3 Analyze and differentiate among types of social engineering attacks
 - 3.4 Analyze and differentiate among types of wireless attacks
 - 3.5 Analyze and differentiate among types of application attacks
 - 3.6 Analyze and differentiate among types of mitigation and deterrent techniques
 - 3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities
 - 3.8 Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning

4. [Application, Data and Host Security](#)
 - 4.1 [Explain the importance of application security](#)
 - 4.2 [Carry out appropriate procedures to establish host security](#)
 - 4.3 [Explain the importance of data security](#)

5. [Access Control and Identity Management](#)
 - 5.1 [Explain the function and purpose of authentication services](#)
 - 5.2 [Explain the fundamental concepts and best practices related to authentication, authorization and access control](#)
 - 5.3 [Implement appropriate security controls when performing account management](#)

6. [Cryptography](#)
 - 6.1 [Summarize general cryptography concepts](#)
 - 6.2 [Use and apply appropriate cryptographic tools and products](#)
 - 6.3 [Explain the core concepts of public key infrastructure](#)
 - 6.4 [Implement PKI, certificate management and associated components](#)

1. Network Security

1.1 Explain the security function and purpose of network devices and technologies

Firewalls

1. Firewalls protect against and filter out unwanted traffic. A firewall can be an individual device or can be added to a router. For example, most SOHO routers have a firewall built in, and Cisco Integrated Services Routers include the Cisco IOS Firewall. Regular routers, and routers with firewall functionality, have the ability to block certain kinds of traffic. For example, if the ICMP protocol has been blocked, then you would not be able to ping the router.
2. A personal firewall is software that resides on the end users computers. This is different from a regular firewall, in the sense that a personal firewall is geared to protect a single user computer.
3. The following are the basic types of firewall architectures:
 - Bastion host
 - Screened host gateway
 - Screened subnet gateway or DMZ

Hub

A hub is basically a multi-port repeater. When it receives a packet, it repeats that packet out each port. This means that all computers that are connected to the hub receive the packet whether it is intended for them or not. It's then up to the computer to ignore the packet if it's not addressed to it. This might not seem like a big deal, but imagine transferring a 50 MB file across a hub. Every computer connected to the hub gets sent that entire file (in essence) and has to ignore it.

Bridge

A bridge is a kind of repeater, but it has some intelligence. It learns the layer 2 (MAC) addresses of devices connected to it. This means that the bridge is smart enough to know when to forward packets across to the segments that it connects. Bridges can be used to reduce the size of a collision domain or to connect networks of differing media/topologies, such as connecting an Ethernet network to a Token Ring network.

Switch

A switch is essentially a multi-port bridge. The switch learns the MAC addresses of each computer connected to each of its ports. So, when a switch receives a packet, it only forwards the packet out the port that is connected to the destination MAC address. Remember that a hub sends the packet out every port.

Router

A router works at the logical layer of the IP stack. It is basically required to route packets from one network (or subnet) to another network (or subnet). In the given question, all the computers are within the same subnet and a router is inappropriate.

Gateway

A gateway works at the top layers of the TCP/IP stack. For example, a Gateway may be used to facilitate communication between a Unix mail server and a Windows mail server.

Load Balancer

A load balancer is used to distribute workload across multiple computers or a computer cluster. It could be done by a dedicated hardware or software.

Proxies

proxies also called as proxy servers cache website information for the clients, reducing the amount of requests that need to be forwarded to the actual corresponding web server on the Internet. These save time, use bandwidth efficiently also help to secure the client connections.

VPN (Virtual Private Network)

1. VPN is private network formed using public Internet. It is formed between two hosts using tunneling protocols such as PPTP, L2TP, etc. Using VPN, you can connect two LANs in geographically distant locations together, as if they were located in the same building. The cost of connecting these LANs together is small since public Internet is used for providing the WAN link.

2. The VPN can be implemented in any of the following combinations:

- a. Gateway-to-gateway VPN: It is transparent to the end users.
- b. Gateway-to-host VPN
- c. Host-to-gateway VPN
- d. Host-to-host VPN :This configuration provides the highest security for the data
The host-to-host configuration provides the highest security for the data. However, a Gate-to-Gateway VPN is transparent to the end users.

3. VPN concentrators allow for secure encrypted remote access.

4. Intranet: It is used by the employees within the organization.

5. Extranet : The customers and vendors of the company use this for order processing, and inventory control on-line.

NIDS (Network Intrusion Detection System)

It is a type of IDS (intrusion detection system) that Detects malicious network activities. It constantly monitor the network traffic. A honeypot or honeynet is used to attract and trap potential attackers. Example Snort,

NIPS (Network Intrusion Prevention System)

It is designed to inspect traffic, and based on its configuration or security policy, it can remove, detain, or redirect malicious traffic. It removes, detains, or redirects malicious traffic. Example MacAfee Intrushield.

Protocol Analyzer And Packet Analyzer (Sniffer)

These are loaded on a computer and are controlled by the user in a GUI environment; they capture packets enabling the user to analyze them and view their contents. Example Network Monitor

Spam filters

Spam filters will help to filter out spam (unwanted e-mail). They can be configured in most e-mail programs or can be implemented as part of an anti-malware package

Network firewalls

These are also called as packet filters and these operate at low level of the TCP/IP stack. These do not allow packets to pass through unless they meet some established set of rules.

Application Firewall

It can control the traffic associated with specific applications. These work on the application layer of TCP/IP stack. These inspect each packet traveling to and from an application like browser, telnet and block them if they are improper according to set rules.

URL Filtering

URL filtering is used to categorize the websites on the internet. You can allow/block specific website access to the web users of the organization. This can be done by referring to central database or by classifying the websites in real time. URL filtering can also be made applicable only during certain times of a day or days of a week, if required.

Content inspection

Content inspection is the process in which user data is actively monitored for malicious elements, and bad behaviour according to configured policies before allowing or denying the content to pass through the gateway and enter into the network. This prevents any confidential data going outside the network.

1.2 Apply and implement secure network administration principles

All web applications such as Web servers, News servers, email servers etc. need to be configured as secure as possible. This can be achieved by

- Removing all unnecessary services. These are the services that are installed but not used. For example, you might have installed TFTP, but not using it. It is better to remove the application or service that is not used as it may provide an opportunity to a hacker to abuse the resource.
- Remove all unnecessary protocols: These are the protocols that are installed but not used. For example, you might have installed Novell Netware protocol but not necessary. It is preferable to remove that protocol.
- Enable server and application logs: The logs provide an opportunity to look into the activity on the server over the past few hours or days. Check for any unusual activity such as failed login attempts etc.

Secure router configuration

Before a router is put on a network make sure you set a username and password for it. Also, the password should be complex and difficult to crack. Make sure you check all default settings and change them according to requirement.

Access control lists (ACLs)

ACL resides on a router, firewalls or computers and decides who can access the network and who cannot.

That means it enable or deny traffic. It specify which user or group of users are allowed what level of access on which resource. It makes use of IP addresses and port numbers.

Port Security

It deals more with switches and the restriction of MAC addresses that are allowed to access particular physical ports.

802.1X

It is an IEEE standard that is known as port-based Network Access Control (PNAC). It works on Data Link Layer. It connect hosts to a LAN or WLAN. It also allows you to apply a security control that ties physical ports to end-device MAC addresses, and prevents additional devices from being connected to the network.

Flood Guards

It can be implemented on some firewalls and other devices. It tracks network traffic to identify scenarios such as SYN, ping, port floods, etc. By reducing this tolerance, it is possible to reduce the likelihood of a successful DoS attack. If it looks that an resource is being overused, then the flood guard comes in to picture.

Loop protection

To avoid loops, many network administrators implement Spanning Tree Protocol in their switches. Loop protection should be enabled on the switch to prevent the looping that can occur when a person connects both ends of a network cable to the same switch

Implicit deny

It requires that all access is denied by default and access permissions are granted to specific resources only when required. An implicit deny clause is implied at the end of each ACL, and it means that if the provision in question has not been explicitly granted, then it is denied.

Log Analysis

Log analysis is used to determine what happened at a specific time on a particular system.

