Unit 1: Introduction to Electronic Commerce

1.1 Concepts of e-Commerce

E=Electronic (Electricity used in things) Commerce = Monitory exchange transaction (Give and Take) Business - Exchange of things or buying and or selling of goods in which goods are shifted from one hand to another or one place to another. So generally, the transactions for products and services with respect to money or in the context of money/ revenue are called Business

At least two parties are involved: (1) the Buyer (2) the Seller
Buyer - One who has money and who wants products and/or services.
Seller. One who gives/provides/fulfills products or goods and/or services/requirements of the buyer may be in exchange for money/revenue.

What is E-Commerce?

E-Commerce is a modern business methodology that addresses the needs of organizations, merchants, and consumers to cut costs while improving the quality of goods and services and increasing the speed of service delivery
.

E-Commerce helps to do business without any geographical limitation/ Space and it is also useful in expanding the business.

E-Commerce can be defined as business activities (buying and selling) conducted using electronic data transmission via the internet and WWW. Most people think only of B2C Business shopping on the web as E- Commerce

Following are some definitions of e-commerce

1. It is the ability to conduct business electronically over the internet.
2. means managing Transactions using networking and electronic means.
3. It is a platform for selling products & services via the internet.

Traditional Commerce v/s E-Commerce

Sr. No.	Traditional Commerce	E-Commerce
1	Heavy dependency on information exchange from person to person.	Information sharing is made easy via electronic communication channels making little dependency on person to person information exchange.
2	Communication/ transaction are done in synchronous way. Manual intervention is required for each communication or transaction.	Communication or transaction can be done in asynchronous way. Electronics system automatically handles when to pass communication to required person or do the transactions.

3	It is difficult to establish and maintain standard practices in traditional commerce.	A uniform strategy can be easily established and maintain in e-commerce.
4	Communications of business depends upon individual skills.	In e-Commerce or Electronic Market, there is no human intervention.
5	Unavailability of a uniform platform as traditional commerce depends heavily on personal communication.	E-Commerce website provides user a platform where al l information is available at one place.
6	No uniform platform for information sharing as it depends heavily on personal communication.	E-Commerce provides a universal platform to support commercial / business activities across the globe.

1.2 Aims of e-Commerce

1. **Reduced coasts**

Reduced costs (Reduce management costs) Businesses aim at reducing the costs incurred for the betterment of their revenue. Automating the e-commerce business can help in reducing management costs significantly. Moreover, the right use of digital marketing can help in reducing the cost spent on driving customers to such an extent that businesses can bring customers free of cost.

2. **Lower product cycle times**

Cycle time is the amount of time it takes to complete a process, which is any process, for example are purchase order process and transferring of purchase order to invoice. E-commerce can reduce this cycle time by eliminating the time taken to process between supplier, intermediaries and customers, which means when a customer placing an order, he or she is directly deal with the supplier website, hence it eliminate the processing time between the intermediaries and supplier.

3. **Faster customer response (Providing a unique customer experience)**

Uncountable ecommerce businesses are functioning out there in the market. When a customer searches for a certain product (for instance, shampoo), they will probably click on the first three links that are shown on the Google Search Engine Results Page. All the rest links are either avoided, never seen, or are visited by a few. his itself shows the competition in the ecommerce market. One of the best ways to stand out from the crowd is by providing a unique customer experience. This includes giving a personalized experience to each customer or visitor of your online store, website, or mobile app. Some other pointers to consider are round the clock customer service, immediate responses to the queries rose, engaging with the customers, and so on.

4. **Improved service quality (Boosting the efficiency of services**

With the continually evolving technology, you need to enhance the efficiency of your services.
By choosing an online ecommerce platform to create an online store, you can efficiently reduce the cost of managing and selling online. Efficiency of your service that eventually enhances the revenue earned.
You have various opportunities to boost the By reducing the delivery time, you can witness happy customers getting back to your business two times faster. Another way is to provide your customers with automated services such as status update, invoice creating, chat support, etc. When you update your

efficiency of delivering products or services to your customers, you are creating a strong online presence that helps you sell more.

5. **Developing relevant target**

Developing relevant traffic for an ecommerce business is a common objective. Whether an ecommerce website or an online store, building traffic is one of the most important objectives. However, you should know that not all traffic is useful for your business. If you are successfully creating traffic for your ecommerce site or store, but most of the people in the traffic do not require the products or services you provide, the traffic is not causing any good to your business. For instance, your marketing strategies were attractive enough for teenagers; your business would not be receiving any boost in sales. herefore, along with boosting your traffic, you need to analyze your traffic. Here comes the need for collecting customer data. Collecting customer data include demographics such as age, location, and gender, customer interests, browsing history, browser history, and so on. By saving these data, you can aim in targeting the relevant market.

