Unit -1

Q) What are the importance of information protection? Explain with example. Ans) The Importance of Information Protection: Information is an important asset. Information can be classified into different categories. This is typically done in order to control access to the information in different ways, depending on its importance, its sensitivity, and its vulnerability to theft or misuse. For e.g. :U.S. government, uses a five-level classification system that progresses from Unclassified information to Top Secret information (to which only the most trusted people have access). • Organizations classify information in different ways in order to differently manage aspects of its handling, such as labelling, distribution, duplication, , storage, encryption, disposal, and methods of transmission). • Companies may have confidential information, such as research and development plans, manufacturing processes, strategic corporate information, product roadmaps, process descriptions, customer lists and contact information, financial forecasts, and earnings announcements that is intended for internal use on a need-to-know basis. Loss or theft of confidential information could violate the privacy of individuals • Specialized information or secret information may include trade secrets, such as formulas, production details, and other intellectual property, research plans, electronic codes, passwords, and encryption keys. If disclosed, this type of information may severely damage the company's competitive advantage. • A Case Study: Egghead Software was a well-known software retailer who discovered in2000 that Internet attackers might have stolen as many as 3.7 million credit card numbers from its web site, housed offsite at an e-commerce service provider that lacked good security.

Q) Write a note on Threat Vector. Ans) 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.

Write a short note on Network-Layer Attack. Ans) Network-layer attacks attempt to compromise network devices and protocol stacks. These attacks are not as common as application-layer attacks. Network-layer attacks include packet-sniffing and protocol-anomaly exploits. **Packet Sniffing** • Sniffing occurs when an unauthorized third party captures network packets destined for computers other than their own. • Packet sniffing allows the attacker to look at transmitted content and may reveal passwords and confidential data. • In order to use sniffing software, an attacker must have a promiscuous network card and specialized packet driver software, must be connected to the network segment they want to sniff, and must use sniffer software • Packet-sniffing attacks are more common in areas where many computer hosts share the same collision domain or over the Internet where the attacker might insert a sniffer in between source and destination traffic. **Protocol Anomaly Attacks** • A rogue attacker can create malformed network packets that do not follow the intended format and purpose of the protocol, with the result that the attacker is able to either compromise a remote host or network, or able to compromise a confidential network data stream. • Network-layer attacks are most often used to get past firewalls and to cause DoS attacks. • Malformed traffic can be created by tools called packet injectors or traffic generators. • Packet injectors are used by legitimate sources to test the throughput of network devices or to test the security defences of firewalls and IDSs. • There are dozens of commercial and open source packet generators that allow a fair amount of flexibility in generating TCP/IP traffic, permitting different protocols (TCP, UDP, and ICMP), packet sizes, payload contents, packet flow rates, flag settings, and customized header options.

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. 3. Develop 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

Q) Explain three D's of security. Ans) Security is a paradigm, and a wat of thinking. Information security is concerned with protecting information in all its forms, Three Ds of security: Defence, 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 behaviour, training programs to acquaint employees with acceptable usage of company computer systems.

Explain the best practices for network defence. Ans) **Following are the best practices for network defence:** 1. Secure the Physical Environment a. Password protect booting b. Password protect CMOS c. Disable booting from USB & CD 2. Harden the OS: To reduce the attack surface of the operating system by removing unnecessary software, disabling unneeded services, and locking down access. 3. Keep patches updated 4. Use Antivirus scanner: It should be deployed on the computer, with forced, automatic updates, and it should be enabled for real-time protection. 5. Use Firewall software 6. Secure Network share permissions: Folders and files accessed remotely over the network should have discretionary ACLs (DACLs) applied using the principle of least privilege and should have complex passwords 7. Use Encryption: Administrators should use SSH instead of Telnet or FTP to manage their computers 8. Secure Applications: Applications can be managed by configuring application security, installing applications to nonstandard directories and ports, locking down applications, securing P2P services, and making sure your application programmers code securely. a. Securely configure applications b. Securing email c. Blocking dangerous file types d. Blocking outlook file attachments e. Install Applications to Nonstandard Directories and Ports f. Lock Down Applications g. Secure P2P Services 9. Backup the System 10. Implement ARP Poisoning defence: Defences include implementing static ARP tables, configuring port rate limiting, or using DHCP snooping with dynamic ARP inspection (DAI) a. Create computer security defence plan b. Implement static ARP tables c. Configure port late limiting d. Use DHCP Snooping and Dynamic ARP Inspection e. Combine PRL and DAI for the Most Effective Defence.

What is malicious mobile code? Explain the variants of malicious mobile code. Ans) • Malicious mobile code (MMC) is any software program designed to move from computer to computer and network to network, in order to intentionally modify computer systems without the consent of the owner or operator. • The lifecycle of malicious mobile code is as shown in figure: **Three recognized variants of malicious mobile code: viruses, worms, and Trojans 1. Virus** - A virus is a self-replicating program that uses other host files or code to replicate. - Most viruses infect files so that every time the host file is executed, the virus is executed too. - A virus infection is simply another way of saying the virus made a copy of itself (replicated) and placed its code in the host in such a way that it will always be executed when the host is executed. - Viruses can infect program files, boot sectors, hard drive partition tables, data files, memory, macro routines, and scripting files. **2. Worm -** A computer worm uses its own coding to replicate, although it may rely on the existence of other related code to do so. - The key to a worm is that it does not directly modify other host code to replicate. - A worm may travel the Internet trying one or more exploits to compromise a computer, and if successful, it then writes itself to the computer and begins replicating again. **3. Trojan -** Trojan horse programs, or Trojans, work by posing as legitimate programs that are activated by an unsuspecting user. - After execution, the Trojan may attempt to continue to pose as the other legitimate program (such as a screensaver) while doing its malicious actions in the background.