1.3 Distinguish and differentiate network design elements and compounds

DMZ (DeMilitalized Zone)

It is a place separate from the LAN where servers reside that can be reached by users on the Internet. If a company intends to host its own servers to be accessed from public Internet, a DMZ is most preferred solution. The network segment within the DMZ is secured by two firewalls, one interfacing with the public Internet, and the other interfacing the internal corporate network. Thus, a DMZ provides additional layer of security to internal corporate network. The type of servers that are hosted on DMZ may include web servers, email servers, file servers, DNS servers, etc.

Subnetting

IP addresses can be manipulated to logically create sub networks .Each of this sub network is a distinct portion of a single network. Some advantages are efficient use of IP address space, reducing collision and traffic and increasing security.

VLAN

Just like subnetting VLAN is used to logically segment a network or part of a network. Some advantages are better organization of network, reducing collision, increase in performance and security. This does not require any change in physical location of the workstations. Users from different corner of the network like different floors in a building or even different buildings can belong to same VLAN as it is just logical segmentation.

NAT (Network Address Translation)

It is primarily used to hide internal network from external network, such as the Internet. A NAT basically translates the internal IP addresses to external IP addresses and vice-versa. This functionality assures that external users do not see the internal IP addresses, and hence the hosts.

Telephony

It is the collection of methods by which telephone services are provided to an organization or the mechanism by which organization uses telephone services for either voice and/or data communications. Traditionally it included POTS or PSTN services with modems but now it has expanded to PBX, VoIP and VPN.

NAC (Network Access Control)

NAC provides network security by setting the rules by which connections to a network are governed. Computers attempting to connect to a network are denied access unless they comply with rules including levels of antivirus protection, system updates, and so on...effectively weeding out those who would perpetuate malicious attacks. The client computer continues to be denied until it has been properly updated, which in some cases can be taken care of by the NAC solution automatically. This often requires some kind of preinstalled software (an agent) on the client computer, or the computer is scanned by the NAC solution remotely.

Virtualization

A workstation can have multiple operating systems installed on it but can run only one OS at a time but by running virtualization software same workstation can run Windows server along with windows 7 and Linux or any other operating system at the same time. This will allow a developer to test a code on various environments at the same time and he can also move code from one operating system to another with basic copy paste. Each virtual desktop will typically need full network access. Configuring permissions for each virtual desktop can be tricky for administrator. Remote administration often uses virtual desktop to work on a workstation without knowledge of user sitting on the workstation.

Cloud Computing

It is used to offer on-demand services it increase capabilities of a person's computer or an organization's network. Some cloud computing services are free like email services and some are paid services like data storage.

Cloud computing services are generally broken down into three categories of services:

- Software as a Service (SaaS): when users access applications over the Internet that are provided by a third party it is SaaS. There is no need to install the application on the local computer mostly these services run with in web-browser. Example: webmail.
- Infrastructure as a Service (IaaS): A service that offers computer networking, storage, load balancing, routing, and VM hosting. More and more organizations are seeing the benefits of offloading some of

their networking infrastructure to the cloud.

- Platform as a Service (PaaS): This service provide software solutions to organizations like application development in a virtual environment without the cost or administration of a physical platform. Its main use is for easy-to-configure operating systems and on-demand computing.

1.4 Implement and use common protocols

IPSec (Internet Protocol Security)

It authenticates and encrypts IP packets, effectively securing communications between the computers and devices that are used in VPN. IPsec operates at the Network Layer of the OSI model. It differs from SSH, SSL, and TLS in that it is the only protocol that does not operate within the upper layers of the OSI model. It can negotiate cryptographic keys and establish mutual. The two primary security services that are provided by IPSec are:

- Authentication Header (AH) : AH provides the authentication of the sender
- Encapsulating Security Payload : ESP provides encryption of the payload.

SNMP (Simple Network Management Protocol)

It enables monitoring of remote systems. There are three main parts of SNMP a manager, an agent, and a database of management information. The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical device(s) being managed. The manager and agent use a Management Information Base (MIB) and a set of commands to exchange information.

SSH (Secure Shell)

It is a protocol that can create a secure channel between two computers or network devices, enabling one computer or device to remotely control the other. It is commonly used on Linux and Unix systems, and nowadays also has widespread use on Windows clients. It uses public key cryptography to authenticate remote computers. One computer (the one to be controlled) runs the SSH daemon, while the other computer runs the SSH client and makes secure connections to the first computer (which is known as a server), as long as a certificate can be obtained and validated.

DNS(Domain Name System)

Resolves IP addresses to host names.

SSL (Secure Socket Layer) / TLS (Transport Layer Security)

These are cryptographic protocols that provide secure Internet communications such as web browsing, instant messaging, e-mail, and VoIP. These protocols rely on a PKI for the obtaining and validating of certificates. These are called Application Layer Protocol. Two types of keys are required when any two computers attempt to communicate with the SSL or TLS protocols: A public key and a session key. Asymmetric encryption is used to encrypt and share session keys, and symmetric encryption is used to encrypt the session data.

TCP/IP (Transmission Control Protocol/Internet Protocol)

It is suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the

Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols, such as Netware, also support TCP/IP.

FTPS (FTP Secure)

FTPS uses SSL or TLS to make secure connections. FTPS can work in two modes: explicit and implicit. In explicit mode the FTPS client must explicitly request security from an FTPS server and then mutually agree on the type of encryption to be used. In implicit mode, there is no negotiation, and the client is expected to already know the type of encryption used by the server. In general, implicit mode is considered to be more secure than explicit mode.

HTTPS (Hypertext Transfer Protocol Secure)

It is a combination of HTTP and either SSL or TLS. Web servers that enable HTTPS inbound connections must have inbound port 443 open. This is common for e-commerce.

SFTP (Secure FTP)

SFTP is the SSH File Transfer Protocol. It is an extension of the SSH protocol, which uses port 22. Contrast this with FTPS, which is FTP Secure or FTP-SSL, which uses port 443.

SCP (Secure Copy)

It is a way of transferring files securely between two hosts it utilizes SSH. It runs on port 22 by default.

ICMP (Internet Control Message Protocol)

The Internet Control Message Protocol (ICMP) protocol is classic example of a client server application. The ICMP server executes on all IP end system computers and all IP intermediate systems (i.e routers). The protocol is used to report problems with delivery of IP datagrams within an IP network. It can be used to show when a particular End System (ES) is not responding, when an IP network is not reachable, when a node is overloaded, when an error occurs in the IP header information, etc. The protocol is also frequently used by Internet managers to verify correct operations of End Systems (ES) and to check that routers are correctly routing packets to the specified destination address.

IPv4 Vs Ipv6

IPv4	IPv6
addresses are 32-bit in length	addresses are 128-bit in length
IP addresses are numeric only	uses a long string of numbers and letters in the IP address
Address is a 32-bit number made up of four octets (8-bit numbers) in decimal notation, separated by periods. A bit can either be a 1 or a 0 (2 possibilities), so the decimal notation of an octet would have 2^8 distinct possibilities	IPv6 addresses are broken down into eight 16-bit sections, separated by colons. Because each section is 16 bits, it can have 2^{16} variations (65,536 distinct possibilities)
Example: 1.160.10.240	Example: 3ffe:1900:4545:3:200:f8ff:fe21:67cf

1.5 Identify commonly used default network ports

Protocol	IP protocol	Port Used
FTP (File Transfer Protocol)	TCP	21
SFTP (Secure FTP)	SCTP,TCP	22
FTPS (FTP Secure)	FTP	443
TFTP (Trivial FTP)	UDP	69
Telnet	TCP	23
HTTP (Hyper Text Transfer Protocol)	TCP	80
HTTPS (HTTP Secure)	TCP	443
SCP (Secure Copy)	SCTP, TCP	22
SSH (Secure SHell)	SCTP, TCP	22
SMTP (Simple Mail Transfer Protocol)	TCP	25
DNS (Domain Name Service))	UDP	53
SNMP (Simple Network Management Protocol)	TCP, UDP	161
SNMP Trap (Simple Network Management Protocol Trap)	TCP, UDP	162
ISAKMP (VPN) – Internet Security Association and Key Management Protocol (virtual private network)	UDP	500
TACACS (Terminal Access Controller Access-Control System)	TCP,UDP	49
POP3 (Post Office Protocol version 3)	TCP	110
NNTP (Network News Transfer Protocol)	TCP	119
IMAP4 (Internet message access protocol version 4)	TCP	143
Kerberos	UDP	88
Syslog	TCP,UDP	514
L2TP (Layer 2 Tunneling Protocol)	UDP	1701
PPTP (Point-to-Point Tunneling Protocol)	TCP	1723
RDP (Remote Desktop Protocol)	TCP, UDP	3389

NetBIOS (Network Basic Input/Output System)

NetBIOS, or Network Basic Input/Output System, allows for session-layer communication on the OSI model. NetBIOS is primarily concerned with two functions: naming and starting/stopping NetBIOS “sessions.” Since NetBIOS is not actually a networking protocol (it's an API) it is not routable and therefore nodes are only visible to other nodes within the same subnet.