6. **Making responsive ecommerce website**

With the increasing use of smart phones for shopping online, it has become more than mandatory for ecommerce businesses to go mobile. Apart from creating a native mobile app, like the one offered from Builder fly, you need to create a responsive e-commerce website. It is one of the major objectives of all leading ecommerce businesses. By responsive, it means to create a website that can be viewed from any devices of varying screen size, equally. Studies say that Google may next rank a website based on its mobile website. It means that any website that has a responsive design would be ranked on top of the website that does not have one. Making your ecommerce website responsive can help you optimize it. A mobile-friendly website earns more traffic than the rest.

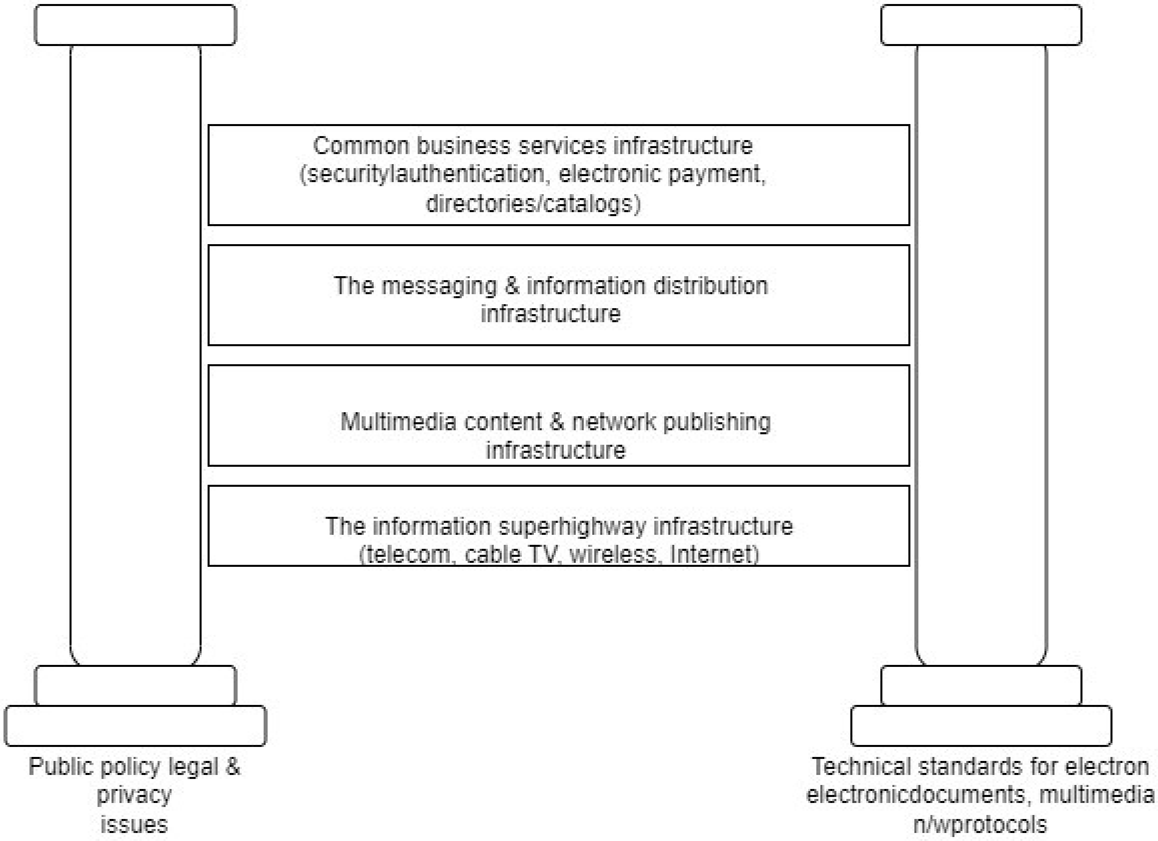
7. **Increasing sales**

The objective of increasing sales will always remain continuous and constant for an ecommerce business. In order to thrive in the ecommerce industry, you need to boost your sales, constantly. All other objectives are zeroed down to make this objective happen. However, you also need to look into your past store analytics and figure out the marketing tactics that have worked well for you to increase sales. Only you can decide what is perfect for your business and what is not. Every business is unique, and so is yours!

8. **Increasing the number of loyal customers**

Customers are the core of all business strategies. Therefore, ensuring the great customer experience is of prime importance for the growth of the business. You need to meet your customers where they spend their time. More than 60% of consumers look for purchasing goods and services online. If you meet your customers where they are already active, the chances of them, interacting with your business increases two folds. You can increase the number of loyal customers by giving the best experience to your already existing customers as well as bring in newer customers.

1.3 e-Commerce Framework


Common business services infrastructure (securitylauthentication, electronic payment, directories/catalogs)
The messaging & information distribution infrastructure
Multimedia content & network publishing infrastructure
The information superhighway infrastructure (telecom, cable TV, wireless, Internet)
Public policy legal & privacy issues
Technical standards for electron electronicdocuments, multimedia n/wprotocols

Architectural framework of e-commerce means the synthesizing of various existing resources like DEMS, data repository, computer languages, software agent-based transactions, monitors or communication protocols to facilitate the integration of data and software for better applications.