explain the onion model Ans) 1) The Onion Model is a security model that represents the layers of security that can be implemented to protect a computer system or network. 2)The model is called the "onion" because it resembles an onion with multiple layers. 3) Each layer represents a different level of security, and together they form a comprehensive security strategy. 4) The outermost layer represents physical security, which includes measures such as locks, access control systems, and CCTV cameras to protect the physical components of the system or network. 5) The next layer represents network security, which includes firewalls, intrusion detection systems, and other network security measures to protect the network infrastructure from external attacks and unauthorized access. 6)The subsequent layers represent system security, application security, and data security, each with their own set of security measures and protocols. 7) System security includes measures such as authentication and access control to protect individual systems or servers from unauthorized access or attacks. 8) Application security includes measures to secure applications and software running on the system or network, such as encryption, secure coding practices, and input validation. 9) Data security includes measures to protect data from unauthorized access, such as encryption, data backup, and disaster recovery plans. 10) Each layer of the Onion Model builds upon the previous layer to create a comprehensive security strategy. 11) The Onion Model is a useful tool for understanding the different layers of security and how they work together to protect a computer system or network.

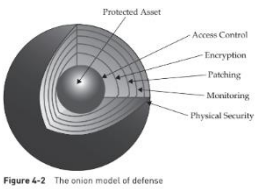

Figure 4-2 The onion model of defense

Q) Explain the statement that "Achieving 100 percent protection against all conceivable attacks is an impossible job." Ans) ➢ 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. ➢ E.g.: 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 defences. ➢ 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 defence, transference is the process of insurance, and acceptance is deciding that the risk does not require any action.

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:** These occur when a program expecting input does not do input validation. For eg: suppose the program was expecting the user to type in a five-digit ZIP code, but instead the attacker replies with 400 characters. The result makes the host program error out and quit, throwing excess data into the CPU. If the buffer overflow attacker can reliably predict where in memory his buffer overflow data is going, the buffer overflow can be used to completely compromise the host. **Password cracking attempts:** 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). If the attacked system locks out accounts after a certain number of invalid login attempts, some password attackers will gain enough access to copy down the password database, and then brute-force it offline

Unit 2

Explain public key Cryptography and its infrastructure in brief.
Ans) **Public Key Cryptography** ➢ This algorithm is asymmetric—it uses a set of related keys. If one key is used to encrypt the message, the other is used to decrypt it, and vice versa. This means that if each party holds one of the keys. ➢ Session key can be securely exchanged. Each party has their own set of these asymmetric keys. One of the key pairs is known as the private key and the other as the public key. Public keys are exchanged and private keys are kept secret. ➢ Public key is meant to be shared openly. It is used to create digital signatures. ➢These algorithms traditionally use very large keys, and while you could use public key cryptography to encrypt whole messages or blocks of data on a disk, the process is remarkably slow compared to symmetric-key cryptography. **Key Exchange** ➢ Public/private key pairs can be used to exchange session keys. The public keys are either exchanged among the parties or kept in a database. The private keys are kept secret. ➢When it is necessary to exchange a key, one party can encrypt it using the public key of the other. The encrypted key is then transmitted to the other party. ➢Since only the intended recipient holds the private key that is related to the public key used to encrypt the session key, only that party can decrypt the session key.

Q) Explain the authorization systems. And it's various types.
Ans) **Authorization:** ➢ Authorization determines what they're allowed to do. This should always be done in accordance with the principle of least privilege—giving each person only the amount of access they require to be effective in their job function. ➢ There are a variety of types of authorization systems, including user rights, role-based authorization, access control lists, and rule-based authorization. **User Rights** -Privileges or user rights are different from permissions. User rights provide the authorization to do things that affect the entire system. The ability to create groups, assign users to groups, log in to a system etc. Other user rights are implicit and are rights that are granted to default groups—groups that are created by the operating system instead of by administrators. These rights cannot be removed. **Role-Based Authorization (RBAC)** - Each job within a company has a role to play. Each employee requires privileges (the right to do something) and permissions (the right to access particular resources and do specified things with them) if they are to do their job. **Access Control Lists (ACLs)-** Attendance at some social events is limited to invitees only. To ensure that only invited guests are welcomed to the party, a list of authorized individuals may be provided to those who permit the guests in. If you arrive, the name you provide is checked against this list, and entry is granted or denied. Information systems may also use ACLs to determine whether the requested service or resource is authorized. Access to files on a server is often controlled by information that is maintained on each file**. ACLs for Network Devices-**ACLs are used by network devices to control access to networks and to Rule-Based Authorization**. Rule-Based Authorization**- Rule-based authorization requires the development of rules that stipulate what a specific user can do on a system. These rules might provide information such as "User A can access resource Z but cannot access resource D."

Q) Define authentication. Explain parts of authentication. Ans) ➢ Authentication is the process by which people prove who they are. It's composed of two parts: a public statement of identity (usually in the form of a username) combined with a private response to a challenge (such as a password). ➢ A password by itself, which is a means of identifying yourself through something you should know, is an example of single-factor authentication. Multifactor authentication refers to using two or more methods of checking identity. ➢The following types of password authentication systems are commonly used today: **Local storage and comparison** • They create and manage their own stored-password file and do no encryption. • Security relies on the protection of the password file. Because passwords can be intercepted by rogue software, these systems are not well protected **Central storage and comparison** • The password entered by the user is encrypted, passed over the network in this state, and then compared by the remote server to its stored encrypted password. • Hash function (code) used for encryption. A hash is one-way code, which means you can create it, but not reverse it. It's like being able to encrypt something without being able to decrypt it. When one computer creates a hash, another computer can use exactly the same inputs to create another hash, and compare the two. If they match, the inputs are the same **• Challenge and response** • Two algorithms are used - CHAP & MS-CHAP • CHAP: The server that receives the request for access issues a challenge code, and the requestor responds with an MD5 hash of the code and password. The server then compares that hash to its own hash made from the same code and password. If they are the same, the user is authenticated • MS-CHAP: requires mutual authentication—the user must authenticate to the server, and the server must also prove its identity. To do so, the server encrypts a challenge sent by the client. Since the server uses the client's password to do so, and only a server that holds the account database in which the client has a password could do so, the client is also assured that it is talking to a valid remote access server **• Kerberos** • a network authentication system based on the use of tickets **• One-time password (OTP)** • Two current methods that use one-time passwords are time-based keys and sequential keys

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. ➢ 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.