1.6 Implement wireless network in a secure manner

WEP (Wired Equivalent Privacy)

A deprecated wireless network security standard, less secure than WPA. Key size is 64 bit. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not very secure. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

WPA (Wi-Fi Protected Access)

A wireless encryption standard created by the Wi-Fi Alliance to secure wireless computer networks. WPA improves on the authentication and encryption features of WEP (Wired Equivalent Privacy). Key size is 128 bits. WPA provides stronger encryption than WEP through use of either of two standard technologies: Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). WPA also includes built-in authentication support that WEP does not offer. WPA provides comparable security to VPN tunneling with WEP, with the benefit of easier administration and use.

WPA2 (Wi-Fi Protected Access Version 2)

It is wireless encryption protocol and is based on the IEEE 802.11i technology standard for data encryption. Key size is 256 bits. It is more secure than WPA and WEP. WPA2 also improves the security of Wi-Fi connections by requiring use of stronger wireless encryption than what WPA requires. Specifically, WPA2 does not allow use of an algorithm called TKIP (Temporal Key Integrity Protocol) that has known security holes (limitations) in the original WPA implementation. There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.

EAP (Extensible Authentication Protocol)

It is a framework for transporting authentication protocols. EAP defines the format of the messages. It uses four types of packets : request, response, success and failure. Request packets are issued by authenticator and ask for response packet from supplicant. If authentication is successful, a success packet is sent to the supplicant is not a failure packet is sent.

PEAP (Protected EAP)

It is designed to simplify deployment of 802.1x by using MS Windows logins and passwords. It is considered more secure than EAP because it creates an encrypted channel between client and authentication server and the channel then protects further authentication exchanges.

LEAP (Lightweight EAP)

It is developed by Cisco Systems. It requires mutual authentication used for WLAN encryption using Cisco client software. There is no native support for LEAP in MS Windows operating system

MAC Filtering

Every Wi-Fi device is assigned a MAC (Media Access Control) address, a unique 12-digit hexadecimal identifier issued by the IEEE, the standards body that developed the Wi-Fi protocol. The MAC address is "hard-coded" in to the device and sent automatically to a Wi-Fi access point when the device tries to connect to the network.

Using the access point configuration software, you can create a safe list of allowed client devices or a black list of banned devices. If MAC filtering is activated, regardless of what encryption security is in place, the AP only allows devices on the safe list to connect, or blocks all devices on the black list – irrespective of encryption used.

Encryption protocols like WPA2 (Wi-Fi Protected Access 2), reduced the necessity for using MAC filtering. Hackers may break in to MAC filtering device by sniffing addresses of connected devices and then spoofing or masquerading as one of them.

To enable MAC address filtering and to allow the devices with matching MAC addresses, perform these steps (these steps are generic in nature, and likely to change from one device type to another):

- Step 1: Access the router's web-based setup page.
- Step 2: When the router's web-based setup page appears, click Wireless, look for MAC address filtering tab.
- Step 3: Enter the MAC addresses of the devices that are allowed to use the wireless network in the table provided.
- Step 3: Click on Save Settings

TKIP (Temporal Key Integrity Protocol)

It is an Encryption protocol used with WEP and WPA. Key size is 128 bits.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)

It is an Encryption protocol used with WPA2. It addresses the vulnerabilities of TKIP and meets requirements of IEEE 802.11i. It uses 128 bit Key.

SSID (Service Set Identifier)

One way to secure your wireless network is to disable the SSID broadcast. This procedure prevents other users from detecting your SSID or your wireless network name when they attempt to view available wireless networks in your area.

To disable SSID Broadcast, perform these steps (these steps are generic in nature, and likely to change from one device type to another):

- Step 1: Access the router's web-based setup page.
- Step 2: When the router's web-based setup page appears, click Wireless, look for Wireless SSID Broadcast, and select Disable.
- Step 3: Click on Save Settings

2. Compliance and Operational Security

2.1 Explain risk related concepts

Security controls

Security controls are measures taken to safeguard an information system from attacks against the confidentiality, integrity, and availability (C.I.A.) of the information system. Security controls fall in three classes

1. Technical

- Access Control , firewalls
- Audit and Accountability

- Identification and Authentication
- System and Communications Protection

2. Management

- Certification, Accreditation, and Security Assessments
- planing
- Risk Assessment
- System and Services Acquisition

3. Operational

- Awareness and Training
- Configuration Management
- Contingency Planning
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- System and Information Integrity
- Maintenance

False positives

False positives are when the system reads a legitimate event as an attack or other error. When a system authenticates a user who should not be allowed access to the system. For example, when an IDS/IPS blocks legitimate traffic from passing on to the network.

Privacy policy

This policy is used to secure user identities and other information related to user. If an internet based application provided by an organization require users to register with them using name and email id then this information provided by the user should be secure and not shared with any third party without user knowledge. Privacy policy should state what information is stored and will be accessed by whom, it should also state if information will be shared with third party.

Acceptable use

This policy restricts how a computer network and other devices and systems will be used. It states what users can do and what not with technology infrastructure of an organization. It is signed by the employees before they begin working on any systems. This protects the organization from employees misusing the systems or network. The policy may put limits on personal use of resources, and resource access time.

Security policy

A company's security policy outlines the security measures to be taken. Implementing the security policy is

the first thing that needs to be done. Some issues that need to be taken care of, while planning security policies are:

- Due care, acting responsibly and doing right thing.
- Privacy, letting the employees and administrator know of the privacy issues
- Separation of duties :It ensures that the vital activities are bifurcated among several individuals. This ensures that one or two individuals can not perform a fraud.
- Need to know, providing employees only the information required to perform their role or duties.
- Password management, auditing the passwords
- Disposal and destruction
- Human rights policies, and
- Incident response, should take care of response to an act.
- least privilege principle means a user should be given only the minimum privileges that are required to do his/her works accurately and completely. Other choices are not appropriate.
- The security policy should clearly state that no one is ever allowed to share his/her password with anyone else. Secondly, the security policy should state that the help desk can only change or assign a new password after positive identification of the individual requesting the information

Risk Management

Risk management can be defined as the identification, assessment, and prioritization of risks, and the mitigating and monitoring of those risks.

1. Risk transference

The purpose of this action is to take a specific risk, which is detailed in the insurance contract, and pass it from one party who does not wish to have this risk (the insured) to a party who is willing to take on the risk for a fee, or premium (the insurer). Example organization that purchases insurance for a group of servers in a data center. The organization still takes on the risk of losing data in the case of server failure, theft, and disaster, but transfers the risk of losing the money those servers are worth in the case they are lost.

2. Risk avoidance

It refers to not carrying out a proposed plan because the risk factor is too great. If an organization decided not to implement a new website based on its calculation that too many attackers would attempt to hack it.

3. Risk acceptance

Also known as risk retention. Most organizations are willing to accept a certain amount of risk. Sometimes, vulnerabilities that would otherwise be mitigated by the implementation of expensive solutions are instead dealt with when and if they are exploited.

4. Risk reduction

This is the main aim of risk management that is to reduce the risk to an acceptable level.

2.2 Carry out appropriate risk mitigation strategies

- Change management refers to a methodology for making modifications and keeping track of those changes. In some instances, changes to network or system configurations are made haphazardly to alleviate a pressing problem. Without proper documentation, a future change may negate or diminish a previous change or even

unknowingly create a security vulnerability. Change management seeks to approach changes systematically and provide the necessary documentation of the changes.

- Incident management can be defined as the “framework” and functions required to enable incident response and incident handling within an organization. The objective of incident management is to restore normal operations as quickly as possible with the least possible impact on either the business or the users
- Routine system audits will check for user rights and permissions as well as analyze log files, for example, the Security log in Windows. The development and implementation of the security policy that enabled the security log should have been done long before actual auditing takes place.

