Unit-1

Introduction to Electronic Commerce

What is ecommerce?

E-commerce, short for electronic commerce, refers to the buying and selling of goods or services over the internet. This can include a wide range of activities, from purchasing physical products from an online retailer to booking travel arrangements, buying digital products such as music or e-books, and using online marketplaces to buy and sell goods and services.

E-commerce has become increasingly popular in recent years due to the convenience and accessibility it offers to both consumers and businesses. For consumers, e-commerce eliminates the need to physically travel to a store and allows for easy price comparisons and product reviews. For businesses, e-commerce provides a low-cost way to reach a global audience and gather valuable data on customer behavior and preferences.

E-commerce can take place on various platforms and channels, including:

- Online marketplaces like Amazon and Flipkart
- Businesses websites and mobile apps
- Social media platforms like Instagram, Facebook and TikTok
- Online classifieds like Craigslist and Gumtree
- Subscription-based services like Netflix and Spotify

There are many different types of e-commerce, including business-to-consumer (B2C), consumer-to-consumer (C2C), business-to-business (B2B), and mobile commerce (M- commerce).

Aims of E-commerce

The aims of e-commerce can vary depending on the type of business and its target market, butsome common goals include:

- **Increasing sales and revenue:** E-commerce allows businesses to reach a global audience, which can lead to increased sales and revenue.
- **Improving customer service:** E-commerce allows businesses to provide customers with a convenient and personalized shopping experience, which can improve customer satisfaction and loyalty.
- **Expanding market reach:** E-commerce allows businesses to expand beyond their local market and sell to customers all over the world.
- **Lowering costs:** E-commerce can lower overhead costs associated with traditional brick-and-mortar stores, such as rent, utilities, and staffing.
- **Gaining customer insights:** E-commerce allows businesses to collect data on customerbehavior and preferences, which can be used to improve products and services and target marketing efforts.
- **Improving inventory management**: E-commerce allows businesses to have a better track of their inventory, this way they can reorder when needed and avoid stockouts.

- **Automation:** E-commerce allows businesses to automate many process, such as order processing, invoicing, and shipping, which can save time and reduce errors.
- **Building a brand:** E-commerce allows businesses to create a strong online presence and build a brand through online marketing and social media.
- **Increasing customer engagement:** E-commerce allows businesses to engage with customers through personalized communications, social media, and other digital channels.
- **Creating new revenue streams:** E-commerce allows businesses to explore new business models, such as subscription-based services and digital products, which can create new revenue streams.

Benefits of E-commerce:

E-commerce offers a wide range of benefits for both consumers and businesses, including:

- **Increased reach:** E-commerce allows businesses to reach a global audience, which can lead to increased sales and revenue.
- **Convenience:** E-commerce allows customers to shop from the comfort of their own homes, without the need to leave their house or wait in line.
- **24/7 availability:** E-commerce websites are open 24/7, allowing customers to shop at any time.
- **Lower costs:** E-commerce businesses do not have the same costs associated with traditional brick-and-mortar stores, such as rent, utilities, and staffing.
- **Personalization and targeting:** E-commerce allows businesses to collect data on customer behavior and preferences, which can be used to personalize the shopping experience and target marketing efforts.
- **Increased competition:** E-commerce creates a level playing field for small and large businesses, as customers can easily compare prices and products from different sellers.
- **Better inventory management:** E-commerce allows businesses to have a better track of their inventory, this way they can reorder when needed and avoid stockouts.
- **Automation:** E-commerce allows businesses to automate many process, such as order processing, invoicing, and shipping, which can save time and reduce errors.
- **Globalization:** E-commerce allows businesses to expand beyond their local market and sell to customers all over the world
- **Easy Comparison and research:** E-commerce allows customers to easily compare products and prices from different vendors, as well as read product reviews and research products before making a purchase.

- **Limitations of E-commerce:**

  There are several limitations of ecommerce, including:

- **Limited physical interaction**: Online shopping does not allow customers to physically examine or test products before purchasing, which can lead to dissatisfaction with the product or difficulty in determining the right fit.

- **Shipping and handling issues**: Ecommerce relies on shipping and handling to deliver products to customers, which can result in delays, damage, or lost packages.
- **Lack of personal interaction**: Shopping online can lack the personal interaction and assistance that customers may receive when shopping in-store.
- **Limited payment options**: Some ecommerce platforms may not accept certain forms of payment, such as cash or checks, which can limit the ability of some customers to make purchases.
- **Cyber security concerns**: Ecommerce is vulnerable to cyber attacks and fraud, which can lead to financial loss and damage to customer trust.
- **Shipping Cost**: Shipping cost may be higher for some remote locations and for heavyitem.
- **Return Policy and Process**: Some e-commerce sites have strict return policies, which can make it difficult for customers to return items that do not meet their expectations.

E-Commerce v/s Traditional Commerce

E-commerce and traditional commerce (also known as brick-and-mortar commerce) are two different ways of buying and selling goods and services. While e-commerce primarily takes place online, traditional commerce typically involves physical storefronts and in-person transactions.

Benefits of e-commerce include:

1. **Increased reach:** E-commerce allows businesses to reach a global audience with minimal overhead costs. This can lead to increased sales and revenue.
2. **Convenience:** E-commerce allows customers to shop from the comfort of their own homes, without the need to leave their house or wait in line.
3. **24/7 availability:** E-commerce websites are open 24/7, allowing customers to shop at any time.
4. **Lower costs:** E-commerce businesses do not have the same costs associated with traditional brick-and-mortar stores, such as rent, utilities, and staffing.
5. **Personalization and targeting:** E-commerce allows businesses to collect data on customer behavior and preferences, which can be used to personalize the shopping experience and target marketing efforts.
6. **Tangible experience:** Physical stores provide customers with the opportunity to touch and try on products before buying, which can lead to increased customer satisfaction.
7. **Immediate satisfaction:** Customers can take their purchases home with them immediately, rather than waiting for delivery.
8. **In-person customer service:** Physical stores often have staff on hand to provide customer service and answer questions.
9. **Brand awareness and reputation:** A physical store can serve as a symbol of a business's reputation and credibility.
10. **Community building:** Physical stores can foster a sense of community and bring people together.

Benefits of traditional commerce include:

It's worth noting that, these days, many businesses are utilizing both e-commerce and traditional commerce strategies to reach customers in different ways. Some businesses use e-commerce to expand their reach, while maintaining a physical storefront to provide customers with a tangible experience. Some businesses use physical storefronts to promote brand awareness and create community, while also having an online store for customers who prefer to shop online.

M-Commerce:

M-commerce, short for mobile commerce refers to the buying and selling of goods or services through mobile devices such as smart phones and tablets. This can include a wide range of activities, from purchasing physical products from an online retailer using a mobile device to using mobile apps to book travel arrangements, buy digital products such as music or e-books, and use mobile-optimized versions of online marketplaces to buy and sell goods and services.

M-commerce has become increasingly popular in recent years due to the widespread use of smart phones and tablets, and the convenience and accessibility it offers to both consumers and businesses. For consumers, m-commerce eliminates the need to be in front of a computer to shop online and allows for easy price comparisons and product reviews on the go. For businesses, m-commerce provides a way to reach customers wherever they are and gather valuable data on customer behavior and preferences.

M-commerce can take place on various platforms and channels, including:

- Mobile apps of online marketplaces like Amazon and Etsy
- Businesses mobile apps
- Mobile optimized version of social media platforms like Instagram, Facebook and TikTok
- Mobile optimized version of online classifieds like Craigslist and Gumtree
- Mobile apps of subscription-based services like Netflix and Spotify

It is also important to note that M-commerce is a subset of e-commerce, as it covers all the buying and selling activities that take place through mobile devices.

What is E-Business?

E-business, short for electronic business, refers to the use of technology and the internet to conduct business operations and transactions. This can include a wide range of activities, from selling products and services online to automating internal business processes, such as human resources and accounting, to communicating and collaborating with customers and partners.

E-business includes e-commerce, but it goes beyond that, it encompasses all the online activities of a business, including internal operations, external interactions with customers and partners, and the use of technology to support these activities. E-business can also include the

Use of digital technologies such as cloud computing, artificial intelligence, and the Internet of Things to improve business operations and create new revenue streams.

Examples of e-business activities include:

- Selling products or services online through e-commerce platforms
- Using social media to connect with customers and promote products or services
- Using digital communication tools like email, instant messaging, and video conferencing to collaborate with remote teams and partners
- Using digital tools to automate internal processes such as accounting, human resources, and inventory management
- Using big data and analytics to gain insights into customer behavior and optimize business operations
- Using online marketing techniques to reach new customers and promote products or services

E-business can provide many benefits to businesses, such as increased efficiency, cost savings, and improved customer service. However, it also poses new challenges, such as the need for businesses to stay on top of rapidly changing technologies and adapt to new market trends.

- **Advantages of e-Commerce**
  - Convenience: E-commerce allows customers to shop and make purchases at any time and from any location.
  - Increased reach: E-commerce allows businesses to reach customers beyond their physical location, which can increase the customer base and revenue.
  - Cost savings: E-commerce can save businesses money by reducing the need for physical storefronts, inventory storage, and other expenses.
  - Personalization: E-commerce platforms have the ability to track customer behavior, preferences and purchase history, which can be used for personalized marketing and recommendations.
  - Automation: Many e-commerce tasks can be automated, such as inventory management, order fulfillment, and marketing campaigns.
  - Data collection and analysis: E-commerce platforms generate a large amount of data that can be used to gain insights into customer behavior, preferences, and buying patterns.
  - Increased competition: E-commerce has made it easier for small businesses to compete with larger ones as they can reach a larger audience and don't need to invest as much in physical infrastructure.
  - Faster buying process: Shopping online is generally faster than physically going to a store, as customers can easily browse through products, compare prices, and complete a purchase in a shorter amount of time.
  - Greater product selection: Online retailers can offer a larger selection of products than physical stores because they don't have the same space constraints.
  - Global market: E-commerce allows businesses to sell to customers worldwide, which can greatly increase

- **Disadvantages of e-Commerce**
  - Limited customer interaction: E-commerce transactions lack the personal touch of face- to-face interactions, which can lead to lower customer satisfaction and loyalty.

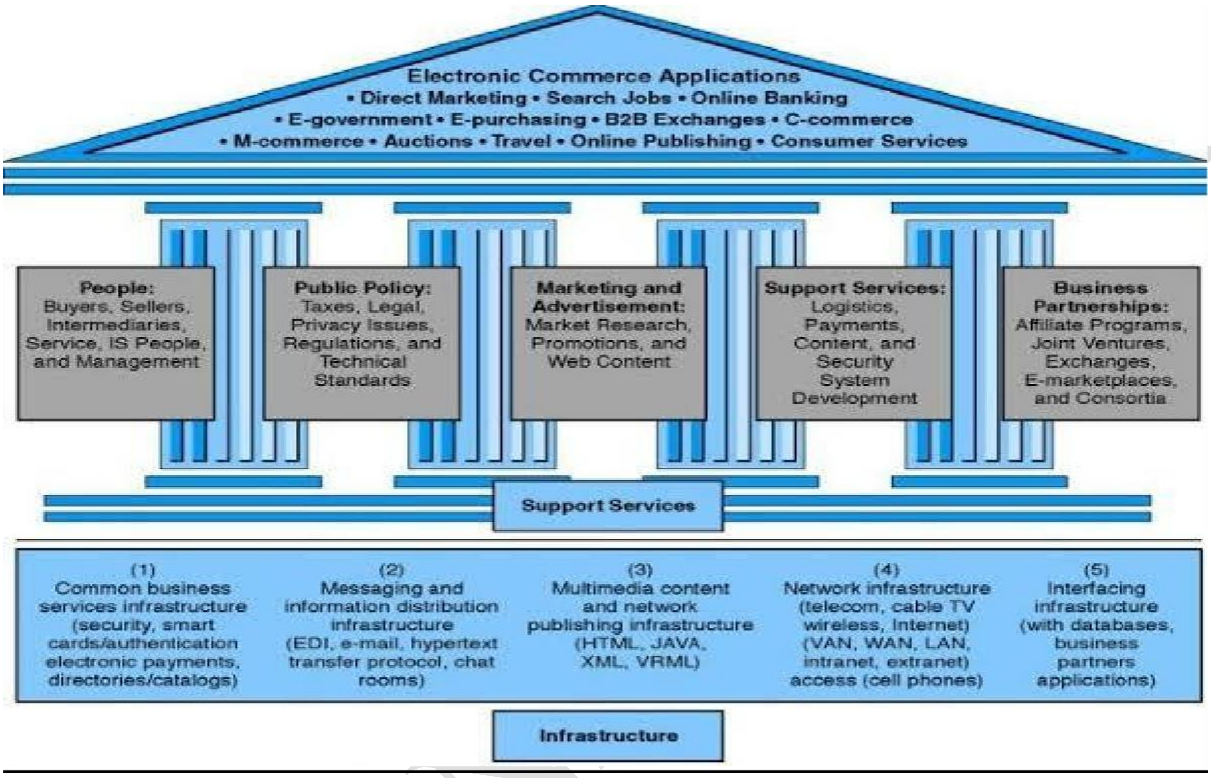
- Shipping and handling issues: Shipping and handling physical goods can be complicated and can lead to issues such as lost or damaged items.
- Shipping costs: Shipping costs can be a significant expense for both the business and the customer.
- Returns and exchanges: Returns and exchanges can be more difficult to handle in an e-commerce setting, leading to increased costs and reduced customer satisfaction.
- Cyber security risks: E-commerce transactions involve sensitive personal and financial information, which can be vulnerable to hacking and other cyber threats.
- Limited product inspection: Customers cannot inspect products in person before purchasing, which can lead to dissatisfaction with the product or the need for returns.
- Dependence on technology: E-commerce relies heavily on technology, which can be vulnerable to outages, breakdowns, and other issues.
- Competition: Online marketplaces are highly competitive, making it difficult for new businesses to establish themselves and for existing businesses to stand out.
- Lack of tactile experience: Online shopping doesn't provide customers with the tactile experience of physically handling and examining a product before buying.
- Limited to digital products: E-commerce is limited to digital products and services, which makes it difficult for businesses that sell physical goods to establish a strong online presence.

- **Advantages of m-Commerce**
  - Convenience and accessibility, as customers can shop and make purchases fromanywhere at any time using their mobile devices.
  - Increased reach and accessibility, as more and more customers are using mobile devicesto browse the internet.
  - Personalization and targeting, as companies can use data from mobile devices to personalize the shopping experience and target advertising.
  - Ability to reach customers through push notifications and other mobile-specificfeatures.
  - Improved customer engagement, as mobile devices allow for interactive features suchas touch, GPS, and camera.
  - Increased sales, as mobile commerce can make it easier for customers to purchaseproducts and services.
  - Better customer experience, as mobile commerce can provide faster loading times, easy navigation, and easy checkout.
  - Cost-effective, as mobile commerce requires less investment in physical infrastructureand maintenance.

- **Disadvantages of m-Commerce**
  - Limited screen size and functionality of mobile devices can make it difficult to navigateand complete transactions on mobile websites or apps.
  - Security concerns, as mobile devices are more susceptible to hacking and data breaches.
  - Limited payment options, as some customers may not have access to mobile paymentmethods or prefer to use other forms of payment.
  - Dependence on internet connectivity, which can be unreliable in some areas or duringcertain times.
  - Mobile websites may not be optimized for search engines, which can make it harder for customers to find the mobile site.

- Limited customer service options, as it can be difficult to provide support via a mobiledevice.
- Potential to be blocked by mobile carrier or government.

E-Commerce Framework:


Electronic Commerce Applications
• Direct Marketing • Search Jobs • Online Banking
• E-government • E-purchasing • B2B Exchanges • C-commerce
• M-commerce • Auctions • Travel • Online Publishing • Consumer Services
People: Buyers, Sellers, Intermediaries, Service, IS People, and Management
Public Policy: Taxes, Legal, Privacy Issues, Regulations, and Technical Standards
Marketing and Advertisement: Market Research, Promotions, and Web Content
Support Services: Logistics, Payments, Content, and Security System Development
Business Partnerships: Affiliate Programs, Joint Ventures, Exchanges, E-marketplaces, and Consortia
Support Services
(1) Common business services infrastructure (security, smart cards/authentication electronic payments, directories/catalogs)
(2) Messaging and information distribution infrastructure (EDI, e-mail, hypertext transfer protocol, chat rooms)
(3) Multimedia content and network publishing infrastructure (HTML, JAVA, XML, VRML)
(4) Network infrastructure (telecom, cable TV wireless, Internet) (VAN, WAN, LAN, intranet, extranet) access (cell phones)
(5) Interfacing infrastructure (with databases, business partners applications)
Infrastructure

An e-commerce framework is a set of guidelines, best practices, and technologies that businesses can use to develop and implement an e-commerce strategy. A typical e-commerce framework includes several key components:

1. E-commerce platform: This is the foundation of an e-commerce business, providing the technical infrastructure for the website and online store. Popular e-commerce platforms include Magento, Shopify, and WooCommerce.
2. Payment gateway: A payment gateway is a service that enables businesses to securely process online payments. Examples include PayPal, Stripe, and Authorize.net.
3. Logistics and fulfillment: E-commerce businesses need to have a logistics and fulfillment system in place to handle the storage, packaging, and shipping of products to customers.
4. Marketing and promotion: E-commerce businesses use various digital marketing techniques, such as search engine optimization (SEO), email marketing, and social media marketing to promote their products and services and drive traffic to their website.
5. Customer service: E-commerce businesses need to provide customers with a good customer service experience. This includes providing information about products and services, answering questions, and handling returns and refunds.
6. Data analytics: E-commerce businesses use data analytics tools to track customer behavior, monitor website performance, and gain insights into customer preferences and trends.
7. Security: E-commerce businesses need to implement security measures to protect customer data and prevent fraud. This includes using encryption and secure payment processing, as well as complying with data privacy laws and regulations.

