NETWORK SECURITY

(For Computer Engg. 6th Semester students)

Chapter 1
Introduction

1. Requirement of Network Security :-

The Network Security is needed for the following given reasons:-

a. To protect the secret information from other users.
b. To protect the information from unwanted editing, accidently or intentionally by unauthorized users.
c. To protect the information from loss and make it to be delivered to its destination properly.
d. To restrict a user to send some message to another user with name of a third one.
e. To protect the message from unwanted delay in the transmission lines in order to deliver it to required destination in time, in case of urgency.
f. To reduce the network congestion problems.

2. key principles of Network Security.

There are mainly three key principles of Network Security which are explained below:-

Confidentiality :- Confidentiality is concerned with preventing unauthorized disclosure of sensitive information. This disclosure could be intentional, such as breaking a cipher and reading the information, or it could be unintentional due to the carelessness or incompetence of individuals handling the information.

Integrity :- There are three goals of integrity.

Preventing the modification of information by unauthorized users

Preventing the unauthorized or unintentional modification of information by unauthorized users

Preserving the internal and external consistency

Availability :- Availability assures that a system's authorized users have timely and uninterrupted access to the information in the system and to the network.

3. the types of Attacks in Network Security.

There are mainly two types of attacks in Network Security - Active and Passive attacks.

Active attacks: An Active attack attempts to alter system resources or effect their operations. Types of active attacks are as following:

1. **Masquerade :-** Masquerade attack takes place when one entity pretends to be different entity.
2. **Modification of messages :-** It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect.

3. **Repudiation :-** This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has sent or received a message.
4. **Denial of Service :-** It prevents normal use of communication facilities. A form of service denial is the disruption of an entire network either by disabling the network or by overloading it by messages so as to degrade performance.

Passive attacks: A Passive attack attempts to make use of information from the system but does not affect system resources.

4. Cyber Crime :-

Cybercrime is any criminal activity that involves a computer, networked device or a network.

A primary impact from cybercrime is financial, and cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals may target private personal information, as well as corporate data for theft and resale.

5. Ethical Hacking :-

Ethical hacking is also known as **White hat Hacking** or **Penetration Testing**. Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system or data. Ethical hacking is used to improve the security of the systems and networks by fixing the vulnerability found while testing.

6. Hacking :-

Gaining access to a system that you are not supposed to have access is considered as hacking. For example: login into an email account that is not supposed to have access, gaining access to a remote computer that you are not supposed to have access, reading information that you are not supposed to able to read is considered as hacking.

7. Cyber Ethics and the rules of Cyber Ethics.

Cyber Ethics refers to the code of responsible behavior on the Internet.

Rules :-

- Do not use rude or offensive language.
- Do not break into someone else's computer.
- Do not use someone else's password.
- Do not attempt to infect or in any way try to make someone else's computer unusable.
- Adhere to copyright restrictions when downloading material from the Internet, including software, games, movies, or music.

8. various methods to protect from hacking.

1. Update your OS (Operating System) and other software frequently.
2. Keep sensitive data off the cloud.
3. Do not use open Wi-Fi on your router.
4. Download and install up-to-date security programs
5. Give creative answers for your security questions

9. Session Hijacking :-

TCP session hijacking is a security attack on a user session over a protected network. Another type of session hijacking is known as a man-in-the-middle attack, where the attacker, using a sniffer, can observe the communication between devices and collect the data that is transmitted.

1. various types of attacks.

the explanation of various types of attacks are as follows:-

Skimming :- Skimming is a method used by identity thieves to capture information from a cardholder. Several approaches can be used by fraudsters to steal card information with the most advanced approach involving a small device called a skimmer.

Phreaker :- A phreak is someone who breaks into the telephone network illegally, typically to make free long-distance phone calls or to tap phone lines.

Hacktivism :- Hacktivism is the act of breaking into a computer system for politically or socially motivated purposes.

Bluejacking :- Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers.

Bluesnarfing :- Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant).

Jailbreaking :- Jailbreaking is the use of an exploit to remove manufacturer or carrier restrictions from a device such as an iPhone or iPad. The exploit usually involves running a privilege escalation attack on a user's device to replace the manufacturer's factory-installed operating system with a custom kernel.

Session Hijacking :- session hijacking is a security attack on a user session over a protected network.

2. the salient features of IT Act 2008?