The architectural framework for e-commerce consists of six layers of functionality or services follows:

1. Application services.
2. Brokerage services, data or transaction management.
3. Interface and support layers.
4. Secure messaging, security and electronic document interchange.
5. Middleware and structured document interchange, and
6. Network infrastructure and the basic communication services

1. Application services

In the application layer services of e-commerce, it is decided what type of e-commerce application is going to be implemented. There are three types of distinguished e-commerce applications i.e., consumer-to-business applications, business-to-business applications, and intra-organizational applications.

2. Information Brokerage and Management Layer

This layer is rapidly becoming necessary in dealing with the voluminous amounts of information on the networks. This layer works as an intermediary who provides service integration between customers and information providers. For example, a person wants to go ta USA from Bangladesh. the person checks the sites or various airlines tar the low-price ticket with the best available service. For this he must know the URLS of all sites. Secondly, to search the services and tne best prices, he also feed the details of the journey again and again on different sites. There is a site that can work as information broker and can arrange the ticket as per the need of the person, it will save the lot of time and efforts of the person. This is just one example of how information brokerages can add value. Another aspect of the brokerage function is the support for data management and traditional transaction services. Brokerages may provide tools to accomplish more sophisticated, time-delayed updates or future compensating transactions.

3. Interface and support services

The third layer of the architectural framework is Interface layer. This Provides interface for e-commerce applications. Interactive catalogs and directory Support services are the examples or this layer interactive catalogs are tne customized interface to customer applications such as home shopping. Interactive catalogs are very similar to the paper-based catalog. The only difference between the interactive catalog and paper-based catalog is that the first one has the additional features such as use of graphics and video to make the advertising more attractive. Directory services have the functions necessary for information search and access. The directories attempt to organize the enormous amount of information and transactions Generated to facilitate e-commerce. The main difference between the interactive catalogs and directory services is that the interactive catalogs deal with people while directory support services interact directly with software applications.

4. Secure Messaging Layer

In any business, electronic messaging is an important issue. The commonly used messaging systems like phone, fax and courier services have certain problems like in the case of phone it the phone line is dead or somehow the number Is wrong. You are not able to deliver the urgent messages. In the case or courier service, T you want to deliver the messages instantly, it is not possible as it will take some time depending on the distance between the source and destination places. The solution for such type of problems s electronic messaging services like E-mail, enhanced fax and EDI. The electronic messaging has changed the way the business operates. The major advantage of the electronic messaging is the ability to access the right information at the right time across diverse work groups. The main constraints of the electronic messaging are security, privacy, and confidentiality through data encryption and authentication techniques.

5. Middleware services

The enormous growth of networks, client server technology and all other forms of Communicating between/among unlike platforms is the reason for the invention of middleware services. The middleware services are used to integrate the diversified software programs and make them talk to one another.

6. Network Infrastructure

We know that the effective and efficient linkage between the customer and the Supplier is a precondition Tor e-commerce, for this a network Infrastructure is required. The early models tor networked computers were the local and long distance telephone companies. The telephone company lines were used for the connection among the computers. As soon as the computer connection was established, the data traveled along that single path. Telephone company switching equipment (both mechanical and computerized) selected specific telephone lines, or circuits, that were connected to create the single path between the caller and the receiver. This centrally-controlled, single-connection model is known as circuit switching

1.4 e-Commerce Consumer Applications

By virtue of its similarities, the scope of operations for E-Commerce is nearly as broad as traditional commerce. E-commerce includes both traditional activities (e.g. providing product information) and new activities (e-g. Conducting online retail in virtual malls, publishing digital information). Some at the common operations that define t-Commerce are specific business-to-business and business-to-customer interactions, such as:

Information exchange
Goods or services trading
Sales promotion and advertising
Online digital content delivery
Electronic funds transfers and transaction processing
Electronic share trading
Electronic bills of landing processing
Collaborative work interaction
Manufacturing management E-Commerce
Accounts settlement
Online sourcing
Public procurement
Direct consumer marketing
Inventory management
Post-sales service
Commercial auction

There are a variety of e-commerce applications that are constantly affecting the trends and prospects of a business. The primary applications of e-commerce are

Business-to-consumer (B2C)
Business-to Business (B2B)
Consumer-to-consumer (C2C)
Consumer-to-Business (C2B)

Other Applications of E-Commerce

1. Business-to-Employee (B2E)
2. Government-to-Government (G2G)
3. Government-to-Employee (G2E)
4. Government-to-Business (G2B)
5. Business-to- Government (B2G)
6. Government-to-Citizen (G2C)
7. Citizen-to-Government (C2G)

1.5 e-Commerce Organizational Applications

The wide range of applications for the consumer marketplace can be broadly classified into:

Entertainment: Movies on demand, video cataloging, interactive ads, multiuser games, online discussion

Financial services and information: Home baking, financial services, and financial news.
Essential services: Home shopping, electronic catalogs, tele-medicine, remote diagnostics.
Educational and training: Interactive education, video conferencing, online databases.