8. Mobile optimization: E-commerce businesses need to make sure their website is mobile- friendly and easy to navigate on a small screen.

An e-commerce framework is a flexible and adaptable system that allows businesses to evolve with the changing market trends and customer needs. Businesses can use it as a guide to develop their own e-commerce strategy and tailor it to their specific goals and target market.

E-Commerce Consumer Application:

An e-commerce consumer application, also known as an e-commerce app, is a mobile application that enables consumers to shop for products and services directly from their mobile devices. These apps typically provide a user-friendly interface and easy navigation to allow customers to browse products, view details, add items to a shopping cart, and complete transactions.

Some of the features that may be included in an e-commerce consumer application include:

1. **Product browsing:** Customers can browse products by category, brand, price, or other filters.
2. **Product details:** Customers can view detailed information about products, including images, descriptions, and customer reviews.
3. **Shopping cart:** Customers can add items to their shopping cart and review the contents before completing a purchase.
4. **Payment processing:** Customers can securely enter their payment information and complete a transaction within the app.
5. **Order tracking:** Customers can track the status of their orders and view order history.
6. **Customer service:** Customers can access customer service through the app and communicate with the business if they have any questions or concerns.
7. **Personalization:** Customers can create an account and save their preferences, and the app will personalize the shopping experience based on their browsing and purchase history.
8. **Push notifications:** Customers will receive notifications of promotions, deals, and other information that the business wants to share with them.

Many e-commerce consumer apps are integrated with the business's e-commerce platform, allowing the customer to access the same inventory and features as the website. This allows customers to shop on the go and make purchases anytime, anywhere.

E-Commerce Organizational Application:

An e-commerce organizational application is a type of software that businesses can use to manage and streamline their e-commerce operations. These applications can include a wide range of features and functionalities, depending on the specific needs of the business. Some examples of e-commerce organizational applications include:

1. **Inventory management**: Allows businesses to manage and track their inventory levels, set reorder points, and generate reports on stock levels and sales.
2. **Order management**: Allows businesses to manage and track customer orders, from initial purchase to final delivery.
3. **Customer relationship management (CRM):** Allows businesses to manage customer information, track customer interactions, and analyze customer behavior and preferences.

4. **Financial management**: Allows businesses to manage financial transactions, such as invoicing, payments, and accounting.
5. **Supply chain management**: Allows businesses to manage relationships with suppliers, track deliveries, and optimize logistics.
6. **Marketing and promotion**: Allows businesses to create, manage, and track marketing campaigns, such as email campaigns and social media promotions.
7. **Analytics and reporting**: Allows businesses to track key performance indicators (KPIs) such as website traffic, sales, and customer behavior.
8. **Digital asset management**: Allows businesses to store organize and manage digital assets such as images and videos.
9. **Workflow management**: Allows businesses to automate and streamline internal processes, such as order fulfillment and customer service.

These e-commerce organizational applications are designed to help businesses more efficiently manage their operations and make data-driven decisions. They can be integrated with e- commerce platforms, mobile apps, and other software systems, and can be customized accordingly.

Unit-2

The Network Infrastructure of e-Commerce, Payment and Security

What is Information Way?

In the context of information technology (IT), an information way refers to the flow of data between different systems and devices. This includes the technologies, protocols, and standards that are used to transmit, store, and process data, as well as the policies and procedures that are used to manage and protect this data.

Some examples of an information way in IT include:

1. **Network infrastructure**: The physical and logical components that make up a network, such as routers, switches, and cables, that are used to transmit data between different devices and systems.
2. **Data transfer protocols**: Standards that dictate how data should be formatted and transmitted over a network, such as TCP/IP and HTTP.
3. **Data storage systems**: Technologies and solutions used to store data, such as databases, cloud storage, and file servers.
4. **Data processing and analysis**: Applications and tools used to process and analyze data, such as data warehousing, business intelligence, and big data analytics.
5. **Data security**: Measures and protocols that are implemented to protect data from unauthorized access, such as encryption, firewalls, and intrusion detection systems.
6. **Data governance**: Policies and procedures that are used to manage and control the flow of data within an organization, such as data retention and archiving policies.

An information way in IT is essential to ensure the smooth flow of data within an organization and to protect the data from unauthorized access. It requires a balance between security, accessibility and efficiency.

Information SuperHighway (I-Way)

The term "information superhighway" is a metaphor that was popularized in the 1990s to describe the internet and the rapid growth of online information and communication. It was used to convey the idea that the internet was becoming a vast network that would connect people, businesses, and governments around the world, much like a physical highway connects cities and towns. The term was often used to describe the potential of the internet to revolutionize communication, commerce, and education. It also refers to the high-speed communication lines, such as fiber-optic cables, that were being installed to support the growing amount of data and traffic on the internet. The idea behind this was that the internet is like a superhighway, allowing large amounts of information to be transmitted quickly and efficiently over long distances.

Components of the I-Way

- **Network access equipment**
- **Local on-Ramps**
- **Global Information Distribution Network**

Network access equipment

Network access equipment, also known as edge devices, are the hardware and software components that provide a connection between a user or device and a network. These devices are located at the edge of a network and are responsible for providing network access, routing data traffic, and enforcing security policies.

Some examples of network access equipment include:

1. **Routers**: These devices are responsible for directing data traffic between different networks. They use routing protocols to determine the best path for data packets to take and can also be used to connect multiple networks together.

   A router is a networking device that forwards data packets between computer networks. It is connected to two or more networks and determines the best path for a data packet to take based on its destination IP address.

   Routers use routing tables and protocols to determine the most efficient path for data packets to travel. When a data packet is sent from a device on one network to a device on another network, the router receives the packet and consults its routing table to determine the best path to forward the packet.

   The router then uses network protocols such as IP (Internet Protocol) and ICMP (Internet Control Message Protocol) to forward the packet to the next hop on its way to the final destination.

   Routers also have the ability to perform Network Address Translation (NAT) to allow multiple devices on a private network to share a single public IP address. They also provide security by using firewall rules to control access to and from the network.

   Routers also have Quality of Service (QoS) features that allow to prioritize certain types of traffic like video conferencing over others like file downloads; this ensures that critical applications get the bandwidth they need to function properly.

2. **Switches**: These devices are used to connect multiple devices within a network.They forward data packets to the appropriate device based on their MAC address. A switch is a networking device that connects devices on a network and forwardsdata between them. It operates at the data link layer (layer 2) of the OSI model anduses MAC addresses to forward data to the appropriate device. Switches arecommonly used to connect devices in a local area network (LAN) and can also beused to connect LANs to other networks, such as a wide area network (WAN) or theInternet.

3. **Access Points**: These devices are used to provide wireless network access to mobile devices

such as laptops and smart phones. They use wireless protocols such as Wi-Fi and Bluetooth to transmit data.

4. **Firewalls**: These devices are used to enforce security policies and protect a network from unauthorized access. They can be hardware or software-based, and use rules and filters to block or allow specific types of network traffic.
5. **VPN concentrators**: These devices are used to create and manage virtual private networks (VPNs), which allow remote users to securely access a network.
6. **Load balancers**: These devices are used to distribute network traffic across multiple servers, in order to ensure that no single server is overwhelmed.
7. **Proxies**: These devices are used to filter and redirect network traffic, in order to improve network performance and security.

Local on-ramps or Access Media

This is the second components of I-way, Access media is an essential component of the information superhighway, as it refers to the various methods and technologies that allow users to connect to the internet and access the vast amount of information and services available online. They are described into four categories:

1. **Telecom based infrastructure**
   Telecom based infrastructure refers to the physical and technological components that make up a telecommunications network. This helps in transferring the information such as text, audio, video and all other information from the one place to another place.

2. **Cable TV based infrastructure**
   Cable TV based infrastructure refers to the physical and technological components that make up a cable television network this helps on transferring the popular channels data as broadcasting to home.

3. **Wireless infrastructure**
   Wireless infrastructure refers to the physical and technological components that make up a wireless network, which is used to transfer the data using wireless technologies.

4. **Commercial on-line infrastructure**
   Commercial online infrastructure refers to the physical and technological components that make up an e-commerce platform, which includes web servers, database servers, content delivery servers, payment gateway, customer service and support, logistics andfulfillment.

Global Information Distributed Networks

Global information distribution networks (GIDNs) refer to the complex network of systems, technologies and infrastructure that enables the distribution and sharing of information on a global scale. GIDNs are made up of a variety of different components, including:

1. **Data centers**: Large facilities that house servers, storage devices, and networking equipment that store and process data.
2. **Transmission networks**: The physical and wireless infrastructure that connects data centers and other devices, including fiber-optic cables, satellite links, and cellular networks.
3. **Content delivery networks (CDNs):** Distributed systems that help to deliver web content and media to users more efficiently by replicating and caching content on servers located closer tousers.
4. **Network service providers (NSPs):** Companies that own and operate the infrastructure and networks that make up the GIDN, such as internet service providers (ISPs) and cloud providers.
5. **Applications and services:** Platforms and tools that allow users to access and share information, such as social media, search engines, and e-commerce sites.

All these different components work together to create a global network that allows for the rapid and efficient distribution of information to users all around the world.

Network for E-Commerce Peer to

Peer (P2P)

A peer-to-peer (P2P) network is a type of decentralized network in which each participant (peer) can act as both a client and a server. In P2P networks, there is no central server or authority that controls the flow of information; instead, each peer acts as a node that can connect to and communicate with other peers.

Some examples of P2P networks are:

1. **File sharing networks**: P2P networks are often used for file sharing, where users can share and download files directly with each other without the need for a central server.
2. **Decentralized platforms**: Blockchain technologies use P2P network to validate and record transactions, eliminating the need for a central authority.
3. **Collaboration networks**: P2P networks can also be used to enable collaboration among peers, such as in online forums and chat groups.
4. **VoIP**: Some Voice over Internet Protocol (VoIP) services use P2P networks to connect users directly, allowing for free or low-cost calling.

P2P networks are considered more resilient and fault-tolerant than client-server networks as there is no single point of failure. However, they can also present security challenges, as the absence of a central authority makes it more difficult to detect and prevent malicious activity.

Client Server Networks

A client-server network is a type of network architecture in which a central server provides resources and services to multiple clients. The clients, also called workstations, request and consume those resources and services.

In a client-server network, the server is responsible for maintaining and managing the network resources, such as data storage, software applications, and hardware devices. The clients, on the other hand, are responsible for displaying and processing the information provided by the server.

Some examples of client-server networks are:

1. **Corporate networks**: Many businesses use client-server networks to manage and share resources such as files, printers, and databases among employees.
2. **Web services**: In web-based services, web servers provide resources and services to clients through a web browser.
3. **Remote access**: Remote desktop and virtual private networks (VPNs) use client-server architecture to allow remote users to access network resources.
4. **Cloud computing**: Cloud-based services such as Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) use client-server architecture.

A client-server network is considered a centralized network, and it is relatively easy to manage and secure. However, if the central server goes down, the whole network will be affected. Additionally, the network's scalability is limited by the capacity of the central server.

The client-server architecture can be divided into tiers, depending on the number of layers and the distribution of functionality between them. The most common tiers are:

1. **Single-tier**: In this architecture, the client and server functionality is combined into a single program. This is typically used for small applications where the client and server functionality is simple and not expected to change.
2. **Two-tier**: In this architecture, the client and server functionality is separated into two distinct programs. The client program handles the user interface, while the server program handles data storage and business logic. This architecture is commonly used for small to medium-sized applications.
3. **Three-tier**: In this architecture, the client, server and database are separated into three distinct programs. The client program handles the user interface, the server program handles the application logic and communicates with the database, and the database stores the data. This architecture is commonly used for larger and more complex applications.
4. **N-tier**: This is an extension of the three-tier architecture, where the functionality is further divided into multiple tiers. This can include additional application servers, web servers, and other services. This architecture is commonly used for large-scale enterprise applications.

Each tier is designed to handle specific functions, which can make the application more scalable, manageable and secure. The choice of the tier depends on the size and complexity of the application, as well as the expected number of users and the need to handle multiple typesof clients

- **Transaction models**

  Transaction models of e-commerce refer to the different ways in which businesses sell their products and services online. The most common transaction models of e- commerce include:

1. **Business-to-business (B2B):** Business-to-business (B2B) e-commerce refers to the buying and selling of goods or services between companies over the internet. This can include a wide range of activities, from purchasing raw materials and supplies to selling finished products to other businesses. B2B e-commerce is often characterized by high-value transactions, complex products or services, and long-term relationshipsbetween buyers and sellers.

   B2B e-commerce platforms, such as Alibaba and ThomasNet, have become increasingly popular in recent years as a way for businesses to efficiently connect with suppliers, customers, and partners.

2. **Business-to-consumer (B2C):** Business-to-Consumer (B2C) e-commerce refers to the buying and selling of goods and services directly between a business and consumers over the internet. This includes online retail websites, such as Amazon and Walmart, as well as digital marketplaces, such as Etsy and Uber. B2C e-commerce allows businesses to reach a global customer base, offer a wider range of products and services, and provide a convenient and efficient shopping experience for consumers. Many businesses also use B2C e-commerce as away to generate additional revenue streams and increase brand awareness.

3. **Consumer-to-consumer (C2C):** Consumer-to-Consumer (C2C) e-commerce refers to the buying and selling of goods and services directly between consumers over the internet. This can include online marketplaces, such as eBay and Craigslist, as well as social media platforms and mobile apps that enable individuals to sell goods and services to other individuals. C2C e-commerce provides a platform for individuals to buy and sell goods and services without the need for a traditional business intermediary. This can enable consumers to find unique or hard-to-find items and also allows them to sell their own goods and services. C2C e-commerce can also provide a source of additional income for individuals who are looking to make money from their hobbies or interests.

4. **Consumer-to-business (C2B):** Consumer-to-Business (C2B) e-commerce refers to a type of e-commerce where consumers offer goods and services to businesses, instead of the traditional business-to-consumer (B2C) model where businesses offer goods and services to consumers. Examples of C2B e-commerce include online platforms where individuals can sell their products, such as stock photos, videos, and designs to business and websites for freelance work or gig work where individuals can offer their services to businesses. C2B e-commerce can be beneficial for businesses, as they can access a wider pool of talent and resources while also reducing costs. Additionally, it can also be beneficial to individuals, as it allows them to leverage their skills and resources to earn income

5. **Business to Government (B2G):** Business-to-Government (B2G) e-commerce refers to the buying and selling of goods and services between businesses and government entities over the internet. This can include procurement of goods and services such as construction, technology, and consulting services. B2G e-commerce can help government entities to reduce costs, increase efficiency and transparency in procurement process, and also providing businesses with easy access to government procurement opportunities. Many governments around the world have implemented

electronic procurement systems to streamline the procurement process for goods and services. These systems allow businesses to submit bids, invoices, and other documents electronically, making it easier for them to do business with government agencies.

6. **Government to Business (G2B):** Government-to-Business (G2B) e-commerce refers to the buying and selling of goods and services between government entities and businesses over the internet. This can include the provision of services, such as licenses and permits, as well as the sale of government-owned goods and resources. G2B e-commerce can help government entities to increase transparency, reduce costs and increase efficiency in the provision of services to businesses. It also allows businesses to access information and services more easily and quickly. Many governments around the world have implemented electronic systems such as portals, websites, and applications that allow businesses to access government services and information online. Examples of G2B e-commerce services are online businessregistration, tax filing, and compliance reporting.

7. **Government to Government (G2G):** Government-to-Government (G2G) e- commerce refers to the buying and selling of goods and services between different levels of government or different government entities over the internet. This can include the sharing of resources, such as information and personnel, as well as the purchasing of goods and services. G2G e-commerce can help government entities to increase collaboration, reduce costs, and improve the delivery of services to citizens. Many governments around the world have implemented electronic systems such as portals, websites, and applications that allow different government entities to share resources and information, and also to facilitate cooperation on various projects and initiatives. G2G e-commerce can also include inter-governmental procurement and the sharing of common goods and services such as IT, logistics, and security.

- **e-Commerce Payment and Security Issues**

E-commerce payment systems are the methods and technologies used to process and authorize payments made by customers through an e-commerce website. Some common e-commerce payment systems include:

1. **Credit Card**: This is the most widely used e-commerce payment system. It involves customers providing their credit card details to the merchant, and the payment is authorizedby the card issuer.
2. **Debit Card**: Debit card payment is similar to credit card payment, but the funds are taken directly from the customer's bank account.
3. **Electronic Funds Transfer (EFT):** EFT is a method of transferring funds electronically, typically between banks. EFT payments can be made through online banking, direct deposit, and wire transfer.
4. **Digital wallets**: Digital wallets such as PayPal, Apple Pay, and Google Wallet allow customers to store their payment information securely and make payments without entering their details each time.
5. **Smart Card:**
6. **E-Cash:**
7. **E-Cheque:**

Each e-commerce payment system has its own advantages and disadvantages, and the choice of the system depends on the specific requirements of the e-commerce business, such as security, convenience, and cost.