(i) The term 'digital signature' has been replaced with 'electronic signature' to make the Act more technology neutral.

(ii) A new section has been inserted to define 'communication device' to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image.

(iii) A new definition has been inserted for intermediary.

(iv) A new section has been added to define cyber cafe as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.

(v) A new section 43A has been inserted to protect sensitive personal data or information

Chapter 2
Securing Data over Internet

1. Difference between Data Encryption and Decryption.

Data encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Encryption helps you to protect the privacy of your messages, documents and sensitive files.

Decryption is the process of converting encrypted data back into its original form, so it is easily understood.

2. Symmetric Key Algorithm or Secret Key Algorithm :-

Symmetric key encryption algorithms use a single secret key to encrypt and decrypt data. You must secure the key from access by unauthorized agents because any party that has the key can use it to decrypt data. Secret-key encryption is also referred to as symmetric encryption because the same key is used for encryption and decryption.

3. DES Algorithm :-

DES (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is 64 bits key size with 64 bits block size. It is a type of Symmetric Key Algorithm. DES uses a key to customize the transformation, so that decryption can only be performed by those who know the particular key used to encrypt. The key consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded.

4. PGP Algorithm :-

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

5. RSA Algorithm :-

In RSA (Rivest-Shamir-Adleman) cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm. It provides a method to assure the confidentiality, integrity, authenticity, and non-repudiation of electronic communications and data storage.

6. Asymmetric Key Algorithm or Public Key Algorithm :-

Asymmetric key algorithm is also called Public-key Algorithm. Public-key cryptography is a fundamental and widely used technology around the world, and enables secure transmission of information on the internet and other communication systems. It is also known as asymmetric cryptography because the key used to encrypt a message differs from the one used to decrypt it. In public-key cryptography, a user has a pair of cryptographic keys – a public-key and a private-key. The private-key is kept secret, while the public-key may be widely distributed and known for any user. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key. Public key is used to encrypt the plaintext and the private key is used to decrypt the ciphertext.

7. Hashing :-

Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called **message digest** or simply **hash values**.

8. MD5 (Message Digest) :-

MD5 was the most popular and widely used hash function for quite some years.

- The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It is a 128-bit hash function.
- MD5 digests have been widely used in the software world to provide assurance about integrity of transferred file.

9. SSL :-

SSL (Secure Socket Layer) provides security to the data that is transferred between web browser and server. SSL encrypt the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

10. SSH (Secure Shell) :-

SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network. Secure Shell provides strong authentication and encrypted data communications between two computers connecting over an open network such as the internet. SSH is widely used by network administrators for managing systems and applications remotely, allowing them to log into another computer over a network, execute commands and move files from one computer to another.

11. HTTPS :-

Hypertext Transfer Protocol Secure (HTTPS) is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit through a secure socket layer (SSL) or transport layer security (TLS) protocol connection.

HTTPS enables encrypted communication and secure connection between a remote user and the primary web server.

12. Digital Certification:-

A Digital Certificate is an electronic password that allows a person, organization to exchange data securely over the Internet using the public key infrastructure (PKI). Digital Certificate is also known as a public key certificate or identity certificate.

13. IPSec :-

IPSec which works at the network layer is a framework consisting of protocols and algorithms for protecting data through an un-trusted network such as the internet. IPSec provides data security in various ways such as encrypting and authenticating data, protection against masquerading and manipulation. IPSec is a complex framework consisting of many settings, which is why it provides a powerful and flexible set of security features that can be used.

14. Difference between Block Cipher and Stream Cipher.

Block Cipher and Stream Cipher are the methods used for converting the plain text into cipher text directly and belong to the family of symmetric key ciphers.

The major difference between a block cipher and a stream cipher is that the block cipher encrypts and decrypts a block of the text at a time. On the other hand, stream cipher encrypts and decrypts the text by taking the one byte of the text at a time.

15. Substitution Cipher Encryption Method :-

Substitution cipher is a data encryption scheme in which units of the plaintext (generally single letters or pairs of letters of ordinary text) are replaced with other symbols or groups of symbols.

1. Differentiate between Symmetric Key Algorithm and Asymmetric Key Algorithm.

Symmetric key encryption algorithms use a single secret key to encrypt and decrypt data. You must secure the key from access by unauthorized agents because any party that has the key can use it to decrypt data. Secret-key encryption is also referred to as symmetric encryption because the same key is used for encryption and decryption.