Write a note on symmetric key cryptography. Ans**) Symmetric key cryptography:** ➢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. **Key exchange in symmetric key cryptography:** ➢All algorithms in symmetric key cryptography use a single, secret key. ➢This key is used to encrypt the data, and the same key, or a copy of it, is used to decrypt the data. This key may be used to produce other keys, but the principle is the same. ➢Symmetric-key encryption can use either stream ciphers or block ciphers **• Stream Cipher:** ➢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. ➢Works on one character at a time. Programmatic stream ciphers use a key to produce a key table, and then a byte of the key table and a byte of plaintext (text that is not encrypted) are XORed. ➢The key table is remixed and a new byte of the table is XORed with the next byte of the plaintext message. When the entire message has been thus encrypted to produce ciphertext, it is delivered **• Block 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. ➢Works on a block of many bits at a time. A nonlinear Boolean function is used. ➢Unlike stream ciphers, early block ciphers did not vary the key, which made the results easier to break because encrypting the same combinations of letters resulted in the same ciphertext. Frequency analysis could effectively be used to break the code.

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. ➢ 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.

Q) Explain certificate-based authentication in detail. Ans) **Certificate:** 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 where more information about the authority that issued the certificate may be found. The certificate is digitally signed by the issuing authority, the certificate authority (CA). **Certificate Authentication: •** When certificates are used for authentication, the private key is used to encrypt or digitally sign some request or challenge. • The related public key (available from the certificate) can be used by the server or a central authentication server to decrypt the request. • If the result matches what is expected, then proof of identity is obtained. • Since the related public key can successfully decrypt the challenge, and only the identity to which the private key belongs can have the private key that encrypted the challenge, the message must come from the identity**. The authentication steps are as follows:** 1. The client issues an authentication request. 2. A challenge is issued by the server. 3. The 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

Explain Database-Level security. Ans) 1) **Definition:** Database-level security refers to a set of controls and measures that are put in place to protect the database management system and the data stored in it from unauthorized access, modification, or disclosure. 2) **Key elements:** Database-level security includes several key elements, such as authentication, authorization, encryption, access control, and audit logging. 3) **Authentication:** Authentication is the process of verifying the identity of a user who is trying to access the database. This can be done through various means such as passwords, biometrics, or multi-factor authentication. 4)**Authorization:** Authorization determines what actions a user is permitted to perform within the database. This includes creating, modifying, or deleting records, running queries, or viewing sensitive data. 5) **Encryption**: Encryption is the process of converting data into a format that can only be read by authorized users. It can be used to protect data both while it is stored in the database and when it is transmitted over a network. 6)**Access control:** Access control is the process of restricting access to the database based on the user's role or level of clearance. This can be achieved by setting up user groups with specific permissions or using firewalls and other network security measures.7)**Audit logging:** Audit logging involves recording all activity within the database, including who accessed what data and when. It can be used to identify suspicious activity or track changes made to the database over time. 8)**Importance:** Database-level security is essential for protecting sensitive data and ensuring the confidentiality, integrity, and availability of the database management system. By implementing effective security controls, organizations can reduce the risk of data breaches, unauthorized access, and other security threats.

Unit 3

Explain the Cisco Hierarchical Internetworking model. Ans) The Cisco three-tier model is derived from the Public Switched Telephone Network (PSTN) model, which is in use for much of the world's telephone infrastructure. The Cisco Hierarchical Internetworking model, depicted in Figure, uses three main layers - core, distribution, and access layers. • **Core layer**:Forms the network backbone and is focused on moving data as fast as possible between distribution layers. it should not be used to perform CPU-intensive operations such as filtering, compressing, encrypting, or translating network addresses for traffic. • **Distribution layer**: Sits between the core and the access layer. This layer is used to aggregate access-layer traffic for transmission into and out of the core. • **Access layer**: Composed of the user networking connections. • Filtering, compressing, encrypting, and address-translating operations should be performed at the access and distribution layers. The Cisco model is highly scalable. As the network grows, additional distribution and access layers can be added. This model assists in higher levels of availability by allowing implementation of redundant hardware at the distribution and core layers.

Explain Network Address Translation (NAT) with its types.
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. ➢ The most common use of static NAT is to provide Internet access to a trusted host **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 intended by RFC 1918 is accomplished by overlapping this address space. ➢Dynamic NAT is usually implemented by simply creating static NATs when an inside host sends a packet through the firewall. ➢The NAT is then maintained in the firewall tables until some event causes it to be terminated.