- **Working of Credit Card**

A credit card works by allowing cardholders to borrow funds up to a certain limit in order to make purchases or withdraw cash. The cardholder is responsible for repaying the borrowed funds, plus any interest charges. The process of using a credit card typically involves the following steps:

1. **Application**: The cardholder applies for a credit card with a credit card issuer, such as a bank or credit union. The issuer will check the cardholder's creditworthiness and may approve or deny the application based on this information.
2. **Activation**: Once the cardholder is approved, the issuer will send them a physical credit card and instructions on how to activate it. The cardholder may need to call the issuer or visit a website to activate the card.
3. **Use**: The cardholder can now use their credit card to make purchases at merchants that accept that particular credit card network (Visa, MasterCard, Amex etc).
4. **Authorization**: When a purchase is made, the merchant submits the transaction to the credit card issuer for approval. The issuer then checks the cardholder's available credit limit and creditworthiness, and if approved, sends an authorization code to the merchant to confirm the transaction.

5. **Billing**: The card issuer will bill the cardholder for the purchase at the end of the billing cycle. The cardholder can either pay off the balance in full by the due date, or make a minimum payment and carry over the balance to the next month, incurring interest charges.
6. **Payment**: The cardholder will be responsible for making payments on the credit card account, including any interest charges.

As a reminder, credit card network such as Visa or MasterCard facilitates the transaction between the merchant and the card issuer, and also ensures that the funds are transferred properly. Additionally, credit cards also offer the added benefit of fraud protection, as credit card companies are able to detect and prevent unauthorized transactions.

- **Working of Debit Card**

Debit card is a payment card that deducts money directly from a consumer's checking account to pay for a purchase. Debit cards are linked to the consumer's bank account and can be used to withdraw cash or make purchases at merchants that accept the card. They are often branded with the logo of a major credit card company, such as Visa or MasterCard, and can be used in a similar way to credit cards. However, the funds are withdrawn from the consumer's account immediately, rather than being borrowed from a lender.

A debit card is a payment card that allows cardholders to access funds they have deposited in a bank account. When a consumer uses a debit card to make a purchase, the funds are transferred from the cardholder's bank account to the merchant's account.

The process of using a debit card typically involves the following steps:

1. **Application**: The cardholder applies for a debit card with their bank or credit union. The bank will check the cardholder's account information and may approve or deny the application based on this information.
2. **Activation**: Once the cardholder is approved, the bank will send them a physical debit card and instructions on how to activate it. The cardholder may need to call the bank or visit a website to activate the card.
3. **Use**: The cardholder can now use their debit card to make purchases at merchants that accept that particular debit card network (Visa, MasterCard, Maestro etc).
4. **Authorization**: When a purchase is made, the merchant submits the transaction to the card issuer's network for approval. The issuer then checks the cardholder's available balance and if approved, sends an authorization code to the merchant to confirm the transaction.
5. **Settlement**: The funds are then transferred from the cardholder's bank account to the merchant's account. The cardholder's bank account balance is reduced by the amount of thepurchase.
6. **Reconciliation**: The cardholder's account statement will show the transactions that have been made with the debit card, and the cardholder will reconcile the statement with their bank account balance.

Unlike credit cards, debit cards do not offer credit and cardholders can only spend the amount they have in their account. Also, debit card transactions are not subject to interest charges as it's not borrowing but using the funds that you have in your account.

- **Electronic Fund Transfer**

EFT stands for "Electronic Funds Transfer." It is a method of transferring money between accounts electronically, without the need for a physical check or cash. EFTs can be used to transfer funds between individuals, businesses, or financial institutions.

There are several types of EFTs, including:

- Automated Clearing House (ACH) transactions, which are used for direct deposit of payroll,social security and other government benefits, and other recurring payments.
- Wire transfers, which are used to transfer funds quickly and securely between financial institutions.
- Point-of-sale (POS) transactions, which are used when a consumer makes a purchase with adebit or credit card.

EFTs are generally considered to be a safe and secure way to transfer funds, as they are processed through secure networks and are subject to strict regulations to prevent fraud. They are also convenient, as they can be initiated and completed quickly, often with just a few clicksof a button.

EFT transactions use routing numbers and account numbers to identify the sender and receiver's account, and the transactions happen in real-time. They are also sometimes called as electronic payments or digital payments.

Electronic Fund Transfer (EFT) is a type of electronic payment system that allows for the transfer of money from one bank account to another without the use of paper checks or cash. EFT transactions can be initiated through online banking, mobile apps, or at an ATM.

The process of an EFT typically starts with the sender initiating a transfer from their bank account to the recipient's account. This is done by providing the recipient's account number and routing number, which is a unique identification code that identifies the bank and branch where the account is held.

Once the sender has entered the necessary information, the EFT system will process the transaction and transfer the funds from the sender's account to the recipient's account. The funds are typically available in the recipient's account within a few business days, depending on the financial institution's policies.

EFTs are considered a secure and efficient way to transfer money. They can be used for a variety of purposes such as paying bills, transferring money to friends and family, or for business transactions. Some of the benefits of EFTs include convenience, speed, and areduction in errors and fraud.

Components of EFT

Electronic Fund Transfer (EFT) is a type of electronic payment system that allows the transfer of funds between accounts without the use of physical money or checks. The components of an EFT system include:

1. **Payment originator:** This is the person or organization initiating the EFT, such as a customer making an online purchase.

2. **Payment recipient:** This is the person or organization receiving the EFT, such as a merchant or vendor.

3. **Payment network:** This is the infrastructure that connects the payment originator and recipient, such as the Automated Clearing House (ACH) network.

4. **Financial institutions:** These are the banks or other financial institutions that hold the accounts involved in the EFT, such as the customer's bank and the merchant's bank.

5. **Security measures:** These are the measures in place to ensure the security and integrity of the EFT, such as encryption and authentication.

- **E-Wallets**

- An e-wallet (or digital wallet) is a type of electronic device or online service that allows individuals to make electronic transactions. It stores information such as credit card numbers, shipping addresses, and account balances in one secure place. This information can then be used to make purchases online, in-store, or through mobile devices.

- E-wallets can take the form of a physical device, such as a card or a key fob, or it can be an app or website that can be accessed through a computer or mobile device. They can be linked to a specific bank account, credit card or debit card, or they can be pre-loaded with a certainamount of money.

- Users can use their e-wallets to make purchases online or in-store, as well as to pay bills, transfer money to other people and make other types of transactions. Some e-wallets also offer rewards or cash back for using the service.

- Popular examples of e-wallets include Apple Pay, Google Wallet, PayPal, Alipay and Venmo. These e-wallets are widely accepted and can be used at a variety of merchants, bothonline and in-store.

- Overall, e-wallets provide a convenient way to store and use payment information, they also offer an extra layer of security as the payment information is not shared directly with merchants.

- **Smart Card**

A smart card is a type of payment card that contains an embedded microprocessor or computer chip. These chips can store and process information and they allow for more advanced functionality than traditional magnetic stripe cards.

Smart cards can be used for a variety of purposes, including:

Storing and using credit, debit, or prepaid account information for electronic transactions.Storing

and using loyalty or rewards program information.

Storing and using personal identification information, such as for access control or public transportation.

Storing and using medical information, such as for electronic medical records or prescription drug coverage.

The chip in a smart card can be either contact or contactless type. Contact smart cards have a small gold or silver square on the front or back of the card, which must be physically inserted into a card reader for the card to be read. Contactless smart cards, on the other hand, use radio- frequency identification (RFID) technology to communicate with a card reader without the need for physical contact.

Smart cards are considered to be more secure than traditional magnetic stripe cards as they are difficult to duplicate and the information stored on them is encrypted. They are also used in various industries such as finance, healthcare, transportation and government.

- **E-Cash**

E-cash, or electronic cash, is a digital form of currency that can be used for online transactions. It is designed to mimic the functionality of physical cash, providing a way for users to make anonymous, untraceable payments.

E-cash typically takes the form of a digital token or digital file that is stored on a user's computer or mobile device. When a user wants to make a payment, they provide the e-cash token or file to the merchant, who then verifies the authenticity of the e-cash and processes thetransaction.

There are different types of e-cash systems, some of them are based on digital signatures, which provide a way to ensure the authenticity of the e-cash and prevent fraud. Other types of e-cash are based on encryption technologies, which provide a way to protect the privacy of the user.

E-cash has been around for decades but it never really took off, this is because of the popularity of credit cards and online payment systems like PayPal, which have similar features and are more widely accepted by merchants. Additionally, the development of block chain and crypto currency has opened new possibilities for digital transactions that provide similarfeatures to e-cash.

- **E-Cheque**

- An E-Check (short for electronic check) is an electronic version of a paper check that allows individuals and businesses to make payments over the internet. An E-Check is created when the payer's bank account is debited and the funds are electronically transferred to the payee's bank account. It uses the Automated Clearing House (ACH) network to transfer funds.

- eChecks work similarly to paper checks. The payer provides their bank account information, including routing and account numbers, to the payee. The payee then initiates the eCheck, which debits the funds from the payer's account and transfers them to the payee's account. The process can take several days for the funds to clear, just like traditional paper checks.

- eChecks are considered to be a secure and cost-effective way to make payments, as they are processed through the secure ACH network and are subject to strict regulations to prevent fraud. They can be used for a variety of transactions, such as paying bills, making online purchases, and funding online accounts.

- eChecks can be processed online via an e-commerce platform, or via an automated clearing house (ACH) that allows for businesses and individual to process payments electronically. They are widely accepted and used by merchants and businesses.

- **Risk of Electronic Payment System**

Electronic payment systems, such as online banking, mobile payments, and digital wallets, have become increasingly popular in recent years due to their convenience and ease of use. However, with this increased usage, there are also potential risks associated with electronic payment systems. Some of the risks include:

1. **Fraud:** Electronic payment systems are vulnerable to fraud, such as phishing scams, where criminals try to steal personal and financial information.
2. **Hacking:** Electronic payment systems are also vulnerable to hacking, which can lead to unauthorized access to personal and financial information.
3. **Data breaches:** Electronic payment systems store sensitive personal and financial information, which can be exposed in the event of a data breach.
4. **Technical problems:** Electronic payment systems can also be prone to technical problems, such as system failures or glitches, which can result in delays or errors in processing transactions.
5. **Privacy concerns:** Electronic payment systems may also raise concerns about privacy, as the use of digital transactions can be tracked and recorded, thus exposing personal information.

To mitigate these risks, it is important to use electronic payment systems that have strong security measures in place, such as encryption and secure servers, and to be vigilant in protecting personal and financial information. Additionally, regularly checking account statements and reporting any suspicious activity promptly can also help protect against fraud.

- **Security on web**

Security is a critical concern for electronic payment systems (EPS) such as credit cards, debit cards, e-wallets, eChecks and smart cards, as they involve the transfer of sensitive financial information over the internet.

To protect against fraud and unauthorized transactions, EPS providers employ a variety of security measures, including:

- **Encryption**: EPS providers use encryption to protect sensitive information as it is transmitted over the internet. This makes it difficult for hackers to intercept and read the information.
- **Secure Socket Layer (SSL) and Transport Layer Security (TLS**): These protocols are used to create a secure connection between the user's web browser and the EPS provider's website. This helps to prevent eavesdropping and tampering of information during transmission.
- **Two-factor authentication:** This requires users to provide two forms of identification in order to access their account, such as a password and a one-time code sent to their phone.
- **Risk management:** EPS providers use advanced algorithms and machine learning to detect and prevent fraud in real-time. This includes monitoring transactions for suspicious patterns and using fraud scoring to identify high-risk transactions.
- **PCI-DSS Compliance:** Payment Card Industry Data Security Standards (PCI-DSS) compliance is a set of security standards that ensure that merchants, service providers, and other organizations that handle credit and debit card information maintain a secure environment.

It's also important for users to take steps to protect their own information, such as by keeping their computer and mobile device secure, avoiding phishing scams, and being wary of giving out personal information online.

Overall, EPS providers use a variety of security measures to protect user's information, but it's important for users to also take the necessary steps to protect their own information.

- **SSL**

  - Secure Sockets Layer (SSL) is a security protocol that is used to establish a secure and encrypted connection between a web server and a web browser. The purpose of SSL is to ensure that all data passed between the web server and browser remains private and integral.

  - When a user connects to a website that uses SSL, the browser and the web server establish an SSL connection using a process called an SSL Handshake. During the SSL Handshake, the browser and web server exchange information to establish a secure connection. This includes the browser providing the web server with a copy of the SSL certificate, which the web server uses to verify the identity of the website.

  - Once the SSL Handshake is completed, the browser and web server will use the established SSL connection to encrypt all data that is exchanged between them. This means that any sensitive information, such as login credentials or credit card information, is encrypted before it is transmitted over the internet. This ensures that the data cannot be intercepted and read by anyone other than the intended recipient.

- SSL was succeeded by Transport Layer Security (TLS) which is an updated version of SSL, but the two terms are often used interchangeably. SSL and TLS are implemented in web browsers and servers to create a secure connection and protect sensitive data in transit.

- Websites that use SSL or TLS are identified by the prefix "https" in the URL, and the padlock icon in the browser address bar. Websites that use SSL or TLS are considered more secure and trustworthy than those that do not.

Secure Socket Layer Protocol:

- **SSL Record Protocol**

  The SSL Record Protocol is a component of the Secure Sockets Layer (SSL) protocol that is responsible for the fragmentation, compression, and encryption of data exchanged between the client and server. The SSL Record Protocol works in conjunction with the SSL Handshake Protocol and the SSL Change Cipher Spec Protocol to establish a secure connection and exchange data.

  The main components of the SSL Record Protocol include:

  - **Record Layer**: This is the layer that provides the core security services of the SSL protocol, including data fragmentation, compression, and encryption.

  - **Data Fragmentation**: The Record Protocol fragment the application data into manageable chunks before it is encrypted, this is done to avoid exceeding the maximum transmission unit (MTU) of the underlying network.

  - **Data Compression**: The Record Protocol can also apply data compression to the application data before it is encrypted, this can improve performance by reducing the amount of data that needs to be transmitted.

  - **Data Encryption**: The SSL Record Protocol uses symmetric key encryption to encrypt the application data. The encryption algorithm and key are agreed upon during the SSL Handshake Protocol.

  - **Data Integrity**: The SSL Record Protocol uses a message authentication code (MAC) to ensure that the data has not been tampered with during transmission.

  - **Data format**: The SSL Record Protocol defines a specific format for the data that is sent and received. This format includes fields for the SSL version number, the length of the data, and the data itself, as well as the MAC for data integrity check.

- **Handshake Protocol**

The SSL Handshake Protocol is a component of the Secure Sockets Layer (SSL) protocol that is responsible for the establishment of a secure connection between the client and server. The Handshake Protocol works in conjunction with the SSL Record Protocol and the SSL Change Cipher Spec Protocol to establish a secure connection andexchange data.

The main components of the SSL Handshake Protocol include:

- **Client Hello**: This is the initial message sent by the client to initiate the SSL Handshake. The Client Hello message includes information about the client's SSL version, supported cipher suites, and a random number called the client random.

- **Server Hello**: This is the message sent by the server in response to the Client Hello. The Server Hello message includes information about the server's SSL version, the chosen cipher suite, and a random number called the server random.

- **Certificate**: This is the message sent by the server to provide its digital certificate to the client. The certificate includes information about the identity of the server and a public key that can be used to encrypt the data.

- **Server Key Exchange**: This is an optional message sent by the server in some cases when the server has no certificate or the certificate doesn't contain the public key.

- **Server Hello Done**: This is the message sent by the server to indicate that the server hello and certificate message (if applicable) are finished.

- **Client Key Exchange**: This message sent by the client after the server hello done, to provide the pre-master secret to the server, that both parties will use to generate the session key.

- **Change Cipher Spec**: This is a message sent by both the client and the server to indicate that all future messages will be encrypted using the session key.

- **Finished**: This is a message sent by both the client and the server to indicate the completion of the SSL Handshake.

Once the SSL Handshake is completed, the SSL Record Protocol is used to encrypt and decrypt data exchanged between the client and server.