Asymmetric key algorithm is also called Public-key Algorithm. Public-key cryptography is a fundamental and widely used technology around the world, and enables secure transmission of information on the internet and other communication systems. It is also known as asymmetric cryptography because the key used to encrypt a message differs from the one used to decrypt it. In public-key cryptography, a user has a pair of cryptographic keys – a public-key and a private-key. The private-key is kept secret, while the public-key may be widely distributed and known for any user. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key. Public key is used to encrypt the plaintext and the private key is used to decrypt the ciphertext.

2. Digital Signature Algorithm :-

DSA (Digital Signature Algorithm) was proposed by the National Institute of Standards and Technology (NIST) in August 1991. A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender. Digital signatures are commonly used for software distribution, financial transactions etc.

Digital signatures employ a type of asymmetric cryptography. The Digital Signature Algorithm includes two processes: Signature Generation and Signature Verification. Encryption is done at the Signature Generation process by using private key of the sender while decryption is done at the Signature verification process by using public key of the sender.

Chapter 3
Virus, Worms and Trojans

1. Difference between Virus, Worms and Trojans.

Virus is a software or computer program that connect itself to another software or computer program to harm computer system.

Worms replicate itself to cause slow down the computer system. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person.

Trojan Horse rather than replicate capture some important information about a computer system or a computer network. It is a destructive program that looks as a genuine application.

2. various symptoms and indications of virus infection.

Following are some signs that tell us that the system is virus infected.

1. Unexpected pop-up windows
2. Slow start up and slow performance
3. Suspicious hard drive activity
4. Lack of storage space
5. Missing files
6. Crashes and error messages
7. High network activity
8. Email is hijacked
9. Security attacks

3. the steps to remove a virus from the system.

The steps to remove a virus from the system are as follows:-

Step 1 : Enter Safe Mode.

Step 2 : Delete Temporary files.

Step 3 : Download a virus scanner.

Step 4 : Run a virus scan.

4. antivirus software :-

- Scan specific files or directories for any malware or known malicious patterns.
- Allow you to schedule scans to automatically run for you.
- Allow you to initiate the scan of a particular file or your entire computer, or of a CD or flash drive at any time.
- Remove any malicious code detected.
- Show you the 'health' of your computer

5. Checksum Verification :-

A checksum is a value used to verify the integrity of a file or a data transfer. In other words, it is a sum that checks the validity of data. Checksums are typically used to compare two sets of data to make sure they are the same.

If the checksums don't match, the data may have been altered or corrupted.

6. Virus Scanner :-

A virus scan is the process of using anti-virus software to scan and identify viruses in a computing device. Virus Scanner is a type of antivirus program that searches a system for virus signatures that have attached to executable programs and applications such as e-mail clients. A virus scanner can either search all executables when a system is booted or scan a file only when a change is made to the file as viruses will change the data in a file.

7. Heuristic Scanner :-

Heuristic analysis can be found in the majority of mainstream antivirus solutions on the market today. Similar to signature scanning, which detects threats by searching for specific strings, heuristic analysis looks for specific commands or instructions that would not typically be found in an application.

Most heuristic antivirus processes use a rule or weight-based system to determine how much danger a program functionality could pose. If these rules exceed a predetermined threshold, an alarm is triggered and preemptive action is taken.

8. Zombie Network :-

A zombie network is a network or collection of compromised computers or hosts that are connected to the Internet. A compromised computer becomes a zombie that is wirelessly

controlled through standards based networking protocols like HTTP and Internet Relay Chat (IRC).
A zombie network is also known as a botnet.

9. Ransomware :-

Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via crypto-currency or credit card.

1. Virus :-

Virus is a software or computer program that connect itself to another software or computer program to harm computer system.

Symptoms of Virus Infection:- Following are some signs that tell us that the system is virus infected.

1. Unexpected pop-up windows
2. Slow start up and slow performance
3. Suspicious hard drive activity
4. Lack of storage space
5. Missing files
6. Crashes and error messages
7. High network activity
8. Email is hijacked
9. Security attacks

Steps to remove a Virus :- The steps to remove a virus from the system are as follows:-

Step 1 : Enter Safe Mode.
Step 2 : Delete Temporary files.
Step 3 : Download a virus scanner.
Step 4 : Run a virus scan.