2.3 Execute appropriate incident response procedures

Order Of Volatility

The sequence of volatile data that must be preserved in a computer forensics investigation

- Register, cache
- routing table, AP cache, process table, kernel statistics, memory
- Temporary file system
- Disk
- Remote logging and monitoring data that is relevant to system
- Physical configuration, network topology
- Archival media

Capture system Image

Forensic imaging program is used to create bit stream image copy of a storage device. The image copy will be stored onto a forensically clean storage device. Hash calculation of original media is performed before and after image copying is performed

Network traffic and logs

In some network environments it may be possible to maintain an ongoing recording of network traffic. Since this would result in huge storage requirement these recording will only maintain a sliding window in minutes or hours of recent network activity

Capture Video

If there are security cameras present then recording of security violation should be preserved. Another is video recording of investigation being performed to collect physical and logical evidences. These can be used for later reviews.

Chain of custody

The chain of custody documents that the evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt the evidence. A chain of custody includes documenting all of the serial numbers of the systems involved, who handled and had custody of the systems and for what length of time, how the computer was shipped, and any other steps in the process.

2.4 Explain the importance of security related awareness and training

Given below are some of the widely known password guessing methods:

- Dictionary: this is the method in which dictionary terms are used for guessing a password
- Birthday: It takes advantage of probabilities, much like two people in a 50-person room shared the same birthday. With every person, the chances of two people having the same birth date increases. In the same way, when you start guessing the password, the chances of a hit keep increasing.
- Brute force: In a Brute Force attack, muscle (in this case, CPU and/or network muscle) is applied to break through a particular security mechanism, rather than using particular intelligence or logic. “Brute force” is most commonly applied to password guessing, taking advantage of computer power available to an attacker, to try every possible password value, until the right one is found. In cryptography, a brute-force attack is an attempt to recover a cryptographic key or password by trying every possible combination until the correct one is found. How quickly this can be done depends on the size of the key, and the computing resources applied.
- Rainbow tables: Rainbow tables are huge lists of keys or passwords. A password-guessing program uses these lists of keys or passwords rather than generating each key or password itself.

2.5 Compare and contrast aspects of business continuity

Any business continuity planning preferably include the following:

- Redundant network connectivity
- Clustering
- Fault tolerance using Raid or similar technique
- Facilities management

Disaster recovery plan is also called as business continuity plan or business process continuity plan. A DRP should include information security, asset security, and financial security plans.

SLA (Short for Service Level Agreement) is the formal negotiated document between two parties. It is a legal document that binds both the parties during the tenure of the agreement.

2.6 Explain the impact and proper use of environmental controls

There are primarily 5 classes of fire:

- Class 'A' Fire: Involves ordinary combustible materials such as wood, cloth and paper. Most fires are of this class.
- Class 'B' Fire: Involves flammable liquids or liquid flammable solids such as petrol, paraffin, paints, oils, greases and fat.
- Class 'C' Fire: Involves gases. Gaseous fires should be extinguished only by isolating the supply. Extinguishing a gas fire before the supply is off may cause an explosion.
- Class 'D' Fire: Involves burning metals. These should only be dealt with, by using special extinguishers, by personnel trained in the handling of combustible metals.

- Class 'F' Fire: Involves flammable liquids (Deep Fat Fryers)

There are five types of extinguishers:

- Water : Water is used with Class A fires.
- Dry chemical :Regular dry chemical extinguishers have a sodium bicarbonate base and are effective on Class B and C fires.
- Halon :Halon Extinguishers are best used on Class B or C fires.
- Carbon dioxide : Carbon Dioxide Extinguishers are used primarily on Class C fires and are also effective on Class B fires.
- Foam: Foam extinguishers are less commonly used.

2.7 Execute disaster recovery plans and procedures

A properly managed tape backups should include the following:

- Regular backups according to a pre-determined plan
- Verifying the backup tapes for integrity
- Labeling tapes properly for easy and unique identification
- Storing tapes securely at off-site location
- Destroying data on old tapes before disposing off the same

There are primarily three types of backups:

- Full backup : Here all the data gets backed up. It usually involves huge amounts of data for large systems, and may take hours to complete. A full backup is preferred instead of incremental or differential backups where it is feasible. However, when there is large amount of data, full backup is done once in a while and incremental or differential backups are done in between. A backup plan is usually put in place prior to taking backup of data.
- Differential backup : A differential backup includes all the data that has changed since last full backup. The “differential backup” that was taken earlier (after the “full backup” but before the current “differential backup”) becomes redundant. This is because all changed data since last “full backup” gets backed up again.
- Incremental backup :It includes all the data changed since last incremental backup. Note that for data restoration the full backup and all incremental backup tapes since last full backup are required. The archive bit is set after each incremental backup. Incremental backup is useful for backing up large amounts of data, as it backs up only the changes files since previous incremental backup.

It is recommended to store the backup tapes in a secure, physically distant location. This would take care of unforeseen disasters like natural disasters, fire, or theft. It is also important that the backup tapes are regularly verified for proper recovery in a test server, even though recovery is not really required at that time. Otherwise, it may so happen that you find a backup tape corrupt when it is really required.

2.8 Exemplify the concepts of confidentiality, integrity and availability (CIA)

- Confidentiality. It is important that only approved individuals are able to access important

information. It ensures that only authorized parties can view the information. For example credit card numbers.

- **Integrity.** Integrity ensures that the information is correct and no unauthorized person or malicious software has altered the data. In the example of the online purchase, the amount to be transferred should not be altered by any one.
- **Availability.** It ensures that data is accessible to authorized users. The total number of items ordered as the result of an online purchase must be made available to an employee in a warehouse so that the correct items can be shipped to the customer

3. Threats and Vulnerabilities

3.1 Analyze and differentiate among types of malware

- **Adware:** Type of spyware that pops up advertisements based on what it has learned about the user.
- **Virus:** A computer virus attaches itself to a program or file so it can spread from one computer to another. Almost all viruses are attached to an executable file, and it cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going.
- **Worm:** Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. The danger with a worm is its capability to replicate itself. Unlike Virus, which sends out a single infection at a time, a Worm could send out hundreds or thousands of copies of itself, creating a huge devastating effect.
- **Trojan Horse:** The Trojan Horse, at first glance appears to be a useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening it because it appears to be receiving legitimate software or file from a legitimate source.
- **Spyware** A type of malicious software either downloaded unwittingly from a website or installed along with some other third-party software.
- **Rootkit:** It is a collection of tools that enable administrator-level access to a computer. Typically, a hacker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to gain root access to the computer and, possibly, other machines on the network.
- A back door is a program that allows access to the system without usual security checks. These are caused primarily due to poor programming practices. The following are know back door programs:
 1. **Back Orifice:** A remote administration program used to remotely control a computer system.
 2. **NetBus:** This is also a remote administration program that controls a victim computer system over the Internet. Uses client –server architecture. Server resides on the victim’s computer and client resides on the hackers computer. The hacker controls the victim’s computer by using the client.

3. Sub7: This is similar to Back Orifice, and NetBus. Used to take control of victim's computer over the Internet.

- Botnet : it is an compromised computer from which malware can be distributed throughout the internet .It is controlled by a master computer where attacker resides.

3.2 Analyze and differentiate among types of attacks

Man-In-The-Middle

These attacks intercept all data between a client and a server. It is a type of active interception. If successful, all communications now go through the MITM attacking computer. The attacking computer can at this point modify the data, insert code, and send it to the receiving computer. This type of eavesdropping is only successful when the attacker can properly impersonate each endpoint.

Distributed Denial of Service (DdoS)

It is an attack where multiple compromised systems (which are usually infected with a Trojan) are used to send requests to a single system causing target machine to become unstable or serve its legitimate users. A hacker begins a DDoS attack by exploiting a vulnerability in one computer system and making it the DDoS "master", also called as "zombie". It is from the zombie that the intruder identifies and communicates with other systems that can be compromised. The intruder loads hacking tools on the compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. This causes Distributed Denial of Service (DDoS) attack on the target computer.