- **Change Cipher Protocol**

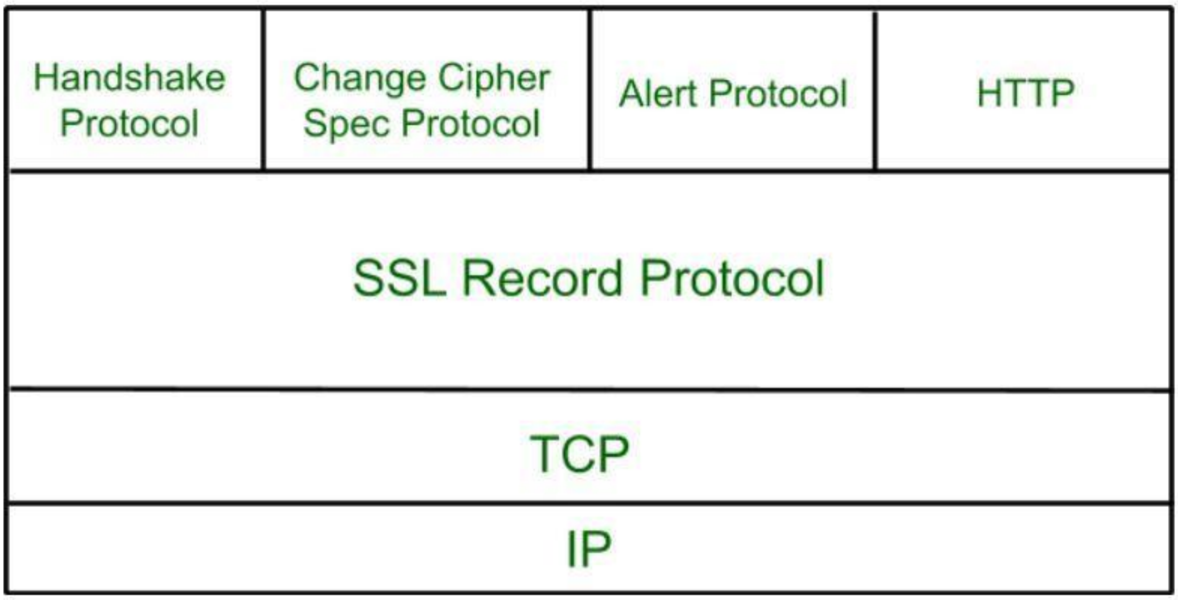
- The SSL (Secure Sockets Layer) Change Cipher Spec Protocol is a part of the SSL/TLS (Transport Layer Security) protocol suite used to provide secure communications on the internet. It is used to signal the end of the SSL/TLS handshake process and the beginning of the secure data transfer phase.

- The Change Cipher Spec Protocol is used to notify the other party that the sender will start using new cryptographic parameters for the secure data transfer. This is done by sending a single message, called the Change Cipher Spec message, whichconsists of a single byte with the value 1.

- When the Change Cipher Spec message is received, the recipient of the message will use the new cryptographic parameters (e.g. keys and algorithms) to secure the data that is sent and received over the SSL/TLS connection. This ensures that the data is protected by the strongest and most up-to-date cryptographic algorithms available.

- **Alert Protocol**

  The SSL (Secure Sockets Layer) Alert Protocol is a part of the SSL/TLS (Transport Layer Security) protocol suite used to provide secure communications on the internet. It is used to convey important information and error messages between the client and server during the SSL/TLS handshake process. The SSL Alert Protocol defines a set of alert messages that can be sent by either the client or server to indicate the status of the SSL/TLS connection, such as a handshake failure or a certificate problem. It uses a 2 byte format with the first byte being the level (warning or fatal) and the second byte being the description of the alert.



What is SSL?

SSL (Secure Sockets Layer) is a protocol for establishing secure communications over the internet. It was developed in the 1990s and was widely used to provide secure connections for web browsers and other internet applications. In 1999, SSL was succeeded by TLS (Transport Layer Security), which is considered to be a more secure and robust protocol for establishing secure connections.

The main purpose of SSL/TLS is to provide a secure channel for data transmission between a client (e.g. a web browser) and a server (e.g. a web server) by using a combination of public- key and symmetric-key encryption.

In general, SSL/TLS is used to encrypt the data being sent and received between a client and server, to authenticate the server to the client, and to provide integrity protection for the data being transmitted. SSL/TLS is often used to protect sensitive information such as login credentials, credit card numbers, and other personal information when it is transmitted over theinternet.

It is generally enabled by installing a SSL/TLS certificate on the server. It will make sure that the data sent and received is encrypted, and the identity of the server is verified using the certificate.

Why we need SSL?

The need for SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security) is to provide a secure channel for data transmission between a client and a server over the internet. This is important for a number of reasons:

- **Data encryption**: SSL/TLS encrypts the data being sent and received between a client and server, making it difficult for anyone to intercept and read the data. This is especially important when sensitive information such as login credentials, credit card numbers, and other personal information is being transmitted.

- **Server authentication**: SSL/TLS is used to authenticate the server to the client, ensuring that the client is communicating with the intended server and not an imposter. This helps to prevent man-in-the-middle attacks.

- **Data integrity**: SSL/TLS provides integrity protection for the data being transmitted, which helps to detect any tampering or modification of the data in transit.

- **Compliance**: Some compliance regulations like PCI-DSS, HIPAA etc, require to use SSL/TLS for online transactions and data transfer.

- **Trust**: Having an SSL/TLS certificate on your website gives a sense of trust and assurance to the customers that their information is safe with you.

In summary, SSL/TLS is used to protect the confidentiality, integrity and authenticity of the data being transmitted over the internet, which is crucial for maintaining security and privacy in online transactions.

SSL Layered Architecture

The SSL (Secure Sockets Layer) protocol has a layered architecture that consists of several different layers, each of which serves a specific purpose in establishing a secure connection between a client and a server. The main layers of the SSL protocol include:

1. **Record Protocol**: This layer is responsible for breaking up the data into smaller, manageable blocks called records and then encrypting and authenticating each record.

2. **Handshake Protocol**: This layer is responsible for negotiating the cryptographic parameters (e.g. keys and algorithms) that will be used to secure the connection. It also authenticates the server to the client.

3. **Alert Protocol**: This layer is used to convey important information and error messages between the client and server during the SSL/TLS handshake process.

4. **Change Cipher Spec Protocol**: This layer is used to signal the end of the SSL/TLS handshake process and the beginning of the secure data transfer phase.

5. **Application Layer**: This layer is where the actual application-specific data is exchanged between the client and server. The data passed through this layer is protected by the cryptographic parameters established during the Handshake Protocol.

Each layer of the SSL/TLS protocol is built on top of the previous layer and provides additional functionality. Together, these layers work to provide a secure, authenticated, and private channel for the exchange of information between a client and a server over the internet.

Unit 3 Introduction to Cyber Crimes

- **Introduction to Cyber Crimes**

Cybercrime, also known as computer crime, refers to any illegal activity that involves the use of computers, networks, or the internet. It encompasses a wide range of criminal activities such as hacking, identity theft, cyber stalking, cyber bullying, and the spread of malware. These crimes can be committed by individuals or groups, and can have serious consequences for both individuals and organizations. With the increasing use of technology in our daily lives, cybercrime has become a growing concern. It is important for individuals and organizations to be aware of the risks and to take steps to protect themselves. This can include using strong passwords, keeping software updated, and being cautious when clicking on links or opening attachments.

- **History of Cyber Crime**

The history of cybercrime can be traced back to the early days of the internet and computer technology. Here are a few key milestones in the history of cybercrime:

1. **1960s**: The first computer viruses and worms began to appear. These early forms of malware were primarily created as pranks or experiments, but they laid the foundation for more malicious forms of cybercrime.
2. **1970s**: The first cases of hacking and unauthorized access to computer systems began to be reported. This was the beginning of cybercrime as we know it today.
3. **1980s**: The first instances of computer fraud and identity theft began to be reported. The development of online banking and e-commerce also made it easier for criminals to steal money and personal information.
4. **1990s**: The World Wide Web and the rise of the Internet made it easier for criminals to perpetrate cybercrime on a global scale. Phishing, spamming, and other forms of online fraud became more prevalent.
5. **2000s**: The use of the Internet and mobile devices became widespread, and cybercrime began to evolve to take advantage of these new technologies. Malware, ransomware and APT became common, data breaches became more frequent.
6. **2010s**: social media and IoT made it easier for cybercriminals to target individuals and organizations on a massive scale. Cybercrime became a major concern for governments and businesses around the world.
7. **2020s**: With more people working from home and using online tools, cybercrime has become more prevalent and sophisticated. Ransomware attacks, BEC and phishing campaigns have become more common.

- **Technical aspects of Cyber Crimes**

The technical aspects of cybercrime involve the use of computer technology and networks tocommit illegal activities. Some examples of these technical aspects include:

1. **Hacking**: unauthorized access to a computer or network, often with the intent to steal or corrupt data.
2. **Malware**: malicious software such as viruses, worms, and trojans that can damage or steal information from a computer or network.
3. **Phishing**: the use of fake emails or websites to trick individuals into providing personal or financial information.
4. **Social Engineering**: tricking people into divulging sensitive information or performing actions that they wouldn't normally do
5. **Distributed Denial of Service (DDoS) attacks**: overwhelming a website or online service with traffic to make it unavailable to users.
6. **Ransomware**: malware that encrypts a victim's files, making them inaccessible until a ransom is paid.
7. **Advanced Persistent Threats (APT**): a set of stealthy and continuous computer hacking processes, often orchestrated by human attackers, targeting a specific entity.
8. **Internet of Things (IoT) attacks**: targeting vulnerabilities in IoT devices, such as smart home devices, to gain unauthorized access to networks.

These are just a few examples of the technical aspects of cybercrime. It's important to note that these tactics and technologies are constantly evolving, and new forms of cybercrime are emerging all the time.

<u>Modes of cyber crime</u>

There are several modes through which cybercrime can be committed:

1. **Social Engineering**: This is the use of psychological manipulation to trick individuals into divulging personal or sensitive information or performing actions that they wouldn't normally do. This can include phishing scams, vishing (voice phishing), and pretexting (creating a false identity to gain trust).
2. **Remote Access**: This involves gaining unauthorized access to a computer or network from a remote location. This can include hacking, malware, and ransomware.
3. **Physical Access**: This involves gaining access to a computer or network by physically accessing the device, such as through the use of USB drives or other removable media.
4. **Insider Threat**: This is when an individual with authorized access to a computer or network uses that access to commit cybercrime. This can include employees, contractors, or other insiders.
5. **Supply Chain Attack**: This is when a cyber criminal targets a third-party vendor or supplier that has access to an organization's network and uses them as an entry point to launch an attack.
6. **Cloud-based attacks**: This is when a cyber criminal targets a cloud-based service such as software as a service (SaaS), infrastructure as a service (IaaS), or platform as a service (PaaS) to gain unauthorized access to a network or steal data.
7. **IoT attacks**: This is when a cyber criminal targets vulnerability in IoT devices to gain unauthorized access to a network.
8. **Crypto jacking**: This is the unauthorized use of someone else's computer to mine crypto currency.

Again, these categories are not mutually exclusive, and an incident can have multiple elements from different categories. Additionally, these tactics and technologies are constantly evolving, and new forms of cybercrime are emerging all the time.

Difference between Cyber Crime and Traditional Crime

Cybercrime and traditional crime are both illegal activities, but they differ in several key ways:

1. **Location**: Traditional crime typically takes place in a physical location, such as a bank or a store. Cybercrime, on the other hand, can take place anywhere that has an internet connection, making it a more borderless and international phenomenon.
2. **Modus Operandi**: Traditional crime often involves physical force or the threat of force, while cybercrime typically relies on technology and the manipulation of information.
3. **Target**: Traditional crime often targets individuals or physical assets, while cybercrime may target computer systems, networks, and data.
4. **Evidence**: Evidence collection is different in both types of crime. Traditional crime involves collecting physical evidence such as fingerprints, DNA, and other physical trace, while in cybercrime, the evidence is digital and forensic analysis is needed to collect evidence.
5. **Impact**: Traditional crime can have a localized impact, while cybercrime can have a global impact, affecting multiple individuals and organizations at once.
6. **Punishment**: Punishment for traditional crime is usually served in the form of imprisonment or fines, while cybercrime punishment is not always as clear cut, and can depend on the country's laws and regulations.

In summary, while traditional crime and cybercrime both involve illegal activities, they differ in terms of location, modus operandi, target, evidence and impact, and the way they are punished.

- **Unauthorized access & Hacking**

Unauthorized access and hacking refer to the act of gaining unauthorized access to a computer or network. Hacking can be done for a variety of reasons, such as to steal personal information, cause damage to a computer or network, or to use the resources of the computer or network for malicious purposes.

Unauthorized access can be achieved through a variety of methods, such as guessing or cracking passwords, exploiting vulnerabilities in software or hardware, or using malware to gain access.

Hacking can be divided into different categories based on the intent and methods used, such as:

- **White hat hacking**: done by ethical hackers to identify vulnerabilities in a system and helpimprove its security.

- **Black hat hacking**: done by malicious hackers with the intent of causing harm or stealing information.
- **Gray hat hacking**: done by hackers who may or may not have malicious intent, but who donot have permission to access the systems they are hacking.

It's important for individuals and organizations to take steps to protect themselves against unauthorized access and hacking. This can include using strong passwords, keeping software updated, and being cautious when clicking on links or opening attachments. Additionally, it's also a good practice to regularly perform security audits and penetration testing to identify vulnerabilities in your systems and to implement security measures to mitigate them.

Virus, Trojan and Worm Attacks

- **Virus**

  A computer virus is a type of malware that is designed to replicate itself and spread to other computers. Once a computer is infected with a virus, it can cause a variety of problems, such as slowing down the performance of the computer, corrupting or deleting files, and stealing personal information. Some viruses are relatively harmless and simply display annoying messages or change the appearance of the computer's desktop, while others can cause serious damage.

  A computer virus is typically spread through email attachments, infected software or apps, and malicious websites. Once a computer is infected, the virus can spread to other computers by sending itself to contacts in an email address book, or by spreading through a network.

  There are different types of viruses, such as:

  - **File infector viruses**: These viruses infect executable files, such as .exe and .com files, and replicate themselves when the infected file is run.
  - **Boot sector viruses**: These viruses infect the boot sector of a disk, which is the area of the disk that is used to start the computer. They replicate themselves by installing a copy of the virus in the boot sector of any disk that is inserted into the infected computer.
  - **Macro viruses**: These viruses infect documents, such as those created in Microsoft Word or Excel, and replicate themselves by infecting other documents that are opened on the infected computer.
  - **Stealth viruses**: These viruses use techniques to evade detection by anti-virussoftware, by hiding themselves or disguising their activities.
  - **Polymorphic viruses**: These viruses can change their appearance or code to evade detection by anti-virus software.
  - **Ransom ware**: These are a type of malware that encrypts the victims' files and demands a ransom to be paid to provide the decryption key.

  - **Rootkits**: These are a type of malware that can hide itself and other malicious software on the infected system, making it difficult to detect and remove.
  - **Adware and Spyware**: These are a type of malware that can track the user's browsing activity and display unwanted ads or steal personal information.

It's important to have up-to-date anti-virus software installed on your computer and to practice safe browsing habits to protect against computer viruses. This includes avoiding suspicious email attachments and links, keeping software updated, and being cautious when downloading files from the internet.

- **Trojan**

A Trojan, or Trojan horse, is a type of malware that disguises itself as legitimate software in order to gain access to a computer or network. Once it has infiltrated the system, a Trojan can perform a variety of malicious actions, such as stealing personal information, installing other malware, or giving hackers remote access to the infected computer.

Unlike viruses, which replicate and spread on their own, Trojans are typically spread through social engineering tactics, such as tricking the user into downloading and installing the malware. They can be disguised as legitimate software or as a software update, and are often spread through email attachments, instant messages, or maliciouswebsites.

There are different types of Trojan, such as:

- **Remote Access Trojans (RATs)**: These Trojans allow an attacker to gain remote access to the infected computer, allowing them to control the computer, steal information, or install other malware.
- **Banking Trojans**: These Trojans are designed to steal financial information, such as login credentials for online banking.
- **Downloader Trojans**: These Trojans download and install other malware, such as viruses and spyware, on the infected computer.
- **Backdoor Trojans**: These Trojans open a "backdoor" on the infected computer, allowing an attacker to gain unauthorized access.
- **Dropper Trojans**: These Trojans are used to install other malware by "dropping" the malware onto the infected computer.
- **Information stealing Trojans**: These Trojans are designed to steal personal information such as login credentials, credit card details and other sensitive information.
- **Rootkit Trojans**: These Trojans are a type of malware that can hide itself and other malicious software on the infected system, making it difficult to detect and remove.
- **Crypto jacking Trojans**: These Trojans are designed to perform crypto mining operations by using the infected computer's resources without the user's knowledge.

- **Worm**

A worm is a type of malware that is designed to replicate itself and spread to other computers. It is similar to a computer virus in that it can cause a variety of problems, such as slowing down the performance of the computer, corrupting or deleting files, and stealing personal information. Unlike viruses, which typically need a host file to replicate, worms can replicate and spread on their own, often through networks and theinternet.

Worms are typically spread through email attachments, infected software or apps, and malicious websites. They can also spread through vulnerabilities in networked systems, such as patched software or weak passwords. Once a computer is infected, the worm can spread to other computers by sending itself to contacts in an email address book, or by spreading through a network.

There are different types of worms, such as:

- **Email worms**: spread through email attachments or links
- **Network worms**: spread through networks
- **Instant messaging worms**: spread through instant messaging
- **File-sharing worms**: spread through peer-to-peer file sharing networks

It's important to have up-to-date anti-virus software installed on your computer and to practice safe browsing habits to protect against computer worms. This includes avoiding suspicious email attachments and links, keeping software updated, and being cautious when downloading files from the internet.