2. the preventive measures of infections in computer systems :-

1. Install Anti-Virus/Malware Software.
2. Keep Your Anti-Virus Software Up to Date.
3. Run Regularly Scheduled Scans with Your Anti-Virus Software.
4. Keep Your Operating System Current.
5. Secure Your Network.
6. Keep Your Personal Information Safe.
7. Don’t Use Open Wi-Fi.
8. Back Up Your Files.
9. Use Multiple Strong Passwords.

Chapter 4

Firewalls

1. Firewall :-

A firewall is a type of cyber-security tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based.

2. the types of Firewall :-

Firewall types can be divided into several different categories based on their general structure and method of operation. Here are eight types of firewall:

- Packet-filtering firewalls
- Circuit-level gateways
- Stateful inspection firewalls
- Application-level gateways (proxy firewalls)
- Next-gen firewalls
- Software firewalls
- Hardware firewalls
- Cloud firewalls

3. the configuration of firewall :-

There are following steps to configure firewall.

Step 1 : Secure your firewall.
Step 2 : Architect your firewall zones and IP addresses
Step 3 : Configure access control lists
Step 4 : Configure your other firewall services
Step 5 : Test your firewall configuration

4. the limitations of Firewall :-

(i) It cannot protect against attacks that by-pass the firewall.
(ii) It may not protect against internal threats when an insider collaborates with an outside adversary.
(iii) It may not be able to protect against viruses and infected files since it may not be possible to scan all incoming traffic.

5. the advantages of Firewall :-

(i) A firewall is an intrusion detection mechanism.
(ii) Firewalls can also block email services to secure against spam.
(iii) Firewall verifies the incoming and outgoing traffic against firewall rules.
(iv) It acts as a router in moving data between networks.
(v) Firewalls can be used to restrict access to specific services.

6. the difference between Whitelisting and Blacklisting :-

Whitelisting automatically denies everything and allows a few things while blacklisting automatically approves everything and rejects a few things. If you blacklist items, you have to know the known threats associated with those programs or applications.

Differences :-

Whitelisting	Blacklisting
1. Default deny	1. Default allow

2. Uses a list of approved apps, software, emails etc.	2. Uses a list of unapproved apps, software, emails etc.
3. Items not on the approved list are restricted or denied, depending on your company's needs.	3. Items not on the unapproved list can be used without any modifications or control.

7. inbound and outbound rules related with firewalls :-

inbound firewall rules protect the network against incoming traffic from the internet or other network segments – namely, disallowed connections, malware and Denial of Service (DoS) attacks.

Outbound firewall rules protect against outgoing traffic, such as requests to dangerous websites, VPN (Virtual Private Network) connections and email services.

A single firewall typically serves both functions.

1. the types of Firewall :-

Firewall types can be divided into several different categories based on their general structure and method of operation. Here are eight types of firewall:

- Packet-filtering firewalls
- Circuit-level gateways
- Stateful inspection firewalls
- Application-level gateways (proxy firewalls)
- Next-gen firewalls
- Software firewalls
- Hardware firewalls
- Cloud firewalls

Packet-filtering firewalls :- The firewall performs a simple check of the data packets coming through the router—inspecting information such as the destination and origination IP address, packet type, port number, and other surface-level information without opening up the packet to inspect its contents.

Circuit-level gateways :- circuit-level gateways work by verifying the transmission control protocol (TCP) handshake. This TCP handshake check is designed to make sure that the session the packet is from is legitimate.

Stateful inspection firewalls :- These firewalls combine both packet inspection technology and TCP handshake verification to create a protection.

Application-level gateways (proxy firewalls) :- Proxy firewalls operate at the application layer to filter incoming traffic between your network and the traffic source.

Next-gen firewalls :- Some common features of next-generation firewall architectures include deep-packet inspection (checking the actual contents of the data packet), TCP handshake checks, and surface-level packet inspection. Next-generation firewalls may include other technologies as well, such as intrusion prevention systems (IPSs) that work to automatically stop attacks against your network.

Software firewalls :- Software firewalls include any type of firewall that is installed on a local device rather than a separate piece of hardware.

Hardware firewalls :- Hardware firewalls use a physical appliance that acts in a manner similar to a traffic router to intercept data packets and traffic requests before they're connected to the network's servers.

Cloud firewalls :- Whenever a cloud solution is used to deliver a firewall, it can be called a cloud firewall, or firewall-as-a-service (FaaS).