Denial-of-service (DoS)

These attacks, are explicit attempts to block legitimate users system access by reducing system availability. Any physical or host-based intrusions are generally addressed through hardened security policies and authentication mechanisms. Although software patching defends against some attacks, it fails to safeguard against DoS flooding attacks, which exploit the unregulated forwarding of Internet packets. Hackers use zombies to launch DoS or DDoS attacks. The hacker infects several other computers through the zombie computer. Then the hacker sends commands to the zombie, which in turn sends the commands to slave computers. The zombie, along with slave computers start pushing enormous amount of useless data to target computer, making it unable to serve it legitimate purpose.

Smurf attack

Smurf attack is a denial-of-service attack that uses spoofed broadcast ping messages to flood a target system

Phishing

Phishing is the act of sending an e-mail to a user claiming to be a reputed organization (such as a bank) in an attempt to scam the user into providing information over the Internet. The e-mail directs the user to a Web site where they are prompted to provide private information, such as credit card, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Zombies

Zombies are malware that puts a computer under the control of a hacker. Hackers use zombies to launch DoS or DDoS attacks. The hacker infects several other computers through the zombie computer. Then the hacker sends commands to the zombie, which in turn sends the commands to slave computers. The zombie, along

with slave computers start pushing enormous amount of useless data to target computer, making it unable to serve it legitimate purpose.

IP spoofing

In IP spoofing, the attacker uses somebody else's IP address as the source IP address. Since routers forward packets based on the destination IP address, they simply forward the packets to the destination without verifying the genuineness of the source IP address.

Replay

A replay attack is a network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. An attacker might use a packet sniffer to intercept data and retransmit it later.

spoofing

When an attacker masquerades as another person by falsifying information.

Pharming

It is when an attacker redirects one website's traffic to another bogus and possibly malicious website. Pharming can be prevented by carefully monitoring DNS configurations and hosts files.

DNS poisoning

The modification of name resolution information that should be in a DNS server's cache.

ARP poisoning

It is an attack that exploits Ethernet networks, and it may enable an attacker to sniff frames of information, modify that information, or stop it from getting to its intended destination. The spoofed frames of data contain a false source MAC address, which deceives other devices on the network.

Transitive access

When one computer uses a second computer to attack a third, based on the trust of the second and third computers

3.3 Analyze and differentiate among types of social engineering attacks

Social engineering

It is a skill that an attacker uses to trick an innocent person such as an employee of a company into doing a favor. For example, the attacker may hold packages with both the hands and request a person with appropriate permission to enter a building to open the door. Social Engineering is considered to be the most successful tool that hackers use. Social engineering can be used to collect any information an attacker might be interested in, such as the layout of your network, names and/or IP addresses of important servers, installed operating systems and software. The information is usually collected through phone calls or as new recruit or guest to your boss.

1. Shoulder surfing is when a person uses direct observation to find out a target's password, PIN, or other such authentication information. The simple resolution for this is for the user to shield the screen, keypad, or other authentication requesting devices.

2. Dumpster diving is when a person literally scavenges for private information in garbage and recycling containers. Any sensitive documents should be stored in a safe place as long as possible. When they are no longer necessary, they should be shredded.
3. Piggybacking is where the intruder poses as a new recruit, or a guest to your boss. The intruder typically uses his social engineering skills to enter a protected premises on someone else's identity, just piggybacking on the victim.
4. Tailgating is essentially the same as Piggybacking with one difference: it is usually without the authorized person's consent.
5. Impersonation is when an unauthorized person impersonate as a legitimate, authorized person.
6. A hoax is the attempt at deceiving people into believing something that is false. hoaxes can come in person, or through other means of communication

Staff training is the most effective tool for preventing attacks by social engineering. Defense against social engineering may be built by:

- Including instructions in your security policy for handling it, and
- Training the employees what social engineering is and how to deal with it.

3.4 Analyze and differentiate among types of wireless attacks

1. Packet sniffing is a form of wire-tap applied to computer networks instead of phone networks. It came into vogue with Ethernet, which is known as a "shared medium" network. This means that traffic on a segment passes by all hosts attached to that segment. Ethernet cards have a filter that prevents the host machine from seeing traffic addressed to other stations. Sniffing programs turn off the filter, and thus see everyone traffic.
2. Bluesnarfing allows hackers to gain access to data stored on a Bluetooth enabled phone using Bluetooth wireless technology without alerting the phone's user of the connection made to the device. The information that can be accessed in this manner includes the phonebook and associated images, calendar, and IMEI (International Mobile Equipment Identity). By setting the device in non-discoverable, it becomes significantly more difficult to find and attack the device.
3. The evil twin is another access point or base station that uses the same SSID as an existing access point. It attempts to fool users into connecting to the wrong AP, compromising their wireless session.
4. Wardriving is the act of using a vehicle and laptop to find open unsecured wireless networks
5. Rogue access points can be described as unauthorized wireless access points/routers that allow access to secure networks
6. Interference happens when devices share channels, are too close to each other, or multiple technologies share the same frequency spectrum

3.5 Analyze and differentiate among types of application attacks

1. Cross-site scripting (XSS) is an attack on website applications that injects client-side script into web pages.

2. SQL injection is when code (SQL-based) is inserted into forms or databases. Input validation is the best way to prevent SQL injection attacks on web servers and database servers
3. LDAP injection is similar to SQL injection, again using a web form input box to gain access, or by exploiting weak LDAP lookup configurations. The Lightweight Directory Access Protocol is a protocol used to maintain a directory of information such as user accounts, or other types of objects. The best way to protect against this (and all code injection techniques for that matter) is to incorporate strong input validation.
4. Buffer overflow occurs when the input is more than that allocated for that purpose. The system doesn't know what to do with the additional input, and it may result in freezing of the system, or sometimes to take control of the system by a hacker. By validating the inputs, it is possible to reduce this vulnerability to a great extent.
5. A zero day attack is an attack executed on a vulnerability in software, before that vulnerability is known to the creator of the software. It's not a specific attack, but rather a group of attacks including viruses, Trojans, buffer overflow attacks, and so on. These attacks can cause damage even after the creator knows of the vulnerability, because it may take time to release a patch to prevent the attacks and fix damage caused by them.

3.6 Analyze and differentiate among types of mitigation and deterrent techniques

The process of securing a computer system is called Hardening. There are several things that one need to remember for hardening a PC. These include:

1. Removing non-essential programs, and services. These may provide back-doors for an attacker.
2. Installing an anti-virus package, and a spyware remover
3. Removing unnecessary protocols. If you are using only TCP/IP (required for connecting to the Internet), keep that protocol and remove all other protocols.
4. Disable guest account
5. Rename Administrator account
6. Enable auditing, so that you can view any logon attempts.
7. Installing latest patches, and service packs to operating system, and software.

A few techniques used by IDS (Intrusion Detection Systems) include the following:

- a. Anomaly detection : Anomaly detection method establishes a baseline of normal usage patterns, and anything that widely deviates from the baseline is investigated for possible intrusion. An example of this would be if a user logs on and off of a machine 10 times a day instead of the normal once or twice a day.
- b. Signature detection : Signature detection uses specifically known patterns of unauthorized behavior to predict and detect subsequent similar attempts. These specific patterns are called signatures.
- c. Target monitoring : Target monitoring systems do not actively search for anomalies or misuse, but instead look for the modification of specified files.
- d. Stealth probes

IDS stands for Intrusion Detection System. There are primarily two types of IDSs. These are Network based IDS (NIDS), and Host based IDS (HIDS). If the IDS monitors network wide communication, it is called Network based IDS, and if the IDS monitors security on a per host basis, it is called Host based IDS.

A host based IDS should be placed on a host computer such as a server. Network based IDS is typically placed on a network device such as a router.

Log Files Explained:

- **Application log:** The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. The developer decides which events to record.
- **System log:** The system log contains events logged by the Windows 2000 system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined.
- **Security log:** The security log can record security events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.
- **Antivirus log:** Antivirus log analyzer can process log files from various antivirus packages and generate dynamic statistics from them, analyzing and reporting events.

Computer log files can be tampered with by a hacker to erase any intrusions. Computer logs can be protected using the following methods:

- Setting minimal permissions
- Using separate logging server
- Encrypting log files
- Setting log files to append only
- Storing them on write-once media

Implementing all the above precautions ensures that the log files are safe from being tampered.