- **E-mail related Crimes**

Email-related crimes refer to illegal activities that involve the use of email or other forms ofelectronic communication. Some examples of email-related crimes include:

1. **Phishing:** the use of fake emails or websites to trick individuals into providing personal or financial information.
2. **Business Email Compromise (BEC):** a type of phishing attack where the attacker poses as a legitimate business or executive to trick employees into transferring funds or providing sensitive information.
3. **Email fraud:** sending fraudulent emails to trick individuals into sending money or providing personal information.
4. **Email spoofing:** creating fake emails that appear to be from a legitimate source in order to trick individuals into providing personal or financial information.
5. **Spamming:** sending unsolicited emails in bulk, often for the purpose of advertising or phishing.
6. **Email bombing:** sending a large number of emails to a specific email address in order to overload the recipient's inbox and disrupt their ability to use email.
7. **Email extortion**: threatening to release sensitive information unless a ransom is paid.

These are just a few examples of email-related crimes, but it's important to note that these tactics and technologies are constantly evolving, and new forms of email-related crimes are emerging all the time. To protect yourself from email-related crimes, it's important to be cautious when clicking on links or opening attachments in emails, especially if they come from unknown sources. Additionally, it's a good practice to use anti-spam and anti-phishing softwareand to be aware of the latest scams and threats.

- **E-mail Spoofing and Spamming E-mail**

Spoofing

- Email spoofing is a technique used by cybercriminals to create fake emails that appear to be from a legitimate source, such as a bank, a government agency, or a well-known company. The goal of email spoofing is to trick individuals into providing personal or financial information, or into clicking on a link or opening an attachment that contains malware.

- There are different ways to spoof an email, but the most common method is to use a technique called "spoofing the sender address" (or "spoofing the From field"), which involves forging the "From" field in the email header so that it appears to be from a legitimate source. This can be done by manipulating the Simple Mail Transfer Protocol (SMTP) and by using software that allows for the creation of custom email headers.

- Email spoofing can also be done through "phishing" attacks, in which a fraudster sends an email that appears to be from a legitimate source, with the intention of tricking the recipient into providing personal or financial information.

- To protect yourself from email spoofing, it's important to be cautious when clicking on links or opening attachments in emails, especially if they come from unknown sources. Additionally, it is a good practice to use anti-spam and anti-phishing software, and to be aware of the latest scams and threats. It is also advisable to hover over the sender's email address to check the actual email address, and not the displayname.

E-mail Spamming

- Email spamming refers to the practice of sending unsolicited emails in bulk, often for the purpose of advertising or phishing. These emails are typically sent to many email addresses at once, and they can be sent from a single sender or from a network of compromised computers (botnet).

- Spam emails can take many forms, but they are often used to advertise products or services, to promote scams or fraud, or to spread malware. They can also be used to phish for personal information, such as login credentials or financial information.

- Spammers use various techniques to send spam emails, such as using email lists that they have purchased or harvested from the internet and using software that can automatically send emails to large numbers of recipients. They can also use botnets, networks of compromised computers that can be controlled remotely, to send spamemails.

- Receiving spam emails can be annoying and can also be a security risk, as they may contain malware or phishing links. To protect yourself from spam emails, it's important to be cautious when clicking on links or opening attachments in emails, especially if they come from unknown sources. Additionally, it's a good practice to use anti-spam software and to be aware of the latest scams and threats. Also, it's advisable to mark the email as spam or unsubscribe if the option is available.

E-mail Bombing

- Email bombing refers to the practice of sending many emails to a specific email address in order to overload the recipient's inbox and disrupt their ability to use email. The goal of email bombing is to flood the recipient's inbox with so many emails that they are unable to access their legitimate messages or to cause the email service to crash or become unavailable.

- Email bombing can be done manually or using automated scripts or software. In a manual email bombing, the attacker will repeatedly send emails to the target address, often from multiple email accounts. Automated email bombing can be done by using software that can repeatedly send emails to a target address, often from a botnet (a network of compromised computers).

- Email bombing can be a form of cyber-harassment and can cause serious disruptions to the targeted individual or organization. It can also consume a significant amount of network resources, causing the targeted server to crash or become unavailable.

- To protect yourself or your organization from email bombing, it is important to have proper email filtering and security measures in place. This may include using anti- spam software, rate limiting, and IP blocking. Additionally, it is important to be aware of the signs of email bombing and to report any suspicious activity to your email service provider or to the authorities.

There are three methods of an email bombing:

1. **Mass Mailing:**

   Mass mailing is the process of sending many emails to many recipients simultaneously. This can be done for a variety of reasons, such as promoting a product or service, sharing important news or information, or sending marketing or promotional messages. Mass mailing can be done using email marketing software or services, which can automate the process of sending emails and manage large lists of recipients.

2. **List linking:**

   List linking is a technique used in email bombing to evade detection and blocking by email servers. It involves using multiple lists of email addresses to send emails, rather than a single list. This can make it more difficult for email servers to detect and block the emails, as the attack is coming from multiple sources.

3. **Zip bombing:**

Zip bombing, also known as "compression bombing" or "file bombing," is a type of email bombing that involves sending many small files in a compressed format, such as a ZIP file, to a target email address or server. The goal of this type of attack is to overload the recipient's email server or storage capacity, causing the server to crash or become unresponsive.

The compressed file may contain many small files, such as text files or images, which can be used to consume a large amount of storage space and cause the email server to crash. The compressed file can also contain malware or other malicious code that can infect the recipients' systems whenthe file is opened.

- **Denial of Service Attacks**

- **Distributed Denial of Service Attacks**

Refer in Unit 4

- **Various Crimes:**

- **IPR Violations: Software Piracy, Copyright infringement, Trademarks Violations,Theft of computer source code, Patent violations**

Intellectual property rights (IPR) violation refers to the unauthorized use, distribution, or infringement of a person or organization's legally protected intellectual property. This can include patents, trademarks, copyrights, trade secrets, and other forms of proprietary information.

In the context of cybercrime, IPR violation can take many forms. For example, individuals or organizations may use the internet to distribute copyrighted material, such as movies, music, or software, without permission from the rights holder. This is known as piracy and it is illegal in most countries.

IPR violation can also occur through trademark infringement, where a company or an individual uses a trademark that is similar to an existing one, in order to mislead customers and gain commercial advantage.

Another form of IPR violation is patent infringement, where a person or an organization uses or sells a patented invention or process without permission from the patent holder.

IPR violation is a serious crime and can result in significant financial losses for the rights holder. It is punishable by law and can lead to fines, legal penalties and even imprisonment.

- **Software Piracy:**

Software piracy refers to the unauthorized use, distribution, or reproduction of copyrighted software. This can include downloading and installing software from unlicensed sources, such as torrent sites or peer-to-peer networks, as well as making copies of software and distributing them to others.

When an individual or organization uses pirated software, they are not only violating copyright law, but they are also breaking the terms of the software license agreement. This can lead to several legal and financial consequences, including fines, legal penalties, and even imprisonment.

Software piracy can also have a significant impact on the software industry, as it results in lost revenue for software companies and can also harm the economy. Some software companies even lose money due to piracy which can hamper the innovation and development of new software.

It's important to note that using unlicensed or pirated software also poses a security risk as it may be infected with malware or other malicious software, which can harm the user's computer or steal sensitive information.

- **Copyright Infringement:**

Copyright infringement refers to the unauthorized use, distribution, or reproduction of copyrighted material. This can include movies, music, books, artwork, software, and other forms of creative expression that are protected by copyright laws.

In the context of the internet, copyright infringement can take many forms. For example, individuals or organizations may use the internet to distribute copyrighted material, such as movies, music, or software, without permission from the rights holder. This is known as online piracy, and it is illegal in most countries. Other examples include reproducing and distributing copyrighted material, such as books or music, on peer-to-peer networks, or sharing copyrighted files on cloud storage sites without permission.

Copyright infringement can also occur when someone uses copyrighted material without permission for commercial gain, like using copyrighted music on a YouTube channel without permission from the rights holder.

Copyright infringement is a serious crime and can result in significant financial losses for the rights holder. It is punishable by law and can lead to fines, legal penalties and even imprisonment.

It's important to note that copyright laws vary by country and region, and it's always best to check the local laws before using or distributing copyrighted material.

- **Trademark Violation:**

Trademark violation, also known as trademark infringement, refers to the unauthorized use of a trademark that is like an existing one, in order to mislead customers and gain commercial advantage. A trademark is a legally protected symbol, word, or phrase that is used to identify and distinguish a company's products or services from those of itscompetitors.

In the context of the internet, trademark infringement can take many forms. For example, individuals or organizations may use a similar trademark to that of an established company in order to sell counterfeit goods or services online. This can be particularly prevalent in e- commerce platforms, where it can be difficult to differentiate between genuine and fake products.

Trademark infringement can also occur when someone uses a trademarked name or logo in an online ad or social media post without permission, or when a company uses a similar name or logo for their business, in order to confuse customers and gain an unfair advantage.

Trademark violation is a serious crime and can result in significant financial losses for the rights holder, as well as damage to their reputation. It is punishable by law and can lead to fines, legal penalties and even imprisonment.

It's important to note that trademark laws vary by country and region, and it's always best to check the local laws before using or registering a trademark.

- **Computer Source code Theft:**

Computer source code theft refers to the unauthorized access, duplication, or use of proprietary source code, which is the underlying programming instructions that make a computer program or software work. Source code is considered intellectual property and isprotected by copyright laws.

Source code theft can occur in various ways, such as an employee of a company stealing source code before leaving the company, or an outsider hacking into a company's computer systems to access and steal source code.

Source code theft can have serious consequences for the affected company. It can lead to financial losses, as the stolen code may be used to create competing products or services. It can also harm the company's reputation and lead to legal action.

Additionally, it can also pose a security risk, as stolen source code may contain vulnerabilities that can be exploited by hackers or cybercriminals to gain unauthorized access to the systems or to steal sensitive information.

It's important to note that source code theft is a serious crime, and it is punishable by law. Companies should take steps to protect their source code, such as implementing access controls, using encryption, and regularly monitoring their systems for any unauthorized access.

- **Patent Violation:**

Patent violation, also known as patent infringement, refers to the unauthorized use or sale of a patented invention or process without permission from the patent holder. A patent is a legally protected right granted to an inventor or company that gives them exclusive rights to prevent others from making, using, or selling an invention for a certain period of time.

In the context of the internet, patent infringement can occur when an individual or company uses or sells a patented invention or process without permission online. This can include manufacturing or selling products that use a patented technology or process or using a patented invention or process to provide a service.

Patent infringement can also occur when a company imports or sells products that were made using a patented process or technology without permission.

Patent infringement can have serious consequences for the affected company or individual. It can lead to financial losses, as well as legal action from the patent holder. It can also harm the company's reputation and can lead to injunctions, fines, or even imprisonment.

It's important to note that patent laws vary by country and region, and it's always best to check the local laws before using or selling a patented invention or process. Additionally, it's important to conduct a patent search to ensure that the invention or process is not already patented by someone else.

- **Cyber Squatting**

Cybersquatting, also known as domain squatting, is the act of registering, trafficking in, or using a domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else. This typically involves registering domain names that are similar or identical to existing trademarks, with the intent to sell the domain name to the trademark owner or a competitor at a higher price, or to use the domain name to divert traffic to another website for commercial gain.

Cyber squatting can be a serious issue for businesses and individuals, as it can harm their reputation and lead to lost revenue. It can also make it difficult for customers to find a legitimate website and can lead to confusion and frustration.

In addition to registering domain names that are similar or identical to existing trademarks, cyber squatters may also register domain names that are misspellings or variations of existing trademarks, or that use variations of top-level domains (TLDs) such as .com, .net,
.org, etc.

There are laws and regulations in place to combat cyber squatting, such as the Anticybersquatting Consumer Protection Act (ACPA) in the United States and the Uniform Domain-Name Dispute-Resolution Policy (UDRP) established by the Internet Corporation for Assigned Names and Numbers (ICANN) that allows trademark owners to file a complaint with a dispute resolution service provider.

It's important to note that businesses and individuals should take steps to protect their trademarks and domain names by regularly monitoring for potential cyber squatting activities and taking legal action if they suspect they are a victim of cyber squatting.

- **Banking/ Credit card related crimes**

Banking-related cybercrime refers to criminal activities that involve the unauthorized access or theft of financial information from banks or other financial institutions. These crimes can take many forms, including phishing scams, which use fraudulent emails or websites to trick victims into providing their personal or financial information, or malware attacks, which use malicious software to infect a victim's computer and steal information.

Another common type of banking-related cybercrime is account takeover, in which a criminal gains unauthorized access to a victim's bank account and transfers funds out of the account without the victim's knowledge. Also, ATM skimming is another form of cybercrime in which criminals use small devices called skimmers to steal card informationwhen people use ATMs.

These types of cybercrime can result in significant financial losses for both individuals and financial institutions. To prevent such crimes, banks and other financial institutions employ various security measures such as encryption, firewalls, and multi-factor authentication to protect their systems, and also educate customers on how to spot and avoid scams.

- **Defamation (Cyber Smearing)**

Cyber defamation is the act of making false and damaging statements about someone on the internet. This can include statements made on social media, in online forums or comments, or on websites. The statements can be in the form of text, images, or videos. The defamatory statements can be about an individual, a company, or a group of people and can be seen by many people who can cause serious harm to the reputation, credibility, and financial stability of the person or entity being defamed. Unlike traditional defamation, which can be difficult to prove, cyber defamation is often easier to trace, as it leaves a digital footprint. Cyber defamation is considered a form of online harassment and can have serious consequences for the person being defamed such as legal action, emotional distress,and financial loss.

- **Cyber Stalking**

Cyber stalking is the use of technology, particularly the internet, to harass, intimidate, or threaten someone. It is a form of online harassment and can take many forms, such as sending threatening emails or messages, posting defamatory information or personal details about the victim online, or using social media to harass or intimidate the victim. Cyber stalking can also involve tracking the victim's online activity, creating fake social media accounts to harass them, or using technology to surveil the victim. Cyber stalking can have serious consequences for the victim, such as emotional distress, fear, and even physical harm. It is a criminal offense in many countries and may also be considered a civilwrong, which can lead to legal action being taken against the perpetrator.

The National Center for Victims of Crime (NCVC) suggests that victims of cyber stalkingtake the following steps:

- For minor, inform parents or a trusted adult.
- File a complaint with the cyber stalker’s Internet service provider.
- Collect evidence, document instances, and create a log of attempts o stop the harassment.
- Present documentation to local law enforcement and explore legal avenues.
- Get a new email address and increase privacy settings on public sites.
- Purchase privacy protection software.
- Request removal from online directories.

- **Cyber Terrorism**

Cyber terrorism is the use of digital technology to disrupt or damage critical infrastructure or to create widespread fear and panic. This can include hacking into government or financial systems, spreading malware or viruses, or using social media to spread false information or propaganda. The goal of cyber terrorism is to cause physical or economic harm and to disrupt the normal functioning of society.

Examples of cyber terrorism include:

1. Hacking into critical infrastructure systems, such as power grids or water treatment plants, with the intent to cause disruptions or damage.
2. Launching a distributed denial-of-service (DDoS) attack to flood a website or network with traffic, making it inaccessible to users.
3. Spreading malware or viruses that can compromise sensitive information or disrupt the normal functioning of computer systems.
4. Using social media to spread false information or propaganda in order to create fear and panic among the population.
5. Attacking financial systems such as banks and stock markets, with the intent of causing economic harm.
6. Cyber espionage: steal sensitive information from government and private organizations
7. Encrypting malware: Ransom ware attack by locking the victims' data or systems, the cyber-criminals demand a ransom to release the data or systems.
8. Cyber-physical attack: hacking into a physical device or system that is controlled by computer systems and making changes that can cause physical damage or injury.

These are just a few examples, and the threat of cyber terrorism is constantly evolving as technology and tactics change.

- **Investment Fraud:**

Investment fraud refers to any form of deception or misrepresentation that is used toinduce individuals or institutions to invest money or assets in a venture or scheme that is not legitimate. This can include Ponzi schemes, pyramid schemes, insider trading, and various forms of stock manipulation. Investment frauds often involve false promises of high returns with little or no risk and may target individuals or groups whoare inexperienced or unsophisticated investors. Investment fraud can result in significant financial losses for those who are defrauded.

Examples of investment fraud include:

1. **Ponzi schemes:** a fraudulent investment operation where returns are paid to existing investors from funds contributed by new investors, rather than from profit earned by the operator.
2. **Pyramid schemes:** a form of investment in which each person involved recruits others to join. Money made by the new member’s funnels up to the higher members.
3. **Insider trading:** buying or selling securities based on material, nonpublic information.
4. **Stock manipulation:** artificially inflating or deflating the price of a stock through illegal means, such as spreading false information or insider trading.
5. **Oil and gas investment scams:** Promising high returns on investments in oil and gas wells that don’t exist or have little chance of success.
6. **Promissory note fraud:** fraud involving investments in promissory notes, which are private debt securities that promise to, pay a fixed or variable rate of interest.
7. **Real estate investment scams:** Promising high returns on investments in property developments that don’t exist or have little chance of success.
8. **Affinity fraud:** targeting victims who belong to a specific group or community, such as religious or ethnic groups.