Q) Explain the features of firewall. Ans) **Firewall**: 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. **Features of firewall**: • **Application Awareness:** The firewall must be able to process and interpret traffic at least from OSI layers three through seven. At layer three, it should be able to filter by IP address; at layer four by port; at layer five by network sessions; at layer six by data type, and, most significantly, at layer seven to properly manage the communications between applications. • **Accurate Application Fingerprinting:** The firewall should be able to correctly identify applications, not just based on their outward appearance, but by the internal contents of their network communications as well. Correct application identification is necessary to ensure that all applications are properly covered by the firewall policy configuration**. • Granular Application:** Control In addition to allowing or denying the communication among applications, the firewall also needs to be able to identify and characterize the features of applications so they can be managed appropriately. File transfer, desktop sharing, voice and video, and in-application games are examples of potentially unwanted features that the firewall should be able to control. • **Bandwidth Management (QoS):** The Quality of Service (QoS) of preferred applications, which might include Voice over IP (VoIP) for example, can be managed through the firewall based on real-time network bandwidth availability. If a sporting event is broadcast live via streaming video on a popular web site, your firewall should be able to proactively limit or block access so all those people who want to watch it don't bring down your network. The firewall should integrate with other network devices to ensure the highest possible availability for the most critical services

What is a firewall? List its strengths and weaknesses. Ans) Firewall: 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. **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.

Explain network availability and security. Ans) **Network Availability:** • Network availability requires that systems are appropriately resilient and available to users on a timely basis (meaning, when users require them). • The opposite of availability is denial of service, which is when users cannot access the resources they need on a timely basis. • Denial of service can be intentional (for example, the act of malicious individuals) or accidental (such as when hardware or software fails). • Unavailable systems result in• Loss of revenue• Reduced employee productivity• Loss of consumer confidence• Negative publicity • The best practice for ensuring availability is to avoid single points of failure within the architecture. This can require redundant and/or failover capabilities at the hardware, network, and application functions. **Network Security:** • When designing and implementing security in network and system architectures, it is helpful to identify critical security controls and understand the consequences of a failure in those controls • **Firewalls** • protect hosts by limiting what services users can connect to on a given system • can allow different sets of users selective access to different services • simply restricting users to specific services may be insufficient to achieve the desired level of security • Flaws, such as a buffer overflows, can allow an attacker to turn a vulnerable server into a conduit through the firewall

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. ➢ In case of outbound filtering, web access considerations and outbound port filtering has to be considered. **Web Access Considerations:** ➢ It is possible to prevent direct connections between internal and external users via proxy services or web filtering. ➢ Proxy servers can be configured to block connections to URLs that are considered likely to be malicious or unnecessary for normal operation, such as those containing certain scripts or other executable files. ➢ Web filtering today can be handled via a variety of specialized products and appliances, including some cloud-based offerings. 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.

What are the countermeasures against the possible abuse of wireless LAN. These countermeasures include: a. Secure replacements for WEP b. Proper wireless user authentication c. Intrusion detection and anomaly tracking on wireless LANs **Temporal Key Integrity Protocol and Counter Mode with CBC-MAC Protocol** The Temporal Key Integrity Protocol (TKIP) and the Counter Mode with CBC-MAC Protocol (CCMP) are WPA2 encryption protocols on 802.11 LANs. TKIP encrypts each data packet with a unique encryption key. To increase key strength, TKIP includes four additional algorithms: A cryptographic message integrity check to protect packets. An initialization-vector (IV) sequencing mechanism that includes hashing. A per-packet key-mixing function to increase cryptographic strength. A rekeying mechanism to provide key generation every 10,000 packets**. 802.1x-Based Authentication and EAP Methods** 802.1x can also be used for the dynamic distribution of WEP keys. An association between the wireless client and the access point is assumed to be a network access port. 802.1x, the wireless client is defined as a supplicant (or peer), and the access point, as an authenticator an authentication server is needed on the wired network segment to which the access point is connected. This service is usually provided by a RADIUS server supplied with some form of user database, such as native RADIUS, LDAP, NDS, or Active Directory. Wireless gateways can implement the authentication server, as well as the authenticator functionality User authentication in 802.1x relies on the layer two Extensible Authentication Protocol. EAP frame exchange between the supplicant, authenticator, and authentication server is summarized. **Wireless Intrusion Detection and Prevention** Wireless IPS identifies wireless attacks using wireless sensors. These wireless sensors typically use the same Wi-Fi radios that are found in access points, Wireless IDS involves receiving packets only. Its coverage is, therefore, more physically broad compared to an access point, which transmits and receives. In a typical access point and sensor use, the rule of thumb is one sensor for every three access points.

Explain the five different types of wireless attacks. Ans) Five types of wireless attacks: **1. Rogue (harmful) Access Points (AP) -** ➢ Rogue AP is an unsanctioned wireless access point connected to the physical network. ➢ It involves a user who brings a consumer-grade access point like a Linksys router into the office. Many organizations attempt to detect rogue APs through wireless assessments. ➢ It is important to validate if they are connected to the physical network. 2. **Wired Side Leakage** ➢ On wireless networks, investigation involves promiscuously listening for wireless packets using a wireless sniffer so the attacker can begin to develop a footprint of the wireless network. ➢ If the attacker were associated to an access point, then he or she could sniff layer three and above. ➢ Most access points and wireless switches allow this traffic to leak into the airspace without being blocked. Figure illustrates this concept with a network device that is connected to an AP via a wired network, leaking internal protocol communications onto the airwaves. ➢ This traffic may reveal network topology, device types, usernames, and even passwords. **3. Misconfigured Access Points** ➢ Human error coupled with different administrators installing the access points and switches can lead to a variety of misconfigurations. ➢ For example, an unsaved configuration change can allow a device to return to its factory default setting the device reboots during a power outage. ➢ These devices must be monitored for configurations that are in line with policies. **4. Wireless Phishing** ➢ Users may unknowingly connect to a wireless network that they believe is the legitimate access point. ➢ But that has, in fact, been set up as a honeypot or open network specifically to attract unsuspecting victims. ➢ For example, they may have a network at home called "Linksys." As a result, their laptop may automatically connect to any other network known as "Linksys." **5. Client Isolation** ➢ Most users connect to the access point to obtain Internet access or access to the corporate network, but they can also fall victim to a malicious user of that same wireless network. ➢ In addition to eavesdropping, a malicious user can also directly target other users as long as they're associated to the same access point. once a user authenticates and associates to the access point, he or she obtains an IP address and, therefore, layer three access.