3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities

Honeypots

Honeypots are designed such that they appear to be real targets to hackers. That is a hacker can not distinguish between a real system and a decoy. This enables lawful action to be taken against the hacker, and securing the systems at the same time.

Protocol Analyzer And Packet Analyzer (Sniffer)

These are loaded on a computer and are controlled by the user in a GUI environment; they capture packets enabling the user to analyze them and view their contents. Example Network Monitor

Honeynet

honeynet is one or more computers, servers, or an area of a network; these are used when a single honeypot is not sufficient. Either way, the individual computer, or group of servers, will usually not house any important company information.

Port scanner

port scanner used to find open ports on multiple computers on the network.

Any software is inherently prone to vulnerabilities. Therefore, software manufacturers provide updates or

patches to the software from time to time. These updates usually take care of any known vulnerabilities. Therefore, it is important to apply these updates. Additional functionality is also one of the reasons for applying software updates. However, many times, it is not the compelling reason to apply the updates.

3.8 Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning

Vulnerability testing is part of testing corporate assets for any particular vulnerability. These may include:

1. Blind testing: Here the hacker doesn't have a prior knowledge of the network. It is performed from outside of a network.
2. Knowledgeable testing: Here the hacker has a prior knowledge of the network.
3. Internet service testing: It is a test for vulnerability of Internet services such as web service.
4. Dial-up service testing: Here the hacker tries to gain access through an organization's remote access servers.
5. Infrastructure testing: Here the infrastructure, including protocols and services are tested for any vulnerabilities.
6. Application testing: The applications that are running on an organization's servers are tested here.

Vulnerability assessment is part of an organization's security architecture.

4. Application, Data and Host Security

4.1 Explain the importance of application security

Fuzzing (fuzz testing) is the automated insertion of random data into a computer program. It is used to find vulnerabilities by the people who developed the program and by attackers.

Cross-site scripting prevention

XSS attack an attacker inserts malicious scripts into a web page in the hopes of gaining elevated privileges and access to session cookies and other information stored by a user's web browser. This code (often JavaScript) is usually injected from a separate "attack site." It can also manifest itself as an embedded JavaScript image tag or other HTML embedded image object within e-mails (that are web-based.)

Cross-site Request Forgery (XSRF)

This attack (also known as a one-click attack), the user's browser is compromised and transmits unauthorized commands to the website. The chances of this attack can be reduced by requiring tokens on web pages that contain forms, special authentication techniques (possibly encrypted), scanning .XML files (which could contain the code required for unauthorized access), and submitting cookies twice instead of once, while verifying that both cookie submissions match.

Application hardening

It is the securing of an application, disabling of unnecessary services, disabling unused accounts, removal of unnecessary applications, and so on.

Application configuration baseline

Baselining is the process of setting up the common, minimum requirements of an enterprise. This could be for a group of computers or all the computers in the network. When a new computer is added to the domain, the common minimum requirements are installed and applied automatically. This saves a lot of time and effort for the administrators. A typical configuration baseline would include changing any default settings (like Guest account), removing unwanted softwares, services, games and enabling operating system security features like enabling Firewall.

Application patch management

Any software is inherently prone to vulnerabilities. Therefore, software manufacturers provide updates or patches to the software from time to time. These updates usually take care of any known vulnerabilities. Therefore, it is important to apply these updates. Additional functionality is also one of the reasons for applying software updates. However, many times, it is not the compelling reason to apply the updates.

4.2 Carry out appropriate procedures to establish host security

In addition to protecting the hardware, the operating system on the host must also be protected. This can be achieved through a five-step process:

1. Develop the security policy.
2. Perform host software baselining.
3. Configure operating system security and settings.
4. Deploy the settings.
5. Implement patch management.

Operating system software has continued to add security protections to its core set of features. In addition, there are third-party anti-malware software packages that can provide added security.

Anti-Virus

This software can examine a computer for any infections as well as monitor computer activity and scan new documents that might contain a virus this action is performed when files are opened, created, or closed. If a virus is detected, options generally include cleaning the file of the virus, quarantining the infected file, or deleting the file. Anti-virus scan files by attempting to match known virus patterns or signatures against potentially infected files. Software contains a virus scanning engine and a regularly updated signature file. The Anti-virus software vendor extracts a sequence of bytes found in the virus as a virus signature. Signatures from all the different computer viruses are organized in a database, which the virus scanning engine uses to search predefined areas of files.

Anti-Spam

Spammers can distribute malware through their e-mail messages as attachments and use spam for social engineering attacks. Different methods for filtering spam exist on the host to prevent it from reaching the user. One method of spam filtering is to install separate filtering software that works with the e-mail client software. Host e-mail clients can be configured to filter spam, such as creating or downloading a list of senders from which no e-mail is to be received (blacklist), create a list from which only e-mail can be received, or block e-mail from entire countries or regions.

Pop-up Blockers and Anti-Spyware

A pop-up is a small Web browser window that appears over the Web site that is being viewed. Most pop-up windows are created by advertisers and launch as soon as a new Web site is visited. A pop-up blocker can be

either a separate program or a feature incorporated within a browser that stops pop-up advertisements from appearing. As a separate program, pop-up blockers are often part of a package known as anti-spyware that helps prevent computers from becoming infected by different types of spyware.

Host-based firewalls

A firewall can be software-based or hardware-based. A host-based software firewall runs as a program on a local system to protect it against attacks.

Application patch management

Any software is inherently prone to vulnerabilities. Therefore, software manufacturers provide updates or patches to the software from time to time. These updates usually take care of any known vulnerabilities. Therefore, it is important to apply these updates. Additional functionality is also one of the reasons for applying software updates. However, many times, it is not the compelling reason to apply the updates.

Hardware security

Hardware security is the physical security that involves protecting the hardware of the host system, particularly portable laptops, netbooks, and tablet computers that can easily be stolen.

- A cable lock can be inserted into a slot in the device and rotated so that cable lock is secured to the device, while a cable connected to the lock can then be secured to a desk or chair.
- When storing a laptop, it can be placed in a safe, which is a ruggedized steel box with a lock. The sizes typically range from small (to accommodate one laptop) to large (for multiple devices).
- Locking cabinets can be prewired for electrical power as well as wired network connections. This allows the laptops stored in the locking cabinet to charge their batteries and receive software updates while not in use.

Secure Mobile Devices

- Screen lock. Uses a password to lock the device. This prevents a thief from using a stolen device.
- Proximity lock. Automatically locks your mobile device or smart-phone when you are away from the phone. It uses a proximity sensor that you may personally carry such as a blue tooth device. Strong password. Any time a password is used to protect a mobile device (or any device or system), it should be strong. This means they are at least eight characters and include multiple character types, such as upper case, lower case, numbers, and symbols. Data encryption. Encryption protects the confidentiality of data and smart-phone security includes device encryption to protect the data against loss of confidentiality. It's possible to selectively encrypt some data on a system, an entire drive, or an entire device.
- Remote wipe. Remote wipe capabilities are useful if the phone is lost. The owner can send a remote wipe signal to the phone to delete all the data on the phone. This also deletes any cached data, such as cached online banking passwords, and provides a complete sanitization of the device, ensuring that all valuable data is removed.
- Voice encryption. It's possible to use voice encryption with some phones to help prevent the interception of conversations Global positioning system (GPS) tracking. A GPS pinpoints the location of the phone. Many phones include GPS applications that you can run on another computer. If you lose your phone, GPS can help you find it. If the data is sensitive, you use remote wipe feature to

erase the data on the mobile. This is useful to know before you send a remote wipe signal.

- Cable locks can secure a mobile computer. They often look about the same as a cable lock used to secure bicycles. Locked cabinet. Small devices can be secured within a locked cabinet or safe. When they aren't in use, a locked cabinet helps prevent their theft.
- Strong password. Any time a password is used to protect a mobile device (or any device or system), it should be strong. This means they are at least eight characters and include multiple character types, such as upper case, lower case, numbers, and symbols.