2. the advantages and disadvantages of Firewall :-

A firewall is a type of cyber-security tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based.

Advantages :-

(i) A firewall is an intrusion detection mechanism.

(ii) Firewalls can also block email services to secure against spam.

(iii) Firewall verifies the incoming and outgoing traffic against firewall rules.

(iv) It acts as a router in moving data between networks.

(v) Firewalls can be used to restrict access to specific services.

Disadvantages :-

(i) It cannot protect against attacks that by-pass the firewall.

(ii) It may not protect against internal threats when an insider collaborates with an outside adversary.

(iii) It may not be able to protect against viruses and infected files since it may not be possible to scan all incoming traffic.

Chapter 5
Intrusion Detection System (IDS)/IPS

1. Intrusion Detection System (IDS) :-

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

2. the limitations or disadvantages of IDS (Intrusion Detection System) :-

(i) Source Addresses :- Intrusion detection software provides information based on the network address that is associated with the IP packet that is sent into the network. This is beneficial if the network address contained in the IP packet is accurate. However, the address that is contained in the IP packet could be fake or scrambled.

(ii) Encrypted Packets :- Encrypted packets are not processed by the intrusion detection software.

(iii) Analytical Module :- The analytical module has a limited ability to analyze the source information that is collected during intrusion detection.

(iv) False Alarms :- intrusion software can create a large number of false alarms. These false

alarms are increased on networks where there are a large number of users.

3. Teardrop Attack :-

A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device.

4. counter measures in network security :-

Security countermeasures are the controls used to protect the confidentiality, integrity, and availability of data and information systems. There is a wide array of security controls available at every layer of the stack. Overall security can be greatly enhanced by adding additional security measures, removing unneeded services, hardening systems, and limiting access.

5. the Host-based Intrusion Detection System (HIDS) :-

A host-based intrusion detection system (HIDS) is a system that monitors a computer system on which it is installed to detect an intrusion and/or misuse, and responds by logging the activity and notifying the designated authority. A HIDS can be thought of as an agent that monitors and analyzes whether anything or anyone, whether internal or external, has circumvented the system's security policy.

A HIDS analyzes the traffic to and from the specific computer on which the intrusion detection software is installed. A host-based system also has the ability to monitor key system files and any attempt to overwrite these files.

6. various IDS countermeasures :-

(i) Frequently update antivirus Signature database.
(ii) Configure the firewall to filter out IP address of an intruder.
(iii) Beep or play .WAV file as an indication.
(iv) Save the attack information (Intruder IP, victim IP, timestamp).
(v) Send intimation to Administrator about attack.
(vi) Force a TCP FIN or RST packet to force a connection termination.

1. the various types of IDS in detail :-

Types of IDS :- For the purpose of dealing with IT, there are four main types of IDS:

Network Intrusion Detection System (NIDS)

It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection Systems gain access to network traffic by connecting to a network hub, a network switch configured for port mirroring, or a network tap.

Host-based Intrusion Detection System (HIDS)

It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications and other host activities and state. In a HIDS, sensors usually consist of a software agent.

Perimeter Intrusion Detection System (PIDS)

Using either electronics or more advanced fiber optic cable technology fitted to the perimeter fence, the PIDS detects disturbances on the fence, and if an intrusion is detected and deemed by the system as an intrusion attempt, an alarm is triggered.

VM based Intrusion Detection System (VMIDS)

It detects intrusions using virtual machine monitoring. By using this, we can deploy the Intrusion Detection System with Virtual Machine Monitoring. It is the most recent type and it's still under development.

Chapter 6
Handling Cyber Assets

1. Cyber Security Asset :-

In information security, computer security and network security an Asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software and confidential information. Assets should be protected from illicit access, use, disclosure, alteration, destruction, theft etc. resulting in loss to the organization.

2. the Security Policy Makers :-

Security policy development is a joint or collective operation of all entities of an organization that is affected by its rules. In general, security policies should not be developed by IT team itself as it is a responsibility of everyone. During policy creating following entity typically involves:-

Board: Company board members must render their advice to some form of a review of policies in response to exceptional or abnormal running condition of business.

IT Team: IT team members usually are the biggest consumers of the policy information in any company, as it involves making standard around the usage of the computer system, especially security controls.

Legal Team: This team ensures the legal points in the document and guides a particular point of appropriateness in the company.