Q) / Write a short note on hubs and switches. 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. **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. **Routers** ➢Routers are network layer devices and are particularly identified as Layer- 3 devices of the OSI Model. ➢They process logical addressing information in the Network header of a packet such as IP Addresses. ➢Router is used to create larger complex networks by complex traffic routing. It has the ability to connect dissimilar LANs on the same protocol. ➢It also has the ability to limit the flow of broadcasts. A router primarily comprises of a hardware device or a system of the computer which has more than one network interface and routing software. ➢When a router receives the data, it determines the destination address by reading the header of the packet. ➢Once the address is determined, it searches in its routing table to get know how to reach the destination and then forwards the packet to the higher hop on the route.

Unit 4

Write a note on H.323 protocol that includes: i) Governing Standard , ii) Purpose iii) Function iv) Known Compromises and Vulnerabilities v) Recommendations Ans) **Governing Standard H.323:** It is itself a "standard" currently in ITU-T revision 7 (H.323 v7). It is a component of the "H-series" ITU-T recommendations for Audiovisual and Multimedia Systems specifically addressing systems and terminal equipment for audiovisual services. The overall H-series recommendations cover a wide variety of different aspects of multimedia networking**. 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. **Function:** H.323 entities may be integrated into PCs or implemented in standalone devices (videoconferencing codecs, IP cameras, MCUs, for example) and support many types of networks and internetworking, including point-to-point, multipoint, broadcast, or multi-access networks. H.323 is the most commonly used approach for videoconferencing over IP. **Known Compromises and Vulnerabilities:** The most common and impacting types of H.323 vulnerabilities are DoS, DDoS, flooding, Gateway compromises (probably the most common, relevant, dangerous, and potentially damaging from a risk perspective), Remote code execution and arbitrary code execution **Recommendations:** Turn it off if it is not being used. Many devices are shipped with this protocol enabled for convenience, so leaving H.323 enabled on an Internet-facing gateway can lead to disaster

Explain different classic security models. Ans) The different classic security models are: **Bell-LaPadula:** One of the first attempts to formalize an information security model. It was designed to prevent users and processes from reading above their security level. This is used within a data classification system—so a given classification cannot read data associated with a higher classification—as it focuses on sensitivity of data according to classification levels. This model prevents objects and processes with any given classification from modifying data **Biba:** It focuses on integrity labels, rather than sensitivity and data classification. (BellLaPadula was designed to keep secrets, not to protect data integrity). It attempts to preserve the first goal of integrity, namely to prevent unauthorized users from modifying data. **Clark-Wilson:** It attempts to define a security model based on accepted business practices for transaction processing. It is much more real-world-oriented and articulates the concept of well-formed transactions that perform steps in order, perform exactly the steps listed, and authenticate the individuals who perform the steps **TCSEC:** It was developed to meet three objectives: - To give users a yardstick for assessing how much they can trust computer systems for the secure processing of classified or other sensitive information - To guide manufacturers in what to build into their new, widely available commercial products to satisfy trust requirements for sensitive applications - To provide a basis for specifying security requirements for software and hardware acquisitions **Labels:** TCSEC makes heavy use of the concept of labels. Labels are simply security-related information that has been associated with objects such as files, processes, or devices. The ability to associate security labels with system objects is also under security control. Sensitivity labels, used to define the level of data classification, are composed of a sensitivity level and possibly some number of sensitivity categories. The number of sensitivity levels available is dependent on the specific operating system. The sensitivity labels identify whether a user is cleared to view certain information, integrity labels identify whether data is reliable enough for a specific user to see

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.

Write a short note on trustworthy computing. Ans)Trustworthy Computing**. The four goals of the Trustworthy Computing initiative are : Security:** As a customer, you can expect to withstand attack. In addition, you can expect the data is protected to prevent availability problems and corruption. **Privacy:** You have the ability to control information about yourself and maintain privacy of data sent across the network. **Reliability:** When you need your system or data, they are available. **Business integrity:** The vendor of a product acts in a timely and responsible manner, releasing security updates when vulnerability is found. Trustworthy Computing initiative, Microsoft created a framework to explain its objectives: its products be secure by design, secure by default, and secure in deployment, it provide communications (SD3+C). Secure by design means all vulnerabilities are resolved prior to shipping the product. **Secure by design requires three steps**. 1. Build a secure architecture. Software needs to be designed with security and features. 2. Add security features. Feature sets need to be added to deal with new security vulnerabilities. 3. Reduce the number of vulnerabilities in new and existing code.

List and explain steps to a successful IPS Deployment Plan.
Ans)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, reporting, alerting, and logging. 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.

Explain network-based intrusion detection system in detail Ans) **Network-Based IDS (NIDS) -**are the most popular IDSs, and they work by capturing and analyzing network packets on the wire. NIDS is designed to protect more than one host. It can protect a group of computer hosts, or monitor an entire network. Captured traffic is compared against protocol specifications and normal traffic trends or the packet's payload data is examined for malicious content. ➢ If a security threat is noted, the event is logged and an alert is generated. NIDS works by examining network packet traffic, including traffic not intended for the NIDS host on the network. ➢ 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

What are the components of Voice Over IP? Explain. Ans: **Components of a modern enterprise IP-based phone or video system are**: • **Call control elements (call agents)** • Appliance or server-based call control—Internet protocol private branch exchange (IPPBX) • Soft switches • Session border controllers (SBCs) • Proxies • **Gateways and gatekeepers** □• Dial peers • **Multi-conference units (MCUs) and specialized conference bridges** • **Hardware endpoints** • Phones • Video codecs • Other devices and specialized endpoints • **Soft clients and software endpoints** • IP phones • Unified messaging (UM) integrated chat and voice clients • Desktop video clients • IP-based smartphone clients • **Contact center components** • Automated call distribution (ACD) and interactive voice response (IVR) systems • Call center integrations and outbound dialers • Call recording systems • Call center workflow solutions • **Voicemail systems**

Write a short note on Private Bank Exchange. 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.