1.6 Introduction to m-Commerce

Short for mobile commerce, m-commerce refers to any commercial transactions that take place via apps or mobile sites. Mobile commerce can be understood broadly as a subcategory of e-commerce, or as the mobile version of e-commerce. The mobile commerce vertical is growing rapidly, with the percentage and share of digital purchases that are taking place on mobile increasing each year. As making purchases on mobile gets more convenient and as more people globally gain access to smartphones and tablets, the capacity for mobile purchases to be made continues to soar.

In short, the definition of m-commerce is: the buying and selling of items via mobile devices.

M-commerce examples and types

Broken into three main categories (mobile shopping, mobile payments, and mobile banking), the highest growth areas for m-commerce are:

- In-app purchasing (such as buying clothing items via a retail app)
- Mobile banking
- Virtual marketplace apps like Amazon
- Digital wallets like Apple Pay, Android Pay, and Samsung Pay
- Mobile ticketing

There is significant crossover with fintech, but that’s only because mobile commerce doesn’t strictly refer to the buying of products, it also encapsulates the smartphone behaviors that lead to making a mobile purchase and the technology that enables it.

Key m-commerce areas include:

Browsing and buying: Similar to an e-commerce flow on a desktop, this form of m-commerce involves the user browsing apps, clicking around mobile websites, and making purchases. This typically occurs via dedicated apps, but can also take place as a ‘social commerce’ purchase, with social media platforms including Instagram and Snapchat offering purchasing options in-app.

Convenience purchases: Many of the purchases that take place on mobile aren’t retail-related, and m-commerce is not restricted to ‘shopping’ per se. These purchases include ordering food or grocery deliveries, and booking taxis or ride-sharing.

Mobile app payments and wallet payments: There are various ways to actually make an m-commerce purchase, and digital wallets are growing in use. Instead of inputting credit card details to each individual app, a user’s digital wallet can be loaded (as a popup/overlay) and the purchase can be made with a single click or by simply using a thumbprint.

Digital content (purchasing and renting): Subscriptions apps are extremely popular on mobile, most commonly with music and video (think Netflix and Spotify). Users pay a subscription fee and can then access an entire library of content from their mobile app.

Unit 2: Network Infrastructure of e-Com, Payment and Security

2.1. Concepts of Information Way

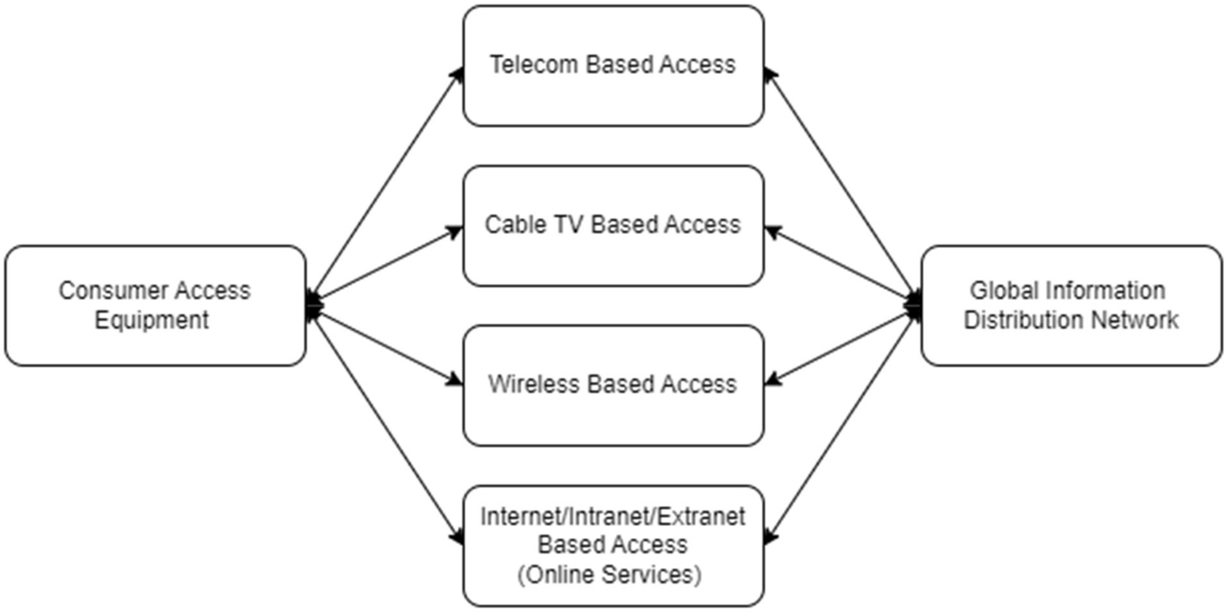
- E-commerce needs a standard network infrastructure to transport the content.
- Internet and intranet are the basic tools to implement e-commerce. The network infrastructure is provided by I-way or business super highway.
- The information super highway may be defined as a high-capacity electronic pipeline that is capable of simultaneously supporting a large number of e-commerce applications and provide interactive phone like connectivity between users and services and among users.
- The ability to translate the content (media) into digital form is fundamental to all the changes associated with the I-way.
- Digitization refers to the process by which all media video, audio, text, graphics are processed by computers: manipulated, mixed, transform and delivered in new way.