These are just a few examples, and new types of investment frauds are constantly emerging as fraudsters come up with new ways to scam investors.

Unit 4: Concept of Cyber Security

- **Basic Terminologies**
  - **IP Address:** An IP address, or Internet Protocol address, is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. This address serves two main purposes: host or network interface identification and location addressing. In simpler terms, it's a unique identifier for a device (such as a computer, Smartphone, or printer) on a network.

    IP addresses come in two main types: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). IPv4 addresses are composed of four sets of numbers separated by periods (e.g., 192.168.0.1), while IPv6 addresses are longer and use a different format to accommodate the growing number of devices connected to the internet.

    IP addresses enable devices to communicate with each other over a network by allowing data to be sent and received. They play a crucial role in routing and directing internet traffic, ensuring that information reaches its intended destination.

  - **MAC Address:** A MAC (Media Access Control) address is a unique identifier assigned to a network interface card (NIC) for communications at the data link layer of a network segment. It is also known as the hardware address, Ethernet address, or physical address.

    MAC address is generally fixed for a specific piece of hardware. MAC addresses are crucial for the proper functioning of network protocols like Ethernet, as they help in the delivery of data frames to the correct destination within a local network.

  - **Domain Name Server (DNS):** DNS stands for Domain Name System. It is a hierarchical system that translates human-readable domain names, like www.example.com, into numerical IP addresses that computers use to identify each other on a network. DNS plays a crucial role in making the internet more user-friendly by allowing us to use domain names instead of remembering complex IP addresses.

  - **DHCP:** DHCP stands for Dynamic Host Configuration Protocol. It is a network management protocol used to automate the process of assigning IP addresses and other configuration parameters to devices on a network. The primary goal of DHCP is to simplify the administration of IP addresses in a network by dynamically assigning them to devices as they connect.
    Here's how DHCP typically works:
    1. **Request by a Device**: When a device (such as a computer, Smartphone, or printer) connects to a network, it sends a DHCP request to the network seeking an IP address and other configuration information.
    2. **DHCP Discovery**: The device broadcasts a DHCP discover message to the

network, indicating that it needs an IP address.

3. **DHCP Offer**: DHCP servers on the network respond with a DHCP offer, providing an available IP address, subnet mask, gateway address, DNS server information, and other configuration parameters.
4. **Request Acceptance**: The device selects one of the offered IP addresses and sends a DHCP request to the chosen DHCP server, informing it that it wants to use the offered configuration.
5. **DHCP Acknowledgment**: The DHCP server acknowledges the request by sending a DHCP acknowledgment (DHCP ACK) message to the device, confirming the assignment of the IP address and providing the requested configuration information.
6. **Configuration and Lease**: The device configures its network interface with the assigned IP address and other parameters. DHCP leases are usually temporary, and the device must renew the lease periodically.

DHCP simplifies the management of IP addresses in a network, especially in environments where devices frequently connect and disconnect. It helps prevent IP address conflicts and ensures efficient use of available IP addresses by dynamically allocating them as needed. DHCP is commonly used in both wired and wireless networks to automate the IP address assignment process.

- ROUTER: A router is a networking device that connects different networks together and directs data traffic between them. It operates at the network layer (Layer 3) of the OSI model and is crucial for routing data between devices on a local network and devices on other networks, such as the internet.

- BOTs: The term "bots" refers to automated software programs that perform tasks on the internet. These tasks can range from simple and repetitive actions to more complex and sophisticated functions. Bots are designed to operate autonomously, without direct human intervention, and they can be programmed for various purposes. Here are some common types of bots:

1. **Web Crawling Bots**: Search engines use web crawling bots to index and catalog web pages. These bots visit websites, analyze their content, and index the information to make it searchable.
2. **Chat bots:** Chat bots are programs designed to simulate conversation with human users. They are often used for customer support, virtual assistants, or interactive services on websites and messaging platforms.
3. **Social Media Bots:** Bots on social media platforms can perform various tasks, including automated posting, liking, and following. Some social media bots are used for legitimate purposes, while others may be employed for spamming or manipulating social media metrics.
4. **Malicious Bots:** Some bots are created for malicious purposes, such as spreading malware, conducting distributed denial-of-service (DDoS) attacks, or engaging in other forms of cybercrime.
5. **Trading Bots:** In the financial world, trading bots are used to execute automated trades on stock exchanges or crypto currency markets. These bots can analyze market data and execute trades at high speeds.
6. **Gaming Bots:** Bots can be used in online gaming to automate certain tasks, gain advantages, or perform repetitive actions. This can sometimes lead to unfair game play and is often discouraged by game developers.
7. **Spam bots:** Spam bots are designed to generate and distribute spam, often through email or online forums. They can flood communication channels with unsolicited and often irrelevant messages.

It's important to note that while some bots serve positive and constructive purposes, others can be used for harmful or unethical activities. The term "bot" itself is neutral, and its impact depends on how the bot is programmed and used. As technology evolves, the development and deployment of bots continue to shape various aspects of our digital interactions.

Cyber Security: Cyber security is the practice of protecting computer systems, networks, and data from digital attacks, unauthorized access, damage, or theft. It encompasses a wide range of technologies, processes, and practices designed to safeguard information and ensure the confidentiality, integrity, and availability of data. The field of cyber security is dynamic and constantly evolving as new threats and vulnerabilities emerge alongside advancements in technology.

- **Types of Threats:** There are various types of cyber threats that individuals, organizations, and governments may face. These threats can target different aspects of information technology systems, networks, and data. Here are some common types of cyber threats:

  - **Malware:** Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. Examples include viruses, worms, trojans, ransom ware, and spyware.
  - **Phishing:** Deceptive attempts to trick individuals into providing sensitive information, such as usernames, passwords, or financial details, by posing as a trustworthy entity.
  - **Ransom ware:** Malware that encrypts a user's files or entire system, rendering it inaccessible until a ransom is paid to the attacker, who claims to have the decryption key.
  - **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks:** Overwhelming a system, network, or website with traffic to disrupt its normal functioning, making it temporarily or permanently unavailable.
  - **Man-in-the-Middle (MitM) Attacks:** Intercepting and potentially altering communication between two parties without their knowledge, compromising the confidentiality and integrity of the data being transmitted.
  - **SQL Injection:** Exploiting vulnerabilities in web applications by injecting malicious SQL code into input fields, potentially allowing attackers to manipulate databases.
  - **Cross-Site Scripting (XSS):** Injecting malicious scripts into web pages that are viewed by other users, allowing attackers to steal information or perform actions on behalf of the victim.
  - **Zero-Day Exploits:** Taking advantage of vulnerabilities in software or hardware that are not yet known to the vendor or have not been patched.
  - **Social Engineering**: Manipulating individuals to divulge confidential information or perform actions that may compromise security, often through psychological manipulation.
  - **IoT (Internet of Things) Threats:** Exploiting vulnerabilities in connected devices, such as smart home devices or industrial IoT devices, to gain unauthorized access or disrupt operations.
  - **Insider Threats:** Malicious or unintentional actions by individuals within an organization, such as employees or contractors, who may compromise security.
  - **Advanced Persistent Threats (APTs):** Sophisticated, long-term cyber-attacks carried out by well-funded and organized groups with specific targets, often for espionage or data theft.
  - **Credential Stuffing:** Using automated tools to try large sets of username and password combinations, exploiting individuals who reuse passwords across multiple platforms.
  - **Fileless Malware:** Malicious software that operates in the computer's memory, leaving little or no trace on the system's hard drive, making it harder to detect.
  - **Supply Chain Attacks:** Compromising the security of a target by exploiting vulnerabilities in its supply chain, often by infiltrating and compromising a trusted third-party vendor.

Staying informed about these types of threats and implementing robust cyber security measures is crucial for effectively mitigating the risks associated with the evolving cyber threat landscape.

- **Common Types of Attacks**

  - **Distributed denial of service attack**

    A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a targeted system, service, or network by overwhelming it with a flood of illegitimate requests or traffic. The primary goal of a DoS attack is to make a resource (such as a website, server, or network) unavailable to its intended users, causing a denial of service.

How Do DoS Attacks Impact Businesses and Users?

DoS attacks can have severe consequences for businesses and users alike. Here are some impacts of DoS attacks:

- Loss of Revenue: DoS attacks can cause businesses to lose significant amounts of revenue as customers are unable to access their website or service.
- Damage to Reputation: DoS attacks can damage a company's reputation and erode the trust of its customers.
- Financial Losses: The cost of mitigating a DoS attack can be significant, and businesses may also have to pay for lost revenue, legal fees and damages.
- Disruption of Critical Services: DoS attacks can disrupt critical services, such as healthcare and emergency services, which can have life-threatening consequences.
- Loss of Data: Data destruction attacks can cause businesses to lose critical data, leading to financial losses and damage to the company's reputation.

Preventing DoS Attacks: There are several measures businesses can take to prevent DoS attacks, including:

- Implementing DDoS protection solutions that can detect and mitigate DoS attacks in real time.
- Ensuring their website and network infrastructure is up-to-date with the latest security patches.
- Using strong authentication mechanisms, such as multi-factor authentication, to prevent unauthorized access to the network.
- Monitoring network traffic to detect unusual patterns and take immediate action to prevent potential attacks.

A Denial of Service (DoS) attack is a type of cyber-attack in which an attacker attempts to make a computer or network resource unavailable to its intended users by overwhelming it with traffic. The goal of a DoS attack is to disrupt the normal functioning of a website, service, or a network, making it unavailable to legitimate users.

There are different types of DoS attacks, such as:

DoS attacks can be launched from a single device or from a network of compromised devices (botnet), and they can be difficult to prevent or mitigate. Some techniques that can be used to protect against DoS attacks include:

1. **Flooding attacks:** These attacks involve overwhelming a network or server with a large amount of traffic. The attacker can use a single device to flood the target with traffic or use a botnet (a network of compromised devices) to amplify the attack. Examples of flooding attacks include:
   1. **ICMP Flood:** The attacker sends many ICMP echo request packets (ping) to the target, overwhelming the network and causing it to becomeunavailable.

    2. **UDP Flood:** The attacker sends many UDP packets to a target, overwhelming the network and causing it to become unavailable.
    3. **SYN Flood:** The attacker sends many SYN packets to a target, overwhelming the network and causing it to become unavailable.

2. **Amplification attacks:** These attacks involve using a network of infected devices (botnet) to amplify the traffic to the target. Examples of amplification attacks include:

    1. **DNS Amplification:** The attacker sends many DNS requests to open DNS resolvers, which then respond to the target, overwhelming it with traffic.
    2. **NTP Amplification**: The attacker sends many NTP requests to open NTP servers, which then respond to the target, overwhelming it with traffic.
    3. **SNMP Amplification:** The attacker sends many SNMP requests to open SNMP servers, which then respond to the target, overwhelming itwith traffic.

3. **Application layer attack:** An Application-layer Denial of Service (DoS) attack is a type of DoS attack that targets specific vulnerabilities in a website or application. This type of attack is designed to exploit weaknesses in the application layer of the OSI model and can cause the targeted application or website to become unavailable or slow down. Examples of Application-layer DoS attacks include:

    1. **HTTP Flood:** The attacker sends many HTTP requests to a website, overwhelming the server and causing it to become unavailable.
    2. **Slowloris**: The attacker opens many connections to a web server and keeps them open, using minimal bandwidth. This causes the server's resources to become exhausted and the website becomes unavailable.
    3. **POST Flood:** The attacker sends many POST requests to a website, overwhelming the server and causing it to become unavailable.

DoS attacks can be launched from a single device or from a network of compromised devices (botnet), and they can be difficult to prevent or mitigate. Some techniques that can be used to protect against DoS attacks include:

- Network traffic filtering: blocking traffic that appears to be part of a DoS attack
- Rate limiting the number of requests that can be made to a server or network
- Scrubbing services: redirecting traffic to a network that can filter and block malicious traffic
- Firewall: protecting the network from unwanted traffic

It is important to note that DoS attacks can be very sophisticated and can change form over time, so it's important to have a proactive approach and to have an incident response plan in place.

<u>Distributed Denial of Service Attack (DDOS):</u> A distributed denial-of-service (DDoS) attack is a type of cyber attack in which many compromised devices, often referred to as "zombies," are used to flood a targeted website or network with traffic. The goal of a DDoS attack is to overwhelm the targeted website or network with so much traffic that it is unable to function properly and becomes inaccessible to legitimate users. DDoS attacks can be launched from a single location or from multiple locations simultaneously, which makes them difficult to prevent and mitigate.

There are several ways to protect against Distributed Denial of Service (DDoS) attacks:

1. **Use a DDoS protection service:** Many companies offer DDoS protection services that can detect and block incoming DDoS traffic before it reaches yournetwork.
2. **Use a Content Delivery Network (CDN**): A CDN can absorb some of the traffic generated by a DDoS attack and can also help to distribute traffic across multiple servers, making it more difficult for an attacker to take down your website.
3. **Use a firewall:** A firewall can be configured to block or limit incoming traffic from suspicious IP addresses, which can help to mitigate the effects of a DDoS attack.
4. **Use rate limiting:** Implement rate limiting on your servers and network devices to limit the amount of traffic that can be sent to your website or network.
5. **Use traffic shaping:** Traffic shaping is a technique that can be used to prioritize important traffic and drop less important traffic during a DDoS attack.
6. **Monitor your network:** Regularly monitor your network for any signs of a DDoS attack, such as a sudden increase in traffic or a decrease in website performance.
7. **Have an incident response plan:** Having an incident response plan in place and practiced can help you quickly respond to a DDoS attack, minimize the damage, and get your services back online as soon as possible.
8. **Keep software and systems updated:** Keep all software and systems up to date to protect against known vulnerabilities that could be exploited by attackers.

It's important to remember that DDoS attacks can come in many forms, and there is no single solution that can protect against all types of attacks. A combination of different methods and techniques is often necessary to provide adequate protection.

Difference between DoS and DDoS

Some of the common differences between DoS and DDoS are mentioned below.

DoS	**DDoS**
DoS Stands for Denial of service attack.	DDoS Stands for Distributed Denial of service attack.
In Dos attack single system targets the victim system.	In DDoS multiple systems attack the victim's system.
Victim's PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from Multiple locations.
Dos attack is slower as compared to DDoS.	A DDoS attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
In DOS Attack only a single device is used with DOS Attack tools.	In a DDoS attack, The volume Bots are used to attack at the same time.

DoS	DDoS
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace.
Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack 4. Flooding Attack	Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks 4. Protocol Attack.

- **Man in the middle attack**

  A Man-in-the-Middle (MitM) attack is a type of cyber security attack where an unauthorized entity intercepts and possibly alters the communication between two parties without their knowledge. The attacker positions themselves between the communication flow, allowing them to eavesdrop on, manipulate, or even inject malicious content into the data being exchanged.

Types of MitM:

1. **Internet Protocol spoofing.** Like identity theft, IP spoofing takes place when cybercriminals alter the source IP address of a website, email address or device for the purpose of masking it. This dupes the users into believing that they are interacting with a legit source and the sensitive information they share during the transaction gets transferred to the cybercriminals instead.
2. **Domain Name System spoofing.** This is a type of man-in-the-middle attack where cybercriminals alter domain names to redirect traffic to fake websites. Users might think that they are reaching a secure and trusted website, but instead, they land on a website operated by cybercriminals. The main aim behind DNS spoofing is to reroute traffic to a fake website or to capture user login credentials.
3. **HTTP spoofing.** The HTTP protocol is the embodiment of secure internet communications. HTTPS indicates a safe and trusted website. During an HTTPS spoofing attack, a browser session is redirected to an unsecured or HTTP-based website without the user's knowledge or consent. Cybercriminals can monitor user interactions and steal shared personal information through this redirection.
4. **Secure Sockets Layer hijacking.** SSL is a protocol that establishes an encrypted connection between a browser and the web server. During SSL hijacking, a cybercriminal might use another computer and a secure server to intercept all information traveling between the server and the end user's computer.
5. **Email hijacking.** This is a type of MiTM attack where cybercriminals gain control of email accounts of banks and other financial institutions to monitor any transactions that users conduct. Cybercriminals

may even spoof the bank's email address and send instructions to customers that lead them to unknowingly transfer their money to the cybercriminals.

6. **Wi-Fi eavesdropping.** This MiTM attack is one of the many risk factors posed by public Wi-Fi. During this attack, public Wi-Fi users get tricked into connecting to malicious Wi-Fi networks and hotspots. Cybercriminals accomplish this by setting up Wi-Fi connections with names that resemble nearby businesses.

7. **Session hijacking.** Also known as stealing browser cookies, this malicious practice takes place when cybercriminals steal personal data and passwords stored inside the cookies of a user's browsing session. Sometimes, cybercriminals can gain endless access to users' saved resources. For example, they might steal users' confidential data and identities, purchase items or steal money from their bank accounts.

8. **Cache poisoning.** Also known as Address Resolution Protocol, or ARP cache poisoning, this popular modern-day MiTM attack enables cybercriminals who are on the same subnet as the victims to eavesdrop on all traffic being routed between them.

○ **Password attack**

A password attack is a cyber security attack in which an attacker attempts to gain unauthorized access to a user's account or system by exploiting vulnerabilities in password security. Passwords are commonly used as a means of authentication, and compromising them can lead to unauthorized access, data breaches, and potential misuse of sensitive information.