Explain the role and functionality of 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:** Multiple extensions Voicemail Call forwarding Fax management Remote control (for support) A Hosted PBX also known as a Virtual PBX, have same functionality and features, but the switching is located a central location and only the phones are at the customer site**. PBX has the following roles:** • To ensure that resources are kept in order to keep connections in the same place. To create connections by acting as a switch between telephone users. • To record any data associated with a call, such as quantities, call volume, metering and statistics. • To correctly terminate a call once one of the users hang up the phone. **Functions of a PBX** • It allows a company to have one single phone number that people can use to contact a number of different internal representatives. It uses an automatic call distribution (ACD) feature, which allows calls to be distributed evenly amongst the various employees of an answering team. • It can provide automated call answers and provide anyone calling in with a number of menu options that'll be used to select which department or extension they want to go to on their own. • It allows for automated greetings that are customizable. • It provides a host of management features. It allows providing custom music to callers that are on hold while waiting for an internal employee to answer. • It can be used to record separate voice messages for each extension. • It allows internal calls to be made in between stations. **Hacking a PBX:** • Attackers hack PBXs for several reasons • To gain access to the confidential information. To place outgoing calls that are charged to the organization's account. • To cause damages by crashing the PBX.

What are the components of Voice Over IP? Explain VoIP Components Ans) 1. Call Control The call control element (the "brains" of the operation) of a VoIP system can be either an appliance, a piece of software that runs on a specialized server operating system, or a piece of network hardware embedded into another networking component. There are special types of call control elements such as session border controllers (SBCs) and voice proxies that are designed to be exposed to or interface with systems under a different administrative domain. 2. Voice and Media Gateways and Gatekeepers Gateways are configured to use dial peers (defined as "addressable endpoints") to originate and receive calls. Some gateways are directly managed by the call control elements via a control protocol (MGCP or H.248), whereas others operate in a more independent, stand-alone capacity (H.323 or SIP). Voice gateways can also run soft switches and perform primary (or survivable) call processing or "all-in-one" functions. 3. MCUs The Conference Bridge, or multi-conference unit (MCU), a multiport bridging system for audio, video, and multimedia collaboration. Conferencing and collaboration is used extensively within and across all enterprises as part of the fundamental communications capability that connects all users to each other. A problem with an MCU can affect a lot of users at once. Like gateways, MCUs are frequently exposed to the outside world, and are commonly used by everyone in the organization up through executive level. MCUs can connect different types of media; require those facilities to be secured

Write short note on Security Information and Event Management(SIEM). Ans) Multiple security systems can report to a centralized Security Information and Event Management (SIEM) system, bringing together logs and alerts from several disparate sources. "Security Incident and Event Management" or "Security Incident and Event Monitoring."—a technology to collect, analyzes, and correlates events and alerts generated by monitoring systems. SIEM platforms take the log files, find commonalities (such as attack types and threat origination), and summarize the results for a particular time period. For example, all logs and alerts from all IDSs, perimeter firewalls, personal firewalls, antivirus scanners, and operating systems can be tied together. SIEM can significantly reduce false positives by verifying information based on other data. That data comes from many sources, including workstations, servers, computing infrastructure, databases, applications, network devices, and security systems. SIEM products need to be fast and effective, with a significant amount of storage and computing power. **SIEM can do the following: 1.Data Aggregation** SIEMs collect information from every available source that is relevant to a security event. These sources take the form of alerts, real-time data, logs, and supporting data. These provide the correlation engine of the SIEM with information it can use to make decisions about what to bring to the security administrator's attention. **2. Alerts** The SIEM's key function is to validate security alerts using many different sources of data to reduce false positives, so only the most reliable alerts get sent on to the security administrator. **3. Real-Time Data** Real-time data such as network flow data gives the SIEM additional information to correlate. Streaming this data into the SIEM provides important information about normal and abnormal traffic patterns that can be used in conjunction with alerts to determine whether an attack is in progress**. 4.Logs Logs** are different from events, in that they are a normal part of system activity and meant for debugging purposes. Logs contain valuable information about what's happening on a system. For example, login failures that may otherwise go unnoticed by a system administrator especially if there are many login failures for a single account, if there are login failures on many different accounts**. 5. Supporting Data** Data can be imported into the SIEM, and it will use that data to make comparative determinations. For example, asset management data containing names, IP addresses, operating systems, and software versions gives the SIEM valuable information it can use to determine whether an IDS alert makes sense within the context of the software environment.

UNIT 5

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.

Explain the reasons for remote administration security. What are the advantages of web remote administration? Ans) Reasons for Remote Administration. Remote administration is needed for various reasons: **Relocated servers** An administrator needs an interface to administer any relocated web servers**. Outsourced services** Managing security products requires knowledge that some organizations don't possess, so they often outsource their entire security management to a firm specializing in that area. **Physical distance** An administrator may need to manage a large number of computers in the organization. Some organizations span several buildings (or cities), and physically attending the computers can be a tedious and time-consuming task. Additionally, physical access may be limited to the actual data centres**. Advantages of remote web administration:** - Quick development time - Developing a web interface is faster than developing a GUI client, in terms of development, debugging, and deployment. - OS support - A web interface can be accessed from all the major OSs by using a browser **Accessibility** A web interface can be accessed from any location on the Internet**. User learning curve** An administrator knows how to use a browser, so the learning curve for the administrator will be shorter. **Accessibility** Because web administration is accessible from anywhere on the Internet, it's also accessible to an attacker who may try to hack it. **Browser control** Because a browser controls the interface, an attacker doesn't need to deploy a specific product control GUI. **Support** Web-based applications are typically easier to support and maintain. **Authenticating Web-Based Remote Administration** When connecting to the remote web administration interface, the first hurdle to clear is the authentication process. If the authentication is weak, an attacker can bypass it and take control of the application or computer. **HTTP Authentication Methods** it's important to go over the current methods available to authenticate HTTP connections: **Securing Web-Based Remote Administration** The best solution for securely logging in to a web-administered server is to use either SSL, which checks for client certificates, or encrypted basic authentication. (SSL can also authenticate the server against a third-party certificate authority to ensure it is the server you meant to connect to.)