Information Super Highway (I-Way):

- Electronic commerce needs a network infrastructure to transport the content-text, audio, video, graphics etc.
- The network infrastructure that provides such a data transmission facility is called I-Way or information super highway.
- Thus, information super highways can be defined as the high capacity, electronic and interactive pipeline to the consumer or business premise that is capable of supporting large number of ecommerce applications simultaneously.
- It is called interactive because it provides two-way communication between users and service providers or between one user and another user.
- It is called high-capacity electronic pipeline because it must provide broadband link.
- Historically, the voice and data networks have evolved separately, with voice networks relying on circuit switching and data networks using packet switching techniques.
- Thus, a business user requiring voice, data, and video conferencing services often had to use three separate networks- a voice network, a data network, and a videoconferencing network.
- I-way provides integration solution to the shortcoming of the need to have separate network for voice, data and video services respectively.
- Nowadays information super high way is emerged as basic network infrastructure for all ecommerce activities due to its capability of providing integrated text, graphics, audio, and video services.

2.2. Components of I-Way

Various components contained in I-way can be broadly divided into three categories: Consumer access equipment, Access Roads or Media, and Global Information distribution network**.**


Telecom Based Access
Cable TV Based Access
Consumer Access Equipment
Global Information Distribution Network
Wireless Based Access
Internet/Intranet/Extranet Based Access (Online Services)

Consumer Access Equipment's:

These are the devices at consumer end and enables consumers to access the network. It consists of hardware and software. Hardware component includes devices such as computers, modems, routers, switches etc. for computer networks, set-top boxes, TV signal descramblers etc. for television networks, Cell phones etc. for cellular networks and so on. And software systems installed in those hardware devices includes browsers, operating systems etc. The type of consumer access equipment used depends upon the communication mode used. These equipment's are also called customer premise equipment's or terminal equipment's

Access Roads/Media (Local on Ramps)

These are the network infrastructure that provides linkage between businesses, homes, and schools to global information distribution network. This component is often called the last mile in telecommunication industry. Access road providers can be divided into four categories: Telecom based, Cable TV based, Wireless based, and Computer based online systems. Main function of access roads is to connect consumers with e-commerce applications.

Telecom Based Access Roads

- Telecom industries provides high speed electronic pipeline which is capable for carrying large volume of audio, video, and text data.
- These industries provide network infrastructure for long distance and local telephone Communication.
- This network infrastructure is useful for ecommerce application to be connected with Global Information Distribution Network.
  Main limitation of telecom-based access roads is that it continues to depend on analog Transmission of data although the industry is rapidly introducing advanced digital transmission technologies.
- However, most of the trunk lines are replaced with high-capacity optical fiber in recent days, local loops are still connected by using copper wire. The customers are constrained with limited capacity of these wires.

- Thus, the telecom industries need to replace these copper wires with high-capacity optical fiber to handle expected flood of information from ecommerce applications.

Cable TV Based Access Roads

- Cable television systems also provides high-capacity broadband network infrastructure to connect large number of customers with their system.
- These systems adopt digital transmission of data and have a lot of unutilized capacity which can be useful for transmitting information from ecommerce applications to customers.
- Cable TV based systems can be of two types: wired cable TV, wireless cable TV.
- In wired cable TV based systems connects customers mainly by using coaxial-cables. But in recent days they are replacing trunk lines from optical fibers whereas local loops are based on coaxial cable links.
- This further strengthened the capacity of cable TV based network infrastructure and provides ecommerce applications with more capacity links.
- Now, cable TV companies have started to use wireless communication to connect customer homes in cost effective way rather than using optical fiber or coaxial cable-based interconnection.
- Direct Broadcast Satellite (DBS) is used for wireless cable TV transmission. It uses Super high frequency (SHF) channels to transmit data over the air.
- These signals are received by special antennas mounted in roofs of subscribers and then it is distributed within the building with help of coaxial cable.
- With help of DBS, it is easy to make cable TV in rural areas at affordable cost.
- Thus, emergence of wireless cable TV infrastructure makes it easy to provide ecommerce services in rural areas also.
- Although there are lots of benefits of wireless cable TV network infrastructure, it also suffers from limitations. For example, heavy rainfall may cause picture quality degradation or interruption.