Here are some common types of password attacks:

- **Brute Force Attack:**

  In a brute force attack, the attacker systematically tries all possible combinations of passwords until the correct one is found. This method can be time-consuming, but it's effective if the password is weak and doesn't have sufficient complexity.

- **Dictionary Attack:**

  A dictionary attack involves using a predefined list of commonly used passwords or words from dictionaries. The attacker tries each word in the list until they find the correct one. This approach is more efficient than brute force and targets common or easily guessable passwords.

- **Credential Stuffing:**

  In a credential stuffing attack, attackers use username and password pairs obtained from previous data breaches or leaks to gain unauthorized access to other accounts where users have reused the same credentials. This type of attack exploits the common practice of using the same password across multiple services.

- **Phishing Attacks:**

  Phishing attacks involve tricking users into revealing their passwords by posing as a trustworthy entity. This can be done through deceptive emails, fake websites, or other means. Once the user enters their credentials, the attacker captures and uses them.

- **Key logging:**

  Key loggers are malicious software or hardware that record keystrokes on a computer or device. By capturing the keystrokes, attackers can obtain passwords as users type them.

- **Rainbow Table Attack:**

  Rainbow tables are precompiled tables containing the hash values of many possible passwords. In a rainbow table attack, the attacker compares the hash of the target password with entries in the table to find a match, effectively bypassing the need to hash each password individually.

  - **Mail attack**

Electronic mail (email) is a digital messaging system that allows users to send and receive messages via the Internet. Email communications are sent and received by email servers, available from all Internet Service Providers (ISP).

Emails are sent between two separate server folders: the senders and the recipients. A sender saves, transmits, or forwards email messages, whereas a recipient accesses an email server to view or download emails.

Some types of emails attack are as under:

1. **Phishing Attacks:**

- **Email Phishing:** Attackers send deceptive emails that appear to be from a legitimate source, aiming to trick recipients into revealing sensitive information, such as usernames, passwords, or financial details.
- **Spear Phishing:** A targeted form of phishing where attackers tailor their messages to a specific individual or organization. They use information gathered from reconnaissance to make the phishing attempt more convincing.

- **Business Email Compromise (BEC):** Attackers compromise or impersonate high-level executives within an organization to trick employees into transferring funds, disclosing sensitive information, or initiating other harmful actions.

  - **Malware**
    Malware attacks are any type of malicious software designed to cause harm or damage to a computer, server, client or computer network and/or infrastructure without end-user knowledge.

Types of Malware Attacks

Most malware types can be classified into one of the following categories:

- **Virus:** When a computer virus is executed, it can replicate itself by modifying other programs and inserting its malicious code. It is the only type of malware that can "infect" other files and is one of the most difficult types of malware to remove.
- **Worm:** A worm has the power to self-replicate without end-user involvement and can infect entire networks quickly by moving from one machine to another.
- **Trojan:** Trojan malware disguises itself as a legitimate program, making it one of the most difficult types of malware to detect. This type of malware contains malicious code and instructions that, once executed by the victim, can operate under the radar. It is often used to let other types of malware into the system.
- **Hybrid malware:** Modern malware is often a "hybrid" or combination of malicious software types. For example, "bots" first appear as Trojans then, once executed, act as worms. They are frequently used to target individual users as part of a larger network-wide cyber attack.
- **Adware:** Adware serves unwanted and aggressive advertising (e.g., pop-up ads) to the end-user.
- **Malvertising:** Malvertising uses legitimate ads to deliver malware to end-user machines.
- **Spyware:** Spyware spies on the unsuspecting end-user, collecting credentials and passwords, browsing history and more.
- **Ransom ware:** Ransomware infects machines, encrypts files and holds the needed decryption key for ransom until the victim pays. Ransom ware attacks targeting enterprises and government entities are on the rise, costing organizations millions as some pay off the attackers to restore vital systems. Cyptolocker, Petya and Loky are some of the most common and notorious families of ransomware.

Examples of Malware Attacks

Here are just a few of the many types of malware cyber attackers use to target sensitive data:

- **Pony malware** is the most commonly used malware for stealing passwords and credentials. It is sometimes referred to as Pony Stealer, Pony Loader or FareIT. Pony malware targets Windows machines and collects information about the system and the users connected to it. It can be used to download other malware or to steal credentials and send them to the command and control server.
- **Loki**, or Loki-Bot, is an information-stealing malware that targets credentials and passwords across approximately 80 programs, including all known browsers, email clients, remote control programs and file sharing programs. It has been used by cyber attackers since 2016 and continues to be a popular method for stealing credentials and accessing personal data.
- **Krypton Stealer** first appeared in early 2019 and is sold on foreign forums as malware-as-a-service (MaaS) for just $100 in cryptocurrency. It targets Windows machines running version 7 and above

and steals credentials without the need for admin permissions. The malware also targets credit card numbers and other sensitive data stored in browsers, such as browsing history, auto-completion, download lists, cookies and search history.

- **Triton malware** crippled operations at a critical infrastructure facility in the Middle East in 2017 in one of the first recorded malware attacks of its kind. The malware is named after the system it targets – Triconex safety instrumented system (SIS) controllers. These systems are used to shut down operations in nuclear facilities, oil and gas plants in the event of a problem, such as equipment failure, explosions or fire. The Triton malware is designed to disable these failsafe mechanisms, which could lead to physical attacks on critical infrastructure and potential human harm.

How to Prevent Malware Attacks

To strengthen malware protection and detection without negatively impacting business productivity, organizations often take the following steps:

- Use anti-virus tools to protect against common and known malware.
- Utilize endpoint detection and response technology to continuously monitor and respond to malware attacks and other cyber threats on end-user machines.
- Follow application and Operating System (OS) patching best practices.
- Implement the **principle of least privilege** and **just-in-time access** to elevate account privileges for specific authorized tasks to keep users productive without providing unnecessary privileges.
- Remove local administrator rights from standard user accounts to reduce the attack surface.
- Apply application greylisting on user endpoints to prevent unknown applications, such as new ransomware instances, from accessing the Internet and gaining the read, write and modify permissions needed to encrypt files.
- Apply application whitelisting on servers to maximize the security of these assets.
- Frequently and automatically backup data from endpoints and servers to allow for effective disaster recovery.

- **Hackers**: a person who uses computers to gain unauthorized access to data. Many hackers who break in to computers hope to steal money, access information, or hold files for ransom.
  - **Injection attacks**

    This type of attack allows an attacker to inject code into a program or query or inject malware onto a computer in order to execute remote commands that can read or modify a database, or change data on a web site.

    - Blind SQL Injection
    - Blind XPath Injection
    - Buffer Overflow
    - Format String Attack
    - LDAP Injection
    - OS Commanding
    - SQL Injection
    - SSI Injection
    - XPath Injection

  - **Breach in authentication Protocol**

    An authentication protocol allows the receiving party (such as a server) to verify the identity of another party (such as a person using a mobile device to log in). Almost every single computer system uses some kind of network authentication to verify users.

As more critical information is stored electronically, and as hackers become more and more adept at theft, authentication becomes more important. Without it, losses can be significant. For example, Deloitte experienced a data breach in 2017 that exposed client email (including some tied to government agencies). Authentication may never keep your information perfectly secure. But it can make theft harder to accomplish. Hackers may move to a different target if your servers are too difficult to penetrate

A breach of authentication occurs when unauthorized individuals exploit vulnerabilities to gain access to systems, risking the compromise of sensitive data and other critical functionalities.

- **Types of Hackers:**

  - **White Hat**

    White hat hackers engage in **legal hacking to improve digital security** for those who contract them. They are paid to infiltrate digital systems to identify potential security vulnerabilities and report their findings to their clients. White hat hacking allows companies and organizations to patch security weaknesses before they can be exploited by malicious hackers.

    For example, an insurance firm might hire a white hat hacker to simulate annual attacks in order to ensure their clients' personal information is secure. White hat hacking is based on consent — clients make a request and are aware that an attempt will be made to hack their systems.

  - **Black Hat**

    Black hat hackers are **cybercriminals who orchestrate scams and exploit vulnerabilities** with the intent to cause harm. The aim of black hat hackers is usually to make money. They do this in many ways, but most involve stealing money outright, cracking passwords to access information that can be sold on the dark web, or holding sensitive data for ransom.

    Black hats are the most dangerous hackers, and they typically go to great lengths to hide their identities — it's extremely rare that a hacker would openly chat with you. They sometimes band together into hacker groups to pull off large-scale hacks.

    Businesses have the most to lose from hacking, as they hold large amounts of our personal data. But individuals can be hacked as well. Black hat hackers often gain access to larger systems by hacking individual devices like phones and routers. Email accounts are also popular targets for hackers.

Unit 5

- **Ethical Hacker**

Ethical hackers use their knowledge to secure and improve the technology of organizations. They provide an essential service to these organizations by looking for vulnerabilities that can lead to a security breach. An ethical hacker reports the identified vulnerabilities to the organization.

- **Advantages of being an ethical hacker:**

Ethical hackers are well recognized in their profession for their job of protecting the system. Below are the advantages of being an ethical hacker:

- Prevent harmful cyber attacks.
- Prevent penetration attacks of intruders.
- Find loopholes in the system and repair them with their expertise.
- Establish security and safety measures within the system.
- Prevent cyber terrorism and hacks from taking place.

○ **Roles and Responsibilities**

Ethical Hackers Role:

- **In-depth Knowledge of Security:** Ethical hackers should be well versed with potential threats and vulnerabilities that can hack organizational systems. Ethical hackers are hired by organizations for their expertise skills and quick resolution to security vulnerabilities. They should be cyber security professionals having knowledge of the computer systems, network and security.
- **Think like Hackers:** The primary role of Ethical hackers is to attack the system like hackers, without adopting authorized methods. They are supposed to think like hackers who want to steal confidential data /information. Ethical hackers look for areas that are most likely to be attacked and the different ways in which attack can take place.
- **In-depth Knowledge of the Organization they intend to provide Service:** Ethical hackers should be well versed with the services of the functional working of the organization they are associated with. It should have the knowledge about the information that is extremely safe and needs to be protected. Ethical hackers should be capable of finding the attack methods for accessing the sensitive content of the organization.

Ethical Hackers Responsibilities:

- **Hacking their own Systems:** Ethical hackers hack their own systems to find potential threats and vulnerabilities. They are hired to find vulnerabilities of the system before they are discovered by hackers.
- **Diffuse the intent of Hackers**: Ethical hackers are hired as a Precautional Step towards Hackers, who aim at breaching the security of computers. Vulnerabilities when detected

early can be fixed and safe confidential information from being exposed to hackers who have malicious intentions.

- **Document their Findings:** Ethical hackers must properly document all their findings and potential threats. The main part of the work they are hired by the organizations is proper reporting of bugs and vulnerabilities which are threat to the security.
- **Keeping the Confidential Information Safe:** Ethical hackers must oblige to keep all their findings secure and never share them with others. Under any kind of situation they should never agree to share their findings and observations.
- **Sign Non-Disclosure Agreements**: They must sign confidential agreements to keep the information they have about the organizations safe with them. This will prevent them to give -out confidential information and legal action will be taken against them if they indulge in any such acts.
- **Handle the loopholes in Security:** Based on their observations, Ethical hackers should restore/ repair the security loopholes. This will prevent hackers from breaching the security of the organization from attacks.

○ Benefits of Ethical Hacking

Following are the benefits of Ethical hacking:

- This helps to fight against cyber terrorism and to fight against national security breaches.
- This helps to take preventive action against hackers.
- This helps to build a system that prevents any kinds of penetration by hackers.
- This offers security to banking and financial establishments.
- This helps to identify and close the open holes in a computer system or network.

○ Skills require to become Ethical hacker

1. Computer Networking Skills

One of the most important skills to become an ethical hacker is networking skills. The computer network is nothing but the interconnection of multiple devices, generally termed as Hosts connected using multiple paths to send/receive data or media. Understanding networks like DHCP, Suoernetting, Subnetting, and more will provide ethical hackers to explore the various interconnected computers in a network and the potential security threats that this might create, as well as how to handle those threats.

2. Computer Skills

Computer skills are knowledge and ability which allow one to use computers and related technology. Typically, basic computer skills include data processing, managing computer files, and creating presentations. Advanced computer skills include managing databases, programming, and running calculations in spreadsheets. Some of the most essential computer skills are MS Office, Spreadsheets, Email, Database Management, Social Media, Web, Enterprise systems, etc. An ethical hacker needs to be a computer systems expert.

3. Linux Skills

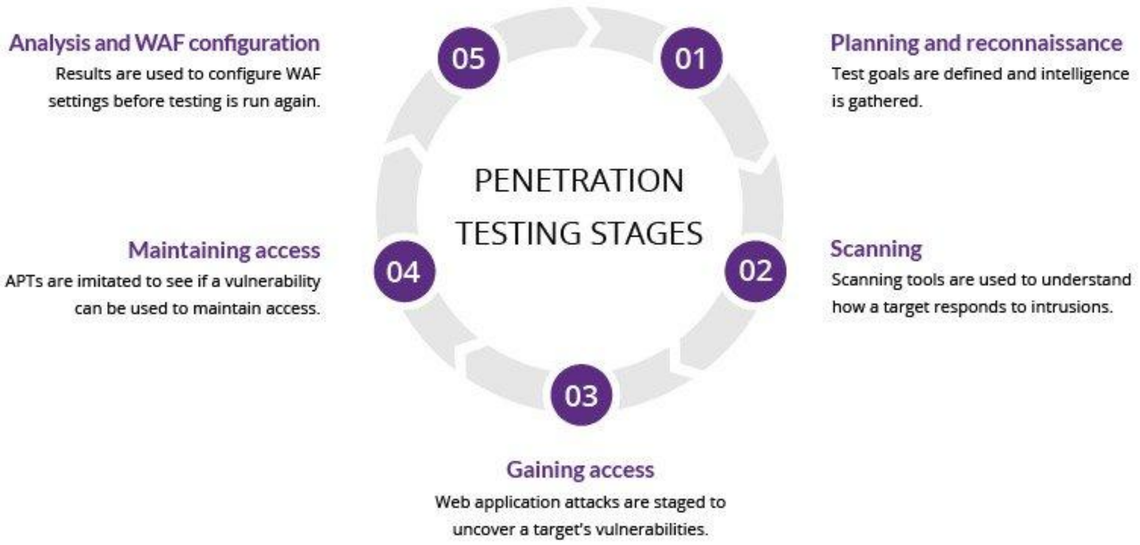
Linux is a community of open-source Unix like operating systems that are based on the Linux Kernel. It is a free and open-source operating system and the source code can be modified and distributed to anyone commercially or non commercially under the GNU General Public License. The main reason to learn Linux for an ethical hacker is, in terms of security, Linux is more secure than any other operating system. It does not mean that Linux is 100 percent secure it has some malware for it but is less vulnerable than any other operating system. So, it does not require any anti-virus software.

4. Programming Skills

Another most important skill to become an ethical hacker is Programming Skills. So what does the word programming in the computer world actually means? It means, **"The act of writing code understood by a computational device to perform various instructions."** So, to get better at programming, one will be writing a lot of code! Before one writes code he/she must choose the best programming language for his/her programming.

- **Penetration testing concepts**

The pen testing process can be broken down into five stages.


PENETRATION TESTING STAGES
01
Planning and reconnaissance
Test goals are defined and intelligence is gathered.
02
Scanning
Scanning tools are used to understand how a target responds to intrusions.
03
Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.
04
Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.
05
Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.

1. Planning and reconnaissance

The first stage involves:

- Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.

- Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

2. Scanning

The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:

- **Static analysis** – Inspecting an application's code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.
- **Dynamic analysis** – Inspecting an application's code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application's performance.

3. Gaining Access

This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target's vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

4. Maintaining access

The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization's most sensitive data.

5. Analysis

The results of the penetration test are then compiled into a report detailing:

- Specific vulnerabilities that were exploited
- Sensitive data that was accessed
- The amount of time the pen tester was able to remain in the system undetected

This information is analyzed by security personnel to help configure an enterprise's WAF settings and other application security solutions to patch vulnerabilities and protect against future attacks.

Penetration testing methods

External testing

External penetration tests target the assets of a company that are visible on the internet, e.g., the web application itself, the company website, and email and domain name servers (DNS). The goal is to gain access and extract valuable data.

Internal testing

In an internal test, a tester with access to an application behind its firewall simulates an attack by a malicious insider. This isn't necessarily simulating a rogue employee. A common starting scenario can be an employee whose credentials were stolen due to a phishing attack.