State and explain the types of cloud services. Ans) **Types of Cloud Services: Infrastructure-as-a-Service (IaaS):** 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):** Delivers a single application through the browser to customers **Utility computing:** Companies that offer storage and virtual servers that IT can access on demand **Platform-as-a-Service (PaaS):** Delivers development environments as a service. You build your own applications that run on the provider's infrastructure and are delivered to your users via the Internet from the provider's servers. **Web services in the Cloud:** Web service providers 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: The integration of cloud-based services mainly serving SaaS providers using inthe-cloud integration technology.

Write a note on Custom Remote Administration Ans) Some applications are controlled remotely via a GUI or through console applications, such as SQL Server, Exchange Server, firewalls, and intrusion detection systems (IDSs). An application may also control clients with probes, as an IDS does**. Advantages: • 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 (and accessing or installing it may not be possible). **Disadvantages: •** 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 (this may involve additional costs if the OS is not free). • 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. In case of custom remote administration, following things should be considered: **Session Security:** It's important that the session between the client (GUI or console) and the application be secure. **Authentication:** It's important that authentication take place and that it isn't based upon easily forged assumptions, like the IP or MAC address of the computer. The sequence of the authentication process is also critical. **Using OS Networking Services:** Some applications use OS networking services, such as remote procedure calls (RPC) or Distributed Component Object Model (DCOM), which allows the administrator to add data integrity, encryption, and authentication. If you don't trust the OS security measures, you can tunnel the network connection through a VPN connection

Explain the classification of Corporate Physical Assets Ans) The classification of corporate physical assets will generally fall under the following categories: **• 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:** Many older systems use storage media devices like magnetic tapes, DATs, CD-ROMs, and Zip drives, so it is still good to be familiar with them. Most systems today use 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, to name a few. **Furniture and fixtures:** Racks, NEMA-rated enclosures, etc. **Assets with direct monetary value:** Cash, jewelry, bonds, stocks, credit cards, personal data, cell phones, etc.

Explain the risk and remediation of cloud computing.
Ans) **CLOUD COMPUTING**: Cloud computing helps in sharing services such as servers, storage, databases, networking, software, analytics, and intelligence over the Internet. It is an emerging style of computing in which applications, data and resources are provided as service to users over the Internet where information is stored on physical servers maintained and controlled by a cloud computing provider. Cloud **Computing Risks and Remediation:** The issues and concerns of integrating the data center and the cloud raises are: • **Availability:** Cloud services are made available as the availability of the services is important for the client but as the services are accessed over the Internet, it is assumed that the service will eventually fail and continuity becomes important. Therefore, SLAs are published by the cloud providers. • **Patriot Act ramifications:** The U.S. government monitors data under its control from a service provider on demand regardless of the customer's knowledge or objections. • **Compliance ramifications:** Cloud services are restricted by some of the government regulations. • PCI compliance: It specifies exactly where and on what physical server the data resides. • **Migration:** Physical-to-cloud and cloud-to-physical capability is required to move data into the cloud from client local or vice versa. • **Confidentiality:** The responsibility for controlling data in a cloud environment is shared between the cloud provider and the customer and isolating data is effective depending upon the virtualization practices. So, private data should be stored in a private cloud not in a public cloud.

What is cloud computing? Explain the types of cloud services. Cloud computing provides a way to increase capacity or add capabilities, training new personnel, or licensing new software cloud service providers have experienced full service outages, performance issues, and various types of security breaches. Cloud providers are well-suited for large file-size content, with lots of read access, such as digital content and streaming media, video, and music, as well as for long-term file storage, such as data backups and data archives. **Types of Cloud Services: The types of services /"cloud" associated :** Infrastructure-as-a-Service (IaaS) -This type of service allows consumers to provision processing, storage, and networking resources, allowing them to deploy and run their own operating systems or applications in their own cloud environment. **Software-as-a-Service (SaaS) -** This type of cloud computing delivers a single application through the browser to customers using a multitenant architecture. Utility computing - Companies that offer storage and virtual servers that IT can access on demand. Enterprise adopters use utility computing for supplemental, non-mission-critical needs. **Platform-as-a-Service (PaaS) -** This form of cloud computing delivers development environments as a service. Build your own applications that run on the provider's infrastructure and are delivered to your users. **Web services in the Cloud -** It offer APIs that enable developers to exploit functionality over the Internet, rather than delivering full-blown applications. **Managed service providers (MSP) -** It is basically an application exposed to IT rather than to end users. Examples include virus scanning services, e-mail spam filtering services, application monitoring services, and managed security services.