4.3 Explain the importance of data security

Data loss prevention (DLP)

These are systems are designed to protect data by way of content inspection. They are meant to stop the leakage of confidential data, often concentrating on communications. There are three types of DLP systems:

- Network-based DLP
- Endpoint-based DLP
- Storage-based DLP

Full Disk Encryption

This works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn't have the key to "undo" the conversion. Without the proper authentication key, even if the hard drive is removed and placed in another machine, the data remains inaccessible

Database Encryption

This allows securing the data as it is inserted to, or retrieved from the database. The encryption strategy can thus be part of the database design and can be related with data sensitivity and/or user privileges. Selective encryption is possible and can be done at various granularities, such as tables, columns, rows

Hardware-based Encryption

- Data encryption. Encryption protects the confidentiality of data on servers just as it can protect the confidentiality of data on mobile devices. It's possible to selectively encrypt individual files or entire disk volumes.
- Mantrap and cipher lock. These are examples of physical security and they can be used to restrict access to a server room.
- Proximity lock. This secures the Server by locking it when the sensor (say a blue-tooth device worn by the administrator) is not within a specified distance from the server.
- Firewall. Software-based firewalls are commonly used on servers but are extremely rare on mobile devices.
- TPM and HSM. Trusted Platform Modules (TPMs) and Hardware Security Modules (HSMs) are hardware encryption devices.

5. Access Control and Identity Management

5.1 Explain the function and purpose of authentication services

Remote Authentication Dial-In User Service (RADIUS)

It provides centralized administration of dial-up, VPN, and wireless authentication and can be used with EAP and 802.1X.

Terminal Access Controller Access-Control System (TACACS)

It is remote authentication protocol used more often in UNIX networks. In UNIX, the TACACS service is known as the TACACS daemon. The newer and more commonly used implementation of TACACS is called TACACS+. It is not backward compatible with TACACS. TACACS+, and its predecessor XTACACS, were developed by Cisco. TACACS+ uses inbound port 49. TACACS and XTACACS are not commonly seen anymore. The two common protocols used today are RADIUS and TACACS+.

Kerberos

Kerberos is basically an authentication protocol that uses secret-key cryptography for secure authentication. In Kerberos, all authentication takes place between clients and servers. The name Kerberos comes from Greek mythology; it is the three-headed dog that guarded the entrance to Hades. It was developed by the Massachusetts Institute of Technology, USA

Kerberos require that the time sources are approximately in synchronization (with in 5 minutes) with each other. However, with recent revisions of Kerberos software, this rule has become flexible.

Some of the features of Kerberos authentication system:

- Uses client-server based architecture.
- Kerberos server, referred to as KDC (Key Distribution Ceter) implements the Authentication Service (AS) and the Ticket Granting Service (TGS).
- The term "application server" generally refers to Kerberized programs that clients communicate with using Kerberos tickets for authentication purpose. For example, the Kerberos telnet daemon (telnetd) is an example of an application server.

When the user wants to talk to a Kerberized service, he uses the TGT to talk to the Ticket Granting Service (TGS, also runs on the KDC). The TGS verifies the user's identity using the TGT and issues a ticket for the desired service.

The TGT ensures that a user doesn't have to enter in their password every time they wish to connect to a Kerberized service. The TGT usually expires after eight hours. If the Ticket Granting Ticket is compromised, an attacker can only masquerade as a user until the ticket expires.

The following are the important properties of Kerberos:

- It uses symmetric encryption
- Tickets are time stamped
- Passwords are not sent over the network

LDAP (Lightweight Directory Access Protocol)

It contains the directory for a network and allows for a single point of user management of that directory.

5.2 Explain the fundamental concepts and best practices related to authentication, authorization and access control

Computer based access controls prescribe not only who or what process may have access to a given resource,

but also the type of access that is permitted. These controls may be implemented in the computer system or in external devices. Different types of access control are:

- **Mandatory Access Control (MAC)** secures information by assigning sensitivity labels on objects (resources) and comparing this to the level of sensitivity a subject (user) is operating at. MAC ensures that all users only have access to that data for which they have matching or greater security label (or security clearance). In general, MAC access control mechanisms are more secure than DAC. MAC is usually appropriate for extremely secure systems including multilevel secure military applications or mission critical data applications.
- **Discretionary Access Control (DAC):** Discretionary Access Control (DAC) is a means of restricting access to information based on the identity of users and/or membership in certain groups. Access decisions are typically based on the authorizations granted to a user based on the credentials he presented at the time of authentication (user name, password, hardware/software token, etc.). In most typical DAC models, the owner of information or any resource is able to change its permissions at his discretion. DAC has the drawback of the administrators not being able to centrally manage these permissions on files/information stored on the web server.
- **Role Based Access Control (RBAC):** In Role-Based Access Control (RBAC), access decisions are based on an individual's roles and responsibilities within the organization. For instance, in a corporation, the different roles of users may include those such as chief executive, manager, executive, and clerk. Obviously, these members require different levels of access in order to perform their functions, but also the types of web transactions and their allowed context vary greatly depending on the security policy. In Role Based Access Control, the administrator sets the roles. Therefore, this type of access control is sometimes considered as a subset of MAC.
- **Rule Based Access Control (RBAC):** The access to a resource in Rule Based Access Control is based a set of rules. ACLs (Access Control Lists) are used for this type of access control. In Rule Based Access Control, the administrator sets the rules. Therefore, this type of access control is sometimes considered as a subset of MAC.

Authentication Types:

- **Mutual authentication:** Here both the server and client computers authenticate each other. This type of authentication is more secure than one-way authentication, where only the client is authenticated.
- **Multifactor authentication:** Here two or more number of authentication methods are used for granting access to a resource. Usually, it combines a password with that of a biometric authentication.
- **Biometric authentication:** Biometric authentication uses measurable physical attributes of a human being such as signature, fingerprint. A biometric authentication depends on the physical characteristic of a human being. It is not something that can be remembered. Usually, bio authentication is very secure, though not widely used due to cost constraints. Biometrics is the ability measure physical characteristics of a human such as fingerprints, speech etc. These measured values are then used for authentication purpose. Given below are few of the measurable quantities:
 - i. **Fingerprint:** Scans and matches finger print to a securely stored value.
 - ii. **Voiceprint:** Identifies a person by measuring speech pattern.
 - iii. **Iris profile:** Identifies a person by using Iris part of the eye.
 - iv. **Signature:** Matches an individual's signature with the stored value.
- **CHAP:** It is an authentication type that uses three-way handshake. The p asswords are transmitted in encrypted form ensuring security. Compare this with PAP, which transmits passwords in clear text.

- Least privilege. Least privilege is a technical control. It specifies that individuals or processes are granted only those rights and permissions needed to perform their assigned tasks or functions. Rights and permissions are commonly assigned on servers, but rarely on mobile devices such as tablets and smart-phones.

5.3 Implement appropriate security controls when performing account management

Mitigates issues associated with users with multiple account/roles

An administrator need two accounts one is a standard account which has normal privileges that every other employee has this account should be used to perform every day work (regular work by employee) and other is an administrative account which should be configured to have only special privileges needed to perform assigned administrative function this should not be used to perform regular work.

This forces user to employ the correct account for the task given at hand. This also limits the amount of time the administrative account is in use and prevents it from being used when administrative access is a risk for example when administrator account is used to access internet, open email or for general file transfer.

For users having multiple roles each role should have its own administrative user account. This could mean a user can have single standard account and one or more administrative accounts. This puts extra burden on the user to keep authentication distinct. Use of multifactor authentication will improve security and will prevent single password from being defined for each account.

Account policy enforcement

Passwords used should be strong which consists of eight or more characters which include at least 3 types of characters (uppercase, lowercase, letters, numerals and keyboard symbols) its should not contain common words, users real name, user name or email address. These features can be implemented as a requirement through account policy enforcement

Password Complexity: Password policy contains requirement for minimum password length, maximum password age, minimum password age, password history retention and some sort of complexity requirement. Passwords are considered strong if consists of eight or more characters which include at least 3 types of characters (uppercase, lowercase, letters, numerals and keyboard symbols) its should not contain common words, users real name, user name or email address.

Expiration: Password should automatically expire after a fixed period of time forcing the user to change it. Commonly this duration is 90 days.

Recovery: Password recovery option is not good for security. When a password is forgotten, it should be changed. Ability to recover a password requires that password storage mechanism should be reversible.

Length: Password length is an important factor to determine password strength. Passwords of 7 character can be cracked in with in few hours, 8 to 9 character password can be cracked with in few days to weeks. Passwords of 10 or more characters can tough to crack.