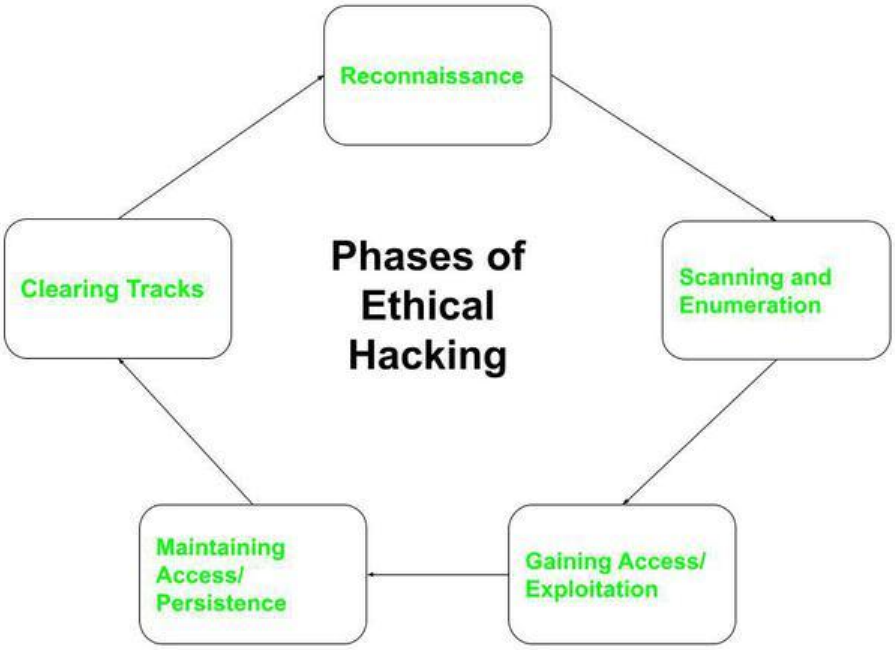
Blind testing

In a blind test, a tester is only given the name of the enterprise that's being targeted. This gives security personnel a real-time look into how an actual application assault would take place.

Double-blind testing
In a double blind test, security personnel have no prior knowledge of the simulated attack. As in the real world, they won't have any time to shore up their defenses before an attempted breach.

Targeted testing
In this scenario, both the tester and security personnel work together and keep each other appraised of their movements. This is a valuable training exercise that provides a security team with real-time feedback from a hacker's point of view.

- **Phase of Ethical Hacking**


Reconnaissance
Scanning and Enumeration
Gaining Access/ Exploitation
Maintaining Access/ Persistence
Clearing Tracks
Phases of Ethical Hacking

1. **Reconnaissance:** This is the first phase where the Hacker tries to collect information about the target. It may include Identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc. Let's assume that an attacker is about to hack a websites' contacts. He may do so by using a search engine like maltego, researching the target say a website (checking links, jobs, job titles, email, news, etc.), or a tool like HTTP Track to download the entire website for later enumeration, the hacker is able to determine the following: Staff names, positions, and email addresses.

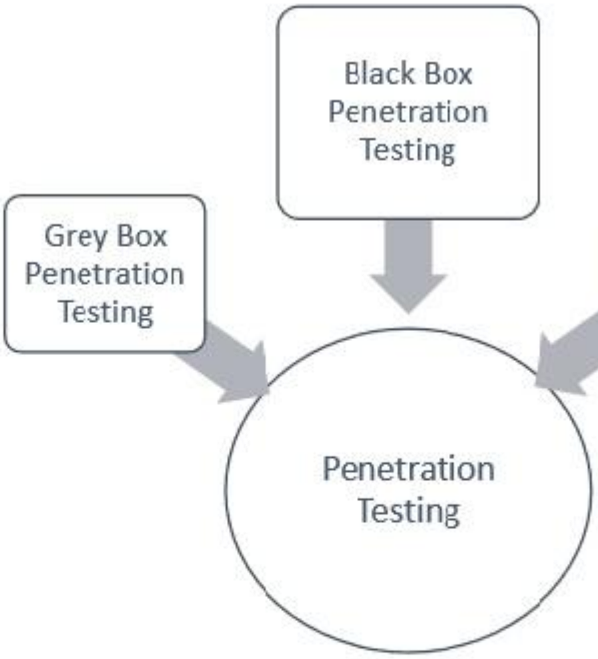
2. **Scanning:** This phase includes the usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data. Hackers are now probably seeking any information that can help them perpetrate attacks such as computer names, IP addresses, and user accounts. Now that the hacker has some basic information, the hacker now moves to the next phase and begins to test the network for other avenues of attacks. The hacker decides to use a couple of methods for this end to help map the network. The hacker looks for an automated email if possible or based on the information gathered he may decide to email HR with an inquiry about a job posting.

3. **Gaining Access:** In this phase, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. The hacker has finished enumerating and scanning the network and now decides that they have some options to gain access to the network. For example, say a hacker chooses a Phishing Attack. The hacker decides to play it safe and use a simple phishing attack to gain access. The hacker decides to infiltrate the IT department. They see that there have been some recent hires and they are likely not up to speed on the procedures yet. A phishing email will be sent using the CTO's actual email address using a program and sent out to the techs. The email contains a phishing website that will collect their login and passwords. Using any number of options (phone app, website email spoofing, Zmail, etc) the hacker sends an email asking the users to log in to a new Google portal with their credentials. They already have the Social Engineering Toolkit running and have sent an email with the server address to the users masking it with a bitly or tinyurl.

4. **Maintaining Access:** Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Once the hacker owns the system, they can use it as a base to launch additional attacks.
   In this case, the owned system is sometimes referred to as a zombie system**.** Now that the hacker has multiple e-mail accounts, the hacker begins to test the accounts on the domain. The hacker from this point creates a new administrator account for themselves based on the naming structure and tries and blends in. As a precaution, the hacker begins to look for and identify accounts that have not been used for a long time. The hacker assumes that these accounts are likely either forgotten or not used so they change the password and elevate privileges to an administrator as a secondary account in order to maintain access to the network. The hacker may also send out emails to other users with an exploited file such as a PDF with a reverse shell in order to extend their possible access. No overt exploitation or attacks will occur at this time. If there is no evidence of detection, a waiting game is played letting the victim think that nothing was disturbed. With access to an IT account, the hacker begins to make copies of all emails, appointments, contacts, instant messages and files to be sorted through and used later.

5. **Clearing Tracks (so no one can reach them):** Prior to the attack, the attacker would change their MAC address and run the attacking machine through at least one VPN to help cover their identity. They will not deliver a direct attack or any scanning technique that would be deemed "noisy".
   Once access is gained and privileges have been escalated, the hacker seeks to cover their tracks. This includes clearing out Sent emails, clearing server logs, temp files, etc. The hacker will also look for indications of the email provider alerting the user or possible unauthorized logins under their account.

- **Areas of penetration testing**


Black Box Penetration Testing
Grey Box Penetration Testing
White Box Penetration Testing
Penetration Testing

- **Black Box Penetration Testing**

In black box penetration testing, tester has no idea about the systems that he is going to test. He is interested to gather information about the target network or system. For example, in this testing, a tester only knows what should be the expected outcome and he does not know how the outcomes arrive. He does not examine any programming codes.

Advantages of Black Box Penetration Testing

- Tester need not necessarily be an expert, as it does not demand specific language knowledge
- Tester verifies contradictions in the actual system and the specifications
- Test is generally conducted with the perspective of a user, not the designer

Disadvantages of Black Box Penetration Testing

- Particularly, these kinds of test cases are difficult to design.
- Possibly, it is not worth, incase designer has already conducted a test case.
- It does not conduct everything.

- **White Box Penetration Testing**

This is a comprehensive testing, as tester has been provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc. It is normally considered as a simulation of an attack by an internal source. It is also known as structural, glass box, clear box, and open box testing.

White box penetration testing examines the code coverage and does data flow testing, path testing, loop testing, etc.

Advantages of White Box Penetration Testing

- It ensures that all independent paths of a module have been exercised.
- It ensures that all logical decisions have been verified along with their true and false value.
- It discovers the typographical errors and does syntax checking.

- It finds the design errors that may have occurred because of the difference between logical flow of the program and the actual execution.

- **Grey Box Penetration Testing**

In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system. It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents.

Advantages of Grey Box Penetration Testing

- As the tester does not require the access of source code, it is non-intrusive and unbiased
- As there is clear difference between a developer and a tester, so there is least risk of personal conflict
- You don't need to provide the internal information about the program functions and other operations

Areas of Penetration Testing

Penetration testing is normally done in the following three areas −

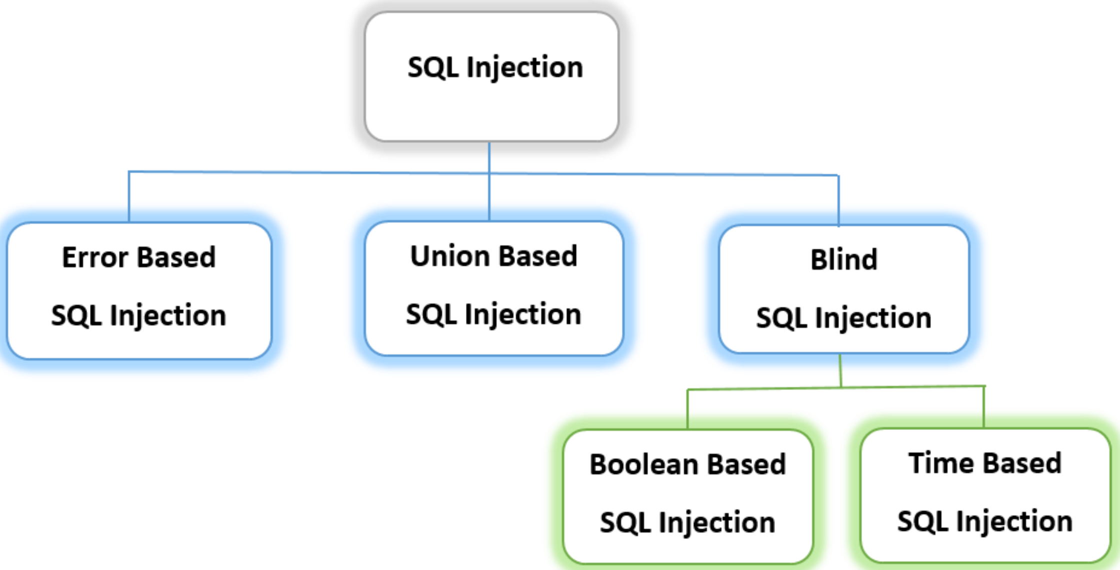
- **Network Penetration Testing** − In this testing, the physical structure of a system needs to be tested to identify the vulnerability and risk which ensures the security in a network. In the networking environment, a tester identities security flaws in design, implementation, or operation of the respective company/organization's network. The devices, which are tested by a tester can be computers, modems, or even remote access devices, etc
- **Application Penetration Testing** − In this testing, the logical structure of the system needs to be tested. It is an attack simulation designed to expose the efficiency of an application's security controls by identifying vulnerability and risk. The firewall and other monitoring systems are used to protect the security system, but sometime, it needs focused testing especially when traffic is allowed to pass through the firewall.
- **The response or workflow of the system** − This is the third area that needs to be tested. Social engineering gathers information on human interaction to obtain information about an organization and its computers. It is beneficial to test the ability of the respective organization to prevent unauthorized access to its information systems. Likewise, this test is exclusively designed for the workflow of the organization/company.

- **SQL Injection**

  - **Concepts of SQL Injection**

    SQL Injection is a code-based vulnerability that allows an attacker to read and access sensitive data from the database. Attackers can bypass security measures of applications and use SQL queries to modify, add, update, or delete records in a database.
    A SQL injection manipulates Structured Query Language code to provide access to protected resources, such as sensitive data, or execute malicious SQL statements. When executed correctly, a SQL injection can expose intellectual property, customer data or the administrative credentials of a private business.

  - **Types of SQL Injection**


SQL Injection
Error Based SQL Injection
Union Based SQL Injection
Blind SQL Injection
Boolean Based SQL Injection
Time Based SQL Injection

.

1. Error-Based SQL Injections:

Error-based SQL Injections obtain information about the database structure from error messages issued by the database server. In rare circumstances, an attacker may enumerate an entire database using only error-based SQL injection.

2. Union-Based SQL Injections:

Union-based SQL Injections use the UNION SQL operator to aggregate the results of two or more SELECT queries into a single result, which is subsequently returned as part of the HTTP response.

3. Blind Boolean-based SQL Injections:

Boolean-based SQL Injection works by submitting a SQL query to the database and forcing the application to produce a different response depending on whether the query returns TRUE or FALSE.

4. Blind Time-Based SQL Injections:

Time-based SQL Injection works by sending a SQL query to the database and forcing it to wait for a predetermined length of time (in seconds) before answering. The response time will tell the attacker if the query result is TRUE or FALSE.

Depending on the outcome, an HTTP response will either be delayed or returned immediately. Even though no data from the database is returned, an attacker can determine if the payload used returned true or false. Because an attacker must enumerate a database character by character, this attack is often slow (particularly on big databases).

- **Firewall**
  - **Concepts of Firewall**

Firewall is a network security device that observes and filters incoming and outgoing network traffic, adhering to the security policies defined by an organization. Essentially, it acts as a protective wall between a private internal network and the public Internet.

A firewall can either be software or hardware. Software firewalls are programs installed on each computer, and they regulate network traffic through applications and port numbers. Meanwhile, hardware firewalls are the equipment established between the gateway and your network. Additionally, you call a firewall delivered by a cloud solution as a cloud firewall.

There are multiple types of firewalls based on their traffic filtering methods, structure, and functionality. A few of the types of firewalls are:

- **Proxy Service Firewall**
  This type of firewall protects the network by filtering messages at the application layer. For a specific application, a proxy firewall serves as the gateway from one network to another.

- **Stateful Inspection**
  Such a firewall permits or blocks network traffic based on state, port, and protocol. Here, it decides filtering based on administrator-defined rules and context.

- **Next-Generation Firewall**
  According to Gartner, Inc.'s definition, the next-generation firewall is a deep-packet inspection firewall that adds application-level inspection, intrusion prevention, and information from outside the firewall to go beyond port/protocol inspection and blocking.

- **Unified Threat Management (UTM) Firewall**
  A UTM device generally integrates the capabilities of a stateful inspection firewall, intrusion prevention, and antivirus in a loosely linked manner. It may include additional services and, in many cases, cloud management. UTMs are designed to be simple and easy to use.

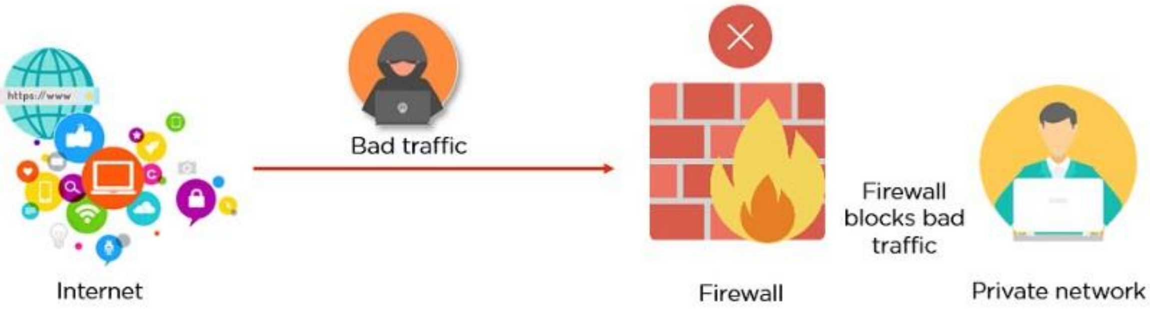
- **Threat-Focused NGFW**
  These firewalls provide advanced threat detection and mitigation. With network and endpoint event correlation, they may detect evasive or suspicious behavior.

○ **<u>Working, Advantages and Importance of firewall</u>**

- Firewalls filter the network traffic within a private network. It analyses which traffic should be allowed or restricted based on a set of rules. Think of the firewall like a gatekeeper at your computer's entry point which only allows trusted sources, or IP addresses, to enter your network.

- A firewall welcomes only those incoming traffic that has been configured to accept. It distinguishes between good and malicious traffic and either allows or blocks specific data packets on pre-established security rules.

- These rules are based on several aspects indicated by the packet data, like their source, destination, content, and so on. They block traffic coming from suspicious sources to prevent cyber attacks.
- For example, the image depicted below shows how a firewall allows good traffic to pass to the user's private network.



- This way, a firewall carries out quick assessments to detect malware and other suspicious activities.
- There are different types of firewalls to read data packets at different network levels. Now, you will move on to the next section of this tutorial and understand the different types of firewalls.

- **Advantages of Using Firewall**
    - Firewalls play an important role in the companies for security management. Below are some of the important advantages of using firewalls.
    - It provides enhanced security and privacy from vulnerable services. It prevents unauthorized users from accessing a private network that is connected to the internet.
    - Firewalls provide faster response time and can handle more traffic loads.
    - A firewall allows you to easily handle and update the security protocols from a single authorized device.
    - It safeguards your network from phishing attacks.

- **How to Use Firewall Protection?**
    - To keep your network and devices safe, make sure your firewall is set up and maintained correctly. Here are some tips to help you improve your firewall security:

- Constantly update your firewalls as soon as possible: Firmware patches keep your firewall updated against any newly discovered vulnerability.

- Use antivirus protection: In addition to firewalls, you need to use antivirus software to protect your system from viruses and other infections.

- Limit accessible ports and host: Limit inbound and outbound connections to a strict white list of trusted IP addresses.

- Have active network: To avoid downtime, have active network redundancies. Data backups for network hosts and other critical systems can help you avoid data loss and lost productivity in the case of a disaster.