Define virtual machine. How is hypervisor responsible for managing all guest OS installations on a VM server? In a virtual machine (VM), the OS (referred to as a "guest OS" when virtualized) and the software applications that it hosts run on virtual hardware. In a virtualized environment, everything is software—therefore, the risks are greater. Virtual machines carry their own security risks, unique from those of computer systems and local area networks. **Protecting Virtual Storage** Guest OS systems can utilize virtual or physical network attached storage (NAS) and storage area networks (SAN) allocated by the hypervisor to meet data storage requirements, as if these storage devices were directly attached to the system. **Protecting the Hypervisor** The hypervisor is responsible for managing all guest OS installations on a VM server, and the service console provides a centralized location for managing all the servers in a virtual environment. Hypervisor and service console servers need to be properly patched and secured, as well as logically separated through the use of isolated networks with strict access controls. **Protecting the Guest OS** Hypervisor manages access to hardware resources so that each guest OS is able to access only its own allocated resources, such as CPU, memory, and storage, but not those resources allocated to other guest OSs. This characteristic is known as partitioning and is designed to protect each guest OS from other guest OS instances, so attacks and malware are unable to "cross over." Partitioning also reduces the threat of side-channel attacks that take advantage of hardware usage characteristics to crack encryption algorithms or implementations. Partitioning, therefore, is considered an important security measure. If an attacker attempts to "break out" of a guest OS to access the hypervisor or 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 the hypervisor's entire guest OSs. The hypervisor monitors and tracks the state of its guest OSs, which is a function commonly, referred to as introspection. Introspection can be integrated with intrusion detection systems (IDS) or intrusion prevention systems (IPS) and security information and event management (SIEM). **Protecting Virtual Networks** The hypervisor can present the guest OS with either physical or virtual network interfaces. hypervisors provides three choices for network configurations: **Network bridging** The guest OS has directs access to the actual physical network interface cards (NIC) of the real server hardware. **Network Address Translation (NAT)** The guest OS has virtual access to a simulated physical NIC that is connected to a NAT emulator by the hypervisor. As in a traditional NAT, all outbound network traffic is sent through the virtual NIC to the underlying subsystem to get routed to the main network, or directly to other guest OSs. **Host-only networking** A guest OS has virtual access to a virtual NIC that does not actually route to any physical NIC. Network packets are translated by the hypervisor from one guest OS to another without any physical network connectivity.

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. Rolespecific 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.

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.

Explain different parameters of security consideration for physical intrusion detection. Ans) **PHYSICAL INTRUSION DETECTION:** Security considerations for physical intrusion detection are discussed in the following sections. **Closed-Circuit Television:** ➢ CCTV is in now a days used everywhere. Placement of CCTV devices should be planned out keeping in mind financial and operational limitations. ➢ Some probable areas for placing a CCTV include: high-traffic areas, critical function areas (such as parking structures, loading docks, and research areas), cash handling areas, and areas of transition (such as the hallway leading from a conference room to a sensitive location), entry, and exit point to the enclosures. ➢ It should be warranted that the cabling used for CCTV devices is not readily accessible, so that no one can easily tap into transmissions or tamper the device to stop or block the process. ➢ Lighting in the area also play a critical role in the effectiveness of the camera capturing the footage. ➢ In case of Wireless CCTV setup, users should take into account that anything transmitted through airwaves is also meant to be received, and can be intercepted easily thorough hackers. **Alarms:** ➢ Alarms should be tested at least monthly, and a test log should be kept. ➢ Points of entry and exit should be fitted with intrusion alarms. ➢ A response plan should be in effect, and everyone who will be responding to an incident must know exactly what their roles and responsibilities are. ➢ Threat alarms should also be taken into consideration for areas that may require them.

What are cloud computing security benefits? Ans) **CLOUD COMPUTING:** Cloud computing helps in sharing services such as servers, storage, databases, networking, software, analytics, and intelligence over the Internet. It is an emerging style of computing in which applications, data and resources are provided as service to users over the Internet where information is stored on physical servers maintained and controlled by a cloud computing provider. **Cloud Computing Security Benefits:** The cloud computing benefits are: • **Centralized data:** Cloud computing helps data to be available centrally as data loss can be reduced from laptop and backup tape. • **Monitoring:** It is easier to control and monitor the central data. • **Forensics and incident response:** A dedicated forensic server can be built in the same cloud with laaS providers as the corporate servers but can be made available offline, ready to be used and brought online as required which helps in reducing procurement time by providing immediate analysis. • **Password assurance testing:** For organizations that routinely crack passwords to check for weaknesses, password cracking times can be significantly decreased • **Logging:** As it provides unlimited storage for logging which decreases the concern about insufficient space allocated for system logging. • **Testing security changes:** The implementation of updates and patches becomes easier using a cloned copy of the production server with low-cost impact testing reducing the startup time. • **Security infrastructure:** SaaS providers offering security technologies share the c with the customers availing the service.

Explain how hypervisor can be protected in virtual machine. Ans) **Virtual machines:** Virtual machines are the ones which allows a virtual operating systems and applications to execute. VMware virtual machines are isolated from one another which enables multiple virtual machines to run securely while sharing hardware and ensure both their ability to access hardware and their uninterrupted performance. **Protecting the Hypervisor:** ➢ The hypervisor is accountable in managing OS installations on a VM server, and the service console provides a centralized location for managing all the servers in a virtual environment. ➢ Hypervisor and service console servers needs patched to be secured Firewalls are used to block access attempts from the virtual machines to the management consoles which prevents attacks and malware on VMs from reaching the service consoles and affecting other VMs. ➢ Since the hypervisor has potential for damages, it is necessary to control its administrative access, as the access to the hypervisor is like having administrative access to all the VMs controlled by it. ➢ Stricting the number of administrators and their privileges can help in reducing the risks of hypervisor attacks via administrator accounts, therefore, the administrators should use different account for management of the privileges. ➢ It is often required to perform security check on administrative activities which helps in ensuring that the security level intact and is not altered intentially. ➢ Securing a hypervisor involves standard actions for any type of software, such as installing updates as they become available, disabling unused virtual hardware; and using the hypervisor's capabilities to monitor the security of each guest OS running within it along with the activity occurring between guests OSS. ➢ Therefore, it is important to provide physical access controls for the hardware on which the hypervisor runs.