HR Team: HR team typically obtains a certified T&C certificate from each employee that they have read and understood the stipulated policy.

1. protect the Cyber Security Assets :-

There are some instructions which can be followed to protect the cyber assets. Some of these are as follows:-

(i) Use multi-factor authentication – this requires more than one step to verify your identity.
(ii) Try a biometric log-in system with fingerprint or facial recognition.
(iii) Back up your data regularly.
(iv) Use strong passwords and change them regularly.
(v) Keep your operating system and applications up to date.
(vi) Use antivirus software.
(vii) Be suspicious of cold calls.
(viii) Use your browser's pop-up blocker.
(ix) Have an information security policy
(x) In the event of a data breach, you have to respond quickly and appropriately in order to minimize the damage to your business.

Chapter 7
Virtual Private Network (VPN)

1. Virtual Private Network (VPN) :-

VPN stands for virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. Virtual Private network is a way to extend a private network using a public network such as internet. In this system, user can be the part of local network sitting at a remote location.

2. the benefits or advantages of VPN (Virtual Private Network) :-

1. VPN ensures security by providing an encrypted tunnel between client and VPN Server.
2. VPN is used to bypass many blocked sites.
3. VPN facilitates anonymous browsing by hiding your IP Address.

3. setup of a VPN Connection :-

Step 1 :- Click the *Start* button. In the search bar, type vpn and then select *Set up a virtual* private network (VPN) connection.
Step 2 :- Enter the IP address or domain name of the server to which you want to connect.
Step 3 :- click Next button.
Step 4 :- On this next screen, you can either put in your username and password, or leave it blank. Click Connect.
Step 5 :- To connect, click on the Windows network logo on the lower-right part of your screen; then select Connect under "VPN Connection."
Step 6 :- In the "Connect VPN Connection" box, enter the appropriate domain and your login credentials; then click Connect.

4. the Internet Key Exchange :-

Internet Key Exchange (IKE) is the protocol used to set up a secure, authenticated communications channel between two parties. IKE typically uses X.509 PKI certificates for authentication and the Diffie–Hellman key exchange protocol to set up a shared session secret.

IKE is part of the Internet Security Protocol (IPSec) which is responsible for negotiating security associations (Sas), which are a set of mutually agreed-upon keys and algorithms to be used by both parties trying to establish a VPN connection/tunnel.

5. to modify the security policy

Go to Policy & Objects > Policy > Ipv4.
Set the following options:

Incoming Interface	Select the local interface to the internal (private) network.
Source Address	Select the name that corresponds to the local network, server(s),

	or host(s) from which IP packets may originate.
Outgoing Interface	Select the local interface to the external (public) network.
Destination Address	Select the name that corresponds to the remote network, server(s), or host(s) to which IP packets may be delivered.
Schedule	Keep the default setting (always) unless changes are needed to meet specific requirements.

1. the various protocols used in VPN :-

Types of VPN protocols are explained below:

(i) Internet Protocol Security or IPSec:

Internet Protocol Security or IPSec is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by authenticating the session and encrypts each data packet during the connection.

IPSec operates in two modes, Transport mode and Tunneling mode, to protect data transfer between two different networks. The transport mode encrypts the message in the data packet and the tunneling mode encrypts the entire data packet. IPSec can also be used with other security protocols to enhance the security system.

(ii) Layer 2 Tunneling Protocol (L2TP):

L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is usually combined with another VPN security protocol like IPSec to create a highly secure VPN connection.

(iii) Point – to – Point Tunneling Protocol (PPTP):

PPTP or Point-to-Point Tunneling Protocol creates a tunnel and encapsulates the data packet. It uses a Point-to-Point Protocol (PPP) to encrypt the data between the connection.

(iv) Secure Sockets Layer (SSL) and Transport Layer Security (TLS):

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) create a VPN connection where the web browser acts as the client and user access is restricted to specific applications instead of entire network. SSL and TLS protocol is most commonly used by online shopping websites and service providers.

(v) Secure Shell (SSH):

Secure Shell or SSH creates the VPN tunnel through which the data transfer happens and also ensures that the tunnel is encrypted. SSH connections are created by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

Chapter 8
Disaster and Recovery

1. Network Disaster Recovery Plan :-

A network disaster recovery plan is a set of procedures designed to prepare an organization to respond to an interruption of network services during a natural or manmade catastrophe.