Wireless Based Access Roads

- Wireless operators provide network infrastructure by using radio frequencies which are Omni directional waves and have high penetration power.
- The wireless-based systems have revolutionized the ways of thinking about information delivery. Technology is the most important factor.
- Thus, wireless based access enables customers to access ecommerce application from anywhere at any time and ecommerce service providers can provide content and services to customers on the basis of location.

Computer Based Online Systems

- The Internet is the global system of interconnected mainframe, personal and wireless computer networks that use the protocol suite TCP/IP to link billions of devices worldwide.
- It is a network of networks that consists of millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.
- Internet, intranets and extranets are providing online services which provides 24-hour computer based supermarkets to customers.

- It targets a wide range of ecommerce applications such as video on demand, home shopping, email, information publishing, information retrieval, video conferencing and many more.
- The demand of these online services is increased dramatically due to widespread use of PCs in homes and businesses.
- Due to low hardware costs and enhanced graphics and multimedia support, customers are fast attracted towards online services entertainment, education, shopping, and information services.
- ISP provides Internet access, employing a range of technologies to connect users to their network and thus provides access roads for ecommerce applications,

GIDN (Global Information Distribution Network)

The global information distribution networks consist of the infrastructure crossing the countries and continents. They include the long-distance telephone lines, satellite networks, and the internet. Long distance telephone connectivity is provided through cable by the inter-exchange carriers. Long distance cellular networks are using the wireless technologies to connect the consumers worldwide. Satellite networks play a vital role in the communication industry. They have advantages over the terrestrial networks in that

1. They are accessible from any point of the globe.
2. They can provide broad band digital services to many points without the cost of acquiring wire/cable installation.
3. They can add receiving and sending sites without significant additional costs.

Requirement of I-Way

The success of e-commerce-based business depends on the information flow and to make Information flow smooth and capable I-way is required. The success or failure of any creativity, product or services is a key driver of market forces. The underlying of market drives of I-way is important because e-commerce applications are Dependent on the underlying I-way.

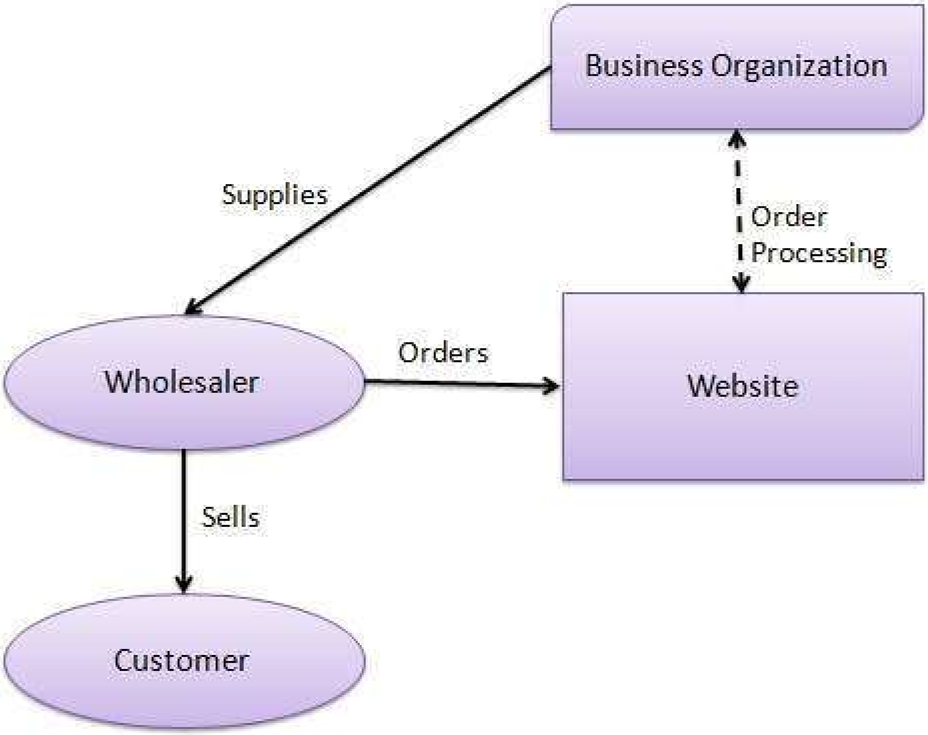
Functions of I-Way

It develops business relationship among all sorts of business and with people all around the world by the help of global information distribution network. It is used for communicate between the business partners at any locations through the network Communications. It acts as an information system for any organizations. I-Way controls unwanted information distributed over the complex network. It allows multiple forms of messages, sent and received over the same network.