Disablement: Disablement or account expiration is an often unused feature it automatically disables an user account at a specific time on specific day. This features can be used for temporary workers or interns whose employment will expire at a specific known date. These accounts can be re enabled and new expiration date can be set.

Lockout: If a user tries to login into an account with wrong password after a set number of login attempts with wrong password account is locked. This is set as 3 to 5 failed attempts in 15 minutes. Only administrator can unlock the account.

Group Based Privileges

It is assignment of a privileges or access to a resource to all members of a group as a collective. This grants every member of the group the same level of access to specific object. Group based privileges are common in many operating systems including Linux and Windows. Each object has 3 types of permissions those for owner, those for group of the owner, and other users. When using group privileges, it is important to consider whether it violates the principle of least privilege.

6. Cryptography

6.1 Summarize general cryptography concepts

Non-repudiation

Non-repudiation ensures that the sender, as well as the receiver cannot refute having sent or received a message. For example, you receive an email from your perspective employer. By using an unsigned email, it might so happen that your employer later denies having sent any such email. Non-repudiation ensures that neither the sender nor the receiver can deny the transmission or the reception of a message respectively. It prevents either the sender or the receiver of messages from denying having sent or received a message

Digital Signatures and Encryption

- Digital signature ensures that the sender cannot repudiate having sent the message at a future date.
- Encryption ensures that the message cannot be read by any person who do not have matching key to decode the coded message
- Hashing ensures that the message is not tampered with, during transit or storage. Note that Hashing not necessarily encode or encrypt a message.

Secret-key encryption

Secret-key encryption is also known as single-key or symmetric encryption. It involves the use of a single key that is shared by both the sender and the receiver of the message. Typically, the sender encrypts the message with a key and transmits the message to the recipient. The recipient then decrypts it by using a copy of the same key used to encrypt it. The disadvantages of using symmetric encryption over asymmetric encryption are given below:

- Inability to support non-repudiation: Since both the sender and receiver use the same key, it is difficult to determine who is the sender, should a dispute arise.
- Impractical for web commerce: Imagine thousands of customers buying goods and services over the Internet. If symmetric encryption standard is used, one unique private key-pair needs to be used for each user. It is therefore, impractical.
- Another major difficulty is with the transmission of private key. With symmetric encryption, the private key needs to be transmitted to the other party for decryption, which may pose security risk.

6.2 Use and apply appropriate cryptographic tools and products

Hash Algorithms

Hash algorithms produce a hash of a message and encrypt it. They use a mathematical formula for hashing, and it is extremely difficult to tamper with the message and still produce the same hash. Basically, Hashing enable a recipient to check whether a message is received intact without being tampered by a third party.

- SHA (Secure Hashing Algorithms): There are several Secure Hashing Algorithms and they primarily differ in the hash length. They are SHA-1, SHA-256, SHA-384 and SHA-512. In SHA-1 the bit length is 160 bits, in SHA-256 it is 256 bits, for SHA-384, 384 bits and in SHA-512 it is 512 bits.
- MD2, MD4, MD5 (Message Digest Series Algorithms): These are another type of hash algorithms. These algorithms were developed by Rivest. All three algorithms take a message of arbitrary length and produce a 128-bit message digest. MD2 is meant for 8 bit machines and MD4, MD5 are suitable for 32 bit machines. These algorithms are primarily used for digital signature applications.
- CHAP (Challenge Handshake Authentication Protocol) works on point to point connections. It uses a three step process for authentication (excluding making the connection itself). If making the connection is also involved, it would be a 4 step process.

A cryptographic hash function is a "one-way" operation. It is practically not possible to deduce the input data that had produced the output hash.

You can decrypt an encoded message using matching secret key. Similarly, Digital certificate is issued by a CA, and can be decrypted to find the contents of the certificate.

PGP uses public-key encryption for sending and receiving email messages. Diffie-Hellman and RSA algorithms are used for encryption/ decryption of PGP messages.

Encryption Schemes:

- AES (Advanced Encryption Standard) is more secure than DES or 3DES.
- AES is a symmetric block cipher that can encrypt (encipher) or decrypt (decipher) information
- AES is based on Rijndael algorithm
- PGP (Pretty Good Privacy) can use Diffie-Hellman or RSA algorithms, but not AES or DES.

PGP (Pretty Good Privacy)

PGP certificates differ from X.509 certificates in two ways:

- PGP certificates are issued (signed) by normal people while the X.509 certificates must be issued by a professional CA, and
- PGP implements a security fault tolerance mechanism, called the Web of Trust. Here an individual is allowed to sign and issue certificates to people they know

6.3 Explain the core concepts of public key infrastructure

Three basic types of distributed trust models are:

Hierarchical trust model

Here one root CA and one or more subordinate CAs will be present. The subordinate CAs provide redundancy and load balancing. The root CA is usually off-line. Here even if a subordinate CA is compromised, the root CA can revoke the subordinate CA, thus providing redundancy.

Web of Trust

This is also called cross-certification model. Here CAs form peer-to-peer relationship. This model is difficult to manage as the number of CAs grow larger. This kind of trust relationship may happen when different divisions of a company has different CAs, and need to work together. Here CAs must trust one another.

Bridge CA architecture

Bridge CA overcomes the complexity involved with Web of Trust model. Here Bridge CA act as the central co-ordinate point. All other CAs (known as principals) must trust only the Bridge CA.

If the CA's private key is compromised, certificates' private key is compromised, certificates issued by that CA issued by that CA are affected. This will lead to issuance of new certificates to all users, and registration. These problems can be overcome by use of a distributed trust model, in which multiple CAs are involved.

In public key infrastructure

- A key is required to encode/decode a message, and the security of a message depends on the security of key.
- A cipher text is the encoded message, and
- A certificate is a digitally signed document by a trusted authority.

Certificate Revocation List (CRL)

A certificate revocation list (CRL) is a list of certificates, which have been revoked, and are no longer valid. A digital certificate is a credential issued by a trusted authority that binds you (and individual or an organization) to an identity that can be recognized and verified electronically by other agencies. Locally issued digital certificates are valid only within an organizations network (like intranet). Therefore, any secure pages or digital signatures containing local registration will not work on the Internet.

6.4 Implement PKI, certificate management and associated components

Public Key Infrastructure (PKI)

It is a framework for all of the entities involved in digital certificates—including hardware, software, people, policies, and procedures to create, store, distribute, and revoke digital certificates. PKI is essentially digital certificate management.

Recovery agent

It is responsible for recovering lost or damaged digital certificates

Certificate Revocation List (CRL)

A certificate revocation list (CRL) is a list of certificates, which have been revoked, and are no longer valid. A digital certificate is a credential issued by a trusted authority that binds you (and individual or an organization) to an identity that can be recognized and verified electronically by other agencies. Locally

issued digital certificates are valid only within an organizations network (like intranet). Therefore, any secure pages or digital signatures containing local registration will not work on the Internet.

Key escrow

Key escrow refers to a process in which keys are managed by a third party, such as a trusted CA. In key escrow, the private key is split and each half is encrypted. The two halves are sent to the third party, which stores each half in a separate location. A user can then retrieve the two halves, combine them, and use this new copy of the private key for decryption. Key escrow relieves the end user from the worry of losing her private key. The drawback to this system is that after the user has retrieved the two halves of the key and combined them to create a copy of the key, that copy of the key can be vulnerable to attacks.

Trust Models

A trust model refers to the type of trusting relationship that can exist between individuals or entities. In one type of trust model, direct trust, a relationship exists between two individuals because one person knows the other person.

A third-party trust refers to a situation in which two individuals trust each other because each trusts a third party.

There are essentially three PKI trust models that use a CA.

- The hierarchical trust model assigns a single hierarchy with one master CA called the root. This root signs all digital certificate authorities with a single key.
- Distributed trust model has multiple CAs that sign digital certificates. This essentially eliminates the limitations of a hierarchical trust model; the loss of a CA's private key would compromise only those digital certificates for which it had signed, the workload of verifying and signing digital certificates can be distributed, and there is no competition regarding who can perform the functions of a CA
- Bridge Trust Model The bridge trust model is similar to the distributed trust model in that there is no single CA that signs digital certificates. However, with the bridge trust model there is one CA that acts as a "facilitator" to interconnect all other Cas. This facilitator CA does not issue digital certificates; instead, it acts as the hub between hierarchical trust models and distributed trust models.