A network disaster recovery plan ensures that all resources and services that rely on the network are backup and running in the event of an interruption within a certain specified time frame.

Such a plan usually includes procedures for recovering an organization's local area networks (LANs), wide area networks (WANs) and wireless networks. It may cover network applications and services, servers, computers and other devices, along with the data at issue.

2. the working of RAID :-

RAID works by placing data on multiple disks and allowing input/output (I/O) operations to overlap in a balanced way, improving performance. Because the use of multiple disks increases the mean time between failures (MTBF), storing data redundantly also increases fault tolerance.

RAID arrays appear to the operating system (OS) as a single logical hard disk. RAID employs the techniques of disk mirroring or disk striping. Mirroring copies identical data onto more than one drive. Striping partitions each drive's storage space into units ranging from a sector (512 bytes) up to several megabytes.

3. Server Redundancy and Clustering :-

Redundancy is basically extra hardware or software that can be used as backup if the main hardware or software fails. Redundancy can be achieved via load clustering, failover, RAID, load balancing, high availability in an automated fashion.

Clustering is very similar to redundant servers and provides fault tolerance. In clustering, all servers take part in processing a service simultaneously. A group of servers are logically combined into a cluster and seen as one device, which provides a type of service. If a device fails within a cluster, the services continue because the other devices within the cluster continue processing the same service.

4. backup and recovery process :-

Backup and recovery describes the process of creating and storing copies of data that can be used to protect organizations against data loss. This is sometimes referred to as operational recovery. Recovery from a backup typically involves restoring the data to the original location, or to an alternate location where it can be used in place of the lost or damaged data.

A proper backup copy is stored in a separate system or medium, such as tape, from the primary data to protect against the possibility of data loss due to primary hardware or software failure.

5. Server UPS :-

UPS stands for Uninterruptible Power Supply. A UPS is a set of batteries that plug into the mains. You can plug your servers into them (as well as PCs, printers and other hardware) and if you have a power cut, the server will recognize the drop in voltage and automatically shut itself down safely. This can increase the lifespan of your servers as it eliminates power surges.

6. a single point of failure :-

A single point of failure, also known as SPOF, is any component of a system that causes the whole system to stop working if it fails. When designing reliable systems, SPOFs can be avoided by implementing redundant components and replicating critical parts of the system. For example, a computer may implement RAID storage so that if a single disk fails, the system can continue operating.

7. the network cabling :-

Network cables are used to connect and transfer data and information between computers, routers, switches and storage area networks. These cables are essentially the carrier or media through which data flows.

There are different types of communication cables which depend on the structure and topology of the overall architecture of the system. The most commonly used types of communication cables are “twisted pair cable”. In local area networks; typically office environments, retail and commercial sites, copper communications cabling, i.e., twisted pair cables are mostly used.

8. the preventive steps to be taken for disaster recovery :-

(i) Backup should be done periodically.
(ii) The headquarters should have one or more internet lines.
(iii) RAID systems should always be used.
(iv) There should always be a spare Hard Disk in the server room.
(v) Only IT personnel should enter the server room at any given point of time.

9. FDDI :-

FDDI stands for Fiber Distributed Data Interface. It is a set of ANSI protocols for sending digital data over fiber optic cable. FDDI networks are token-passing networks and support data rates of upto 100 Mbps. FDDI networks are typically used as backbones for wide-area networks.

10. IP Address :-

The Internet Protocol Address (or IP Address) is a unique address that computing devices such as personal computers, tablets, and smart-phones use to identify itself and communicate with other devices in the IP network. Any device connected to the IP network must have a unique IP address within the network.

The traditional IP Address (known as IPv4) uses a 32-bit number to represent an IP address, and it defines both network and host address.

An IP address is written in dotted decimal notation, which is 4 sets of numbers separated by period. Each set represents 8-bit number ranging from (0-255).

An example of IPv4 address is 216.3.128.12

1. RAID :-

RAID stands for redundant array of independent disks. It is a way of storing the same data in different places on multiple hard disks to protect data in the case of a drive failure.

Working of RAID :- RAID works by placing data on multiple disks and allowing input/output (I/O) operations to overlap in a balanced way, improving performance. Because the use of multiple disks increases the mean time between failures (MTBF), storing data redundantly also increases fault tolerance.