2.3. Transaction Models

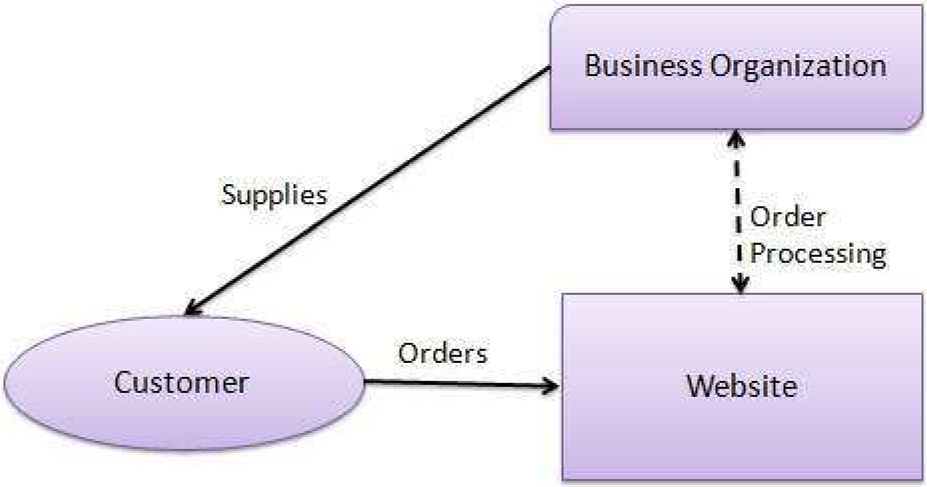
Business - to - Business

A website following the B2B business model sells its products to an intermediate buyer who then sells the product to the final customer. As an example, a wholesaler places an order from a company's website and after receiving the consignment, sells the endproduct to the final customer who comes to buy the product at one of its retail outlets.



Business - to – Consumer

A website following the B2C business model sells its products directly to a customer. A customer can view the products shown on the website. The customer can choose a product and order the same. The website will then send a notification to the business organization via email and the organization will dispatch the product/goods to the customer.



Intra-organizational e-commerce

Intra-organizational e-commerce is the purchase of goods, services, or resources by an organization from within the same organization. This can include everything from purchasing office supplies from coworkers to hiring a consultant from within the company. Some common intra-organizational e-commerce examples include:

1. Purchasing office supplies from coworkers - This is a common intra-organizational e-commerce scenario, as it can be cost effective and faster than ordering supplies online.
2. Hiring a consultant from within the company - Consultants can be a valuable resource, and it can be faster and easier to hire one within your organization than to find one outside of it.
3. Purchasing intellectual property from within the company - Intra-organizational e-commerce can also involve purchasing intellectual property, such as patents or trademarks. This can be useful in protecting your intellectual property, and it can be quicker and easier to do than seeking out external sources.

2.4.1 E-Commerce Payment Systems

E-commerce sites use electronic payment, where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing the paperwork, transaction costs, and labor cost. Being user friendly and less time-consuming than manual processing, it helps business organization to expand its market reach/expansion. Listed below are some of the modes of electronic payments −

Credit Card
Debit Card
Smart Card
E-Money
Electronic Fund Transfer (EFT)

Credit Card

Payment using credit card is one of most common mode of electronic payment. Credit card is small plastic card with a unique number attached with an account. It has also a magnetic strip embedded in it which is used to read credit card via card readers. When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle. Following are the actors in the credit card system.

The card holder − Customer
The merchant − seller of product who can accept credit card payments.
The card issuer bank − card holder's bank
The acquirer bank − the merchant's bank
The card brand − for example, visa or MasterCard.

Credit Card Payment Process

Step 1:- Bank issues and activates a credit card to the customer on his/her request.
Step 2:- he customer presents the credit card information to the merchant site or to the merchant from whom he/she wants to purchase a product/service.
Step 3:- Merchant validates the customer's identity by asking for approval from the card brand company.

Step 4:- Card Brand Company authenticates the credit card and pays the transaction by credit. Merchant keeps the sales slip.
Step 5:-Merchant submits the sales slip to acquirer banks and gets the service charges paid to him/her.
Step 6:-Acquirer bank requests the card brand company to clear the credit amount and gets the payment.
Step 7:-Now the card brand company asks to clear the amount from the issuer bank and the amount gets transferred to the card brand company.

Debit Card

Debit card, like credit card, is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank. The major difference between a debit card and a credit card is that in case of payment through debit card, the amount gets deducted from the card's bank account immediately and there should be sufficient balance in the bank account for the transaction to get completed; whereas in case of a credit card transaction, there is no such compulsion.

Debit cards free the customer to carry cash and cheques. Even merchants accept a debit card readily. Having a restriction on the amount that can be withdrawn in a day using a debit card helps the customer to keep a check on his/her spending.

Smart Card

Smart card is again similar to a credit card or a debit card in appearance, but it has a small microprocessor chip embedded in it. It has the capacity to store a customer’s work-related and/or personal information. Smart cards are also used to store money and the amount gets deducted after every transaction.

Smart cards can only be accessed using a PIN that every customer is assigned with. Smart cards are secure, as they store information in encrypted format and are less expensive/provides faster processing. Mondex and Visa Cash cards are examples of smart cards.