RAID arrays appear to the operating system (OS) as a single logical hard disk. RAID employs the techniques of disk mirroring or disk striping. Mirroring copies identical data onto more than one drive. Striping partitions each drive's storage space into units ranging from a sector (512 bytes) up to several megabytes.

RAID levels :-

RAID 0: This configuration has striping, but no redundancy of data. It offers the best performance, but no fault tolerance.

RAID 1: Also known as disk mirroring, this configuration consists of at least two drives that duplicate the storage of data.

RAID 2: This configuration uses striping across disks, with some disks storing error checking and correcting information.

RAID 3: This technique uses striping and dedicates one drive to store parity information. The embedded ECC information is used to detect errors.

RAID 4: This level uses large stripes, which means you can read records from any single drive.

RAID 5: This level is based on block -level striping with parity.

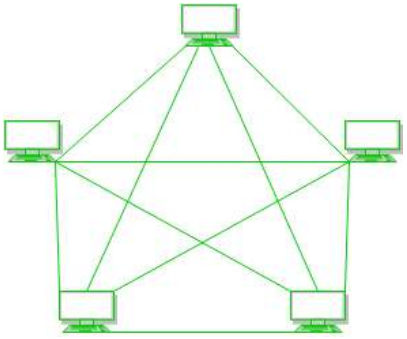
RAID 6: This technique is similar to RAID 5, but includes a second parity scheme that is distributed across the drives in the array. The use of additional parity allows the array to continue to function even if two disks fail simultaneously.

RAID 10 (RAID 1+0): Combining RAID 1 and RAID 0, this level is often referred to as RAID 10, which offers higher performance than RAID 1, but at a much higher cost. In RAID 1+0, the data is mirrored and the mirrors are striped.

2. the Network Topologies :-

The arrangement of a network which comprises of nodes and connecting lines via sender and receiver is referred as network topology. The various network topologies are :-

a) Mesh Topology : In mesh topology, every device is connected to another device via particular channel.



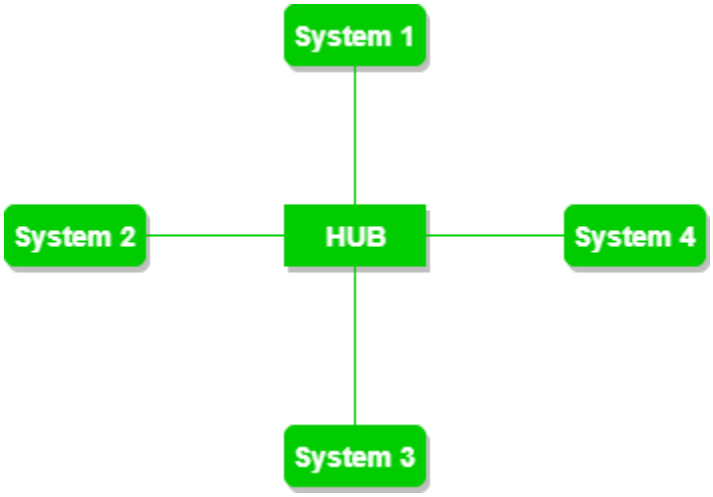
Advantages of this topology :

1. It is robust.
2. Fault is diagnosed easily.
3. Data is reliable because data is transferred among the devices through dedicated channels or links.

Problems with this topology :

1. Installation and configuration is difficult.
2. Cost of cables are high as bulk wiring is required.
3. Cost of maintenance is high.

b) Star Topology : In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Advantages of this topology :

1. If N devices are connected to each other in star topology, then the number of cables required to connect them is N.
2. Each device require only 1 port i.e. to connect to the hub.

Problems with this topology :

1. Cost of installation is high.
2. Performance is based on the single concentrator i.e. hub.

c) Bus Topology : Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction.

Advantages of this topology :

1. If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1
2. Cost of the cable is less as compared to other topology.

Problems with this topology :

1. If the common cable fails, then the whole system will crash down.
2. If the network traffic is heavy, it increases collisions in the network.

d) Ring Topology : In this topology, it forms a ring connecting the devices.

Advantages of this topology :

1. The possibility of collision is minimum in this type of topology.
2. Cheap to install and expand.

Problems with this topology :

1. Troubleshooting is difficult in this topology.
2. Addition of stations in between or removal of stations can disturb the whole topology.

e) Hybrid Topology : This topology is a collection of two or more topologies. This is a scalable topology which can be expanded easily.