E-Money

E-Money transactions refer to situation where payment is done over the network and the amount gets transferred from one financial body to another financial body without any involvement of a middleman. E-money transactions are faster, convenient, and saves a lot of time.

Online payments done via credit cards, debit cards, or smart cards are examples of e-money transactions. Another popular example is e-cash. In case of e-cash, both customer and merchant have to sign up with the bank or company issuing e-cash.

Electronic Fund Transfer

It is a very popular electronic payment method to transfer money from one bank account to another bank account. Accounts can be in the same bank or different banks. Fund transfer can be done using ATM (Automated Teller Machine) or using a computer.

Nowadays, internet-based EFT is getting popular. In this case, a customer uses the website provided by the bank, logs in to the bank's website and registers another bank account. He/she then places a request to transfer certain amount to that account. Customer's bank transfers the amount to other account if it is in the same bank, otherwise the transfer request is forwarded to an ACH (Automated Clearing House) to transfer the amount to other account and the amount is deducted from the customer's account. Once the amount is transferred to other account, the customer is notified of the fund transfer by the bank.

Credit/Debit card fraud

A credit card allows us to borrow money from a recipient bank to make purchases. The issuer of the credit card has the condition that the cardholder will pay back the borrowed money with an additional agreed-upon charge.

A debit card is of a plastic card which issued by the financial organization to account holder who has a savings deposit account that can be used instead of cash to make purchases. The debit card can be used only when the fund is available in the account

E-cash

E-cash is a paperless cash system which facilitates the transfer of funds anonymously. E-cash is free to the user while the sellers have paid a fee for this. The e-cash fund can be either stored on a card itself or in an account which is associated with the card. The most common examples of e-cash system are transit card, PayPal, Google Pay, Paytm, etc.

E-cash has four major components-

Issuers - They can be banks or a non-bank institution.
Customers - They are the users who spend the e-cash.
Merchants or Traders - They are the vendors who receive e-cash.
Regulators - They are related to authorities or state tax agencies.

E-cheque

E-cheques are cheques that are written and processed electronically. This means that the funds are transferred from the payer’s account to the payee’s account through an electronic network instead of a physical cheque. These cheques are also known as “digital cheques” or “electronic cheques”. The process of writing and processing an e-cheque is similar to that of a traditional cheque. The payer fills out a form with the necessary information, including the amount to be transferred, and submits it to the bank. The bank then verifies the funds and processes the transaction.

This work makes it a safe, fast, and easy way to transfer money electronically. If you are looking for a more efficient and secure way to process cheques, then e-cheques may be the solution for you.

Features of E-cheques

Nowadays many people are using these cheques because they provide a number of benefits over traditional paper cheques. For example, e-cheques are faster and more secure than paper cheques. Let’s take a closer look at some of the features of e-cheques:

Faster: E-cheques are processed faster than traditional paper cheques. This is because there is no need to wait for the cheque to be physically delivered to the payee.

More Secure: E-cheques are more secure than traditional paper cheques because they are processed through an electronic network. This means that there is less chance for them to be lost or stolen.

Easier to Track: E-cheques can be easily tracked through online banking systems. This makes it easy to see where the funds are going and who they are being transferred to.

Reduces Paper Waste: E-cheques reduce paper waste because they do not require the use of physical cheque stock. This means that fewer trees need to be chopped down in order to produce paper cheques.

Saves Time and Money: E-cheques save time and money because they eliminate the need for manual processing. This means that there is less chance for human error and that the funds will be transferred more quickly.

Overall, e-cheques offer a number of benefits over traditional paper cheques. They are faster, more secure, and easier to track and reduce paper waste. They also save time and money. If you are looking for a more efficient and secure way to process cheques, then e-cheques may be the solution for you.

E-wallets

E-wallet is a type of electronic card which is used for transactions made online through a computer or a smartphone. Its utility is same as a credit or debit card. An E-wallet needs to be linked with the individual's bank account to make payments.

E-wallet is a type of pre-paid account in which a user can store his/her money for any future online transaction. An E-wallet is protected with a password. With the help of an E-wallet, one can make payments for groceries, online purchases, and flight tickets, among others.

E-wallet has mainly two components, software and information. The software component stores personal information and provides security and encryption of the data. The information component is a database of details provided by the user which includes their name, shipping address, payment method, amount to be paid, credit or debit card details, etc.

For setting up an E-wallet account, the user needs to install the software on his/her device, and enter the relevant information required. After shopping online, the E-wallet automatically fills in the user's information on the payment form. To activate the E-wallet, the user needs to enter his password. Once the online payment is made, the consumer is not required to fill the order form on any other website as the information gets stored in the database and is updated automatically.

2.5 Security on Web, SSL

What is SSL?

Secure sockets layer is a computer networking protocol that supervises server identification and authentication. It also manages client authentication and encrypted communication between servers and clients.

How does it work?

SSL utilizes a combination of protective measures to securely encrypt transferred information. It uses public-key and symmetric-key encryption to secure a connection between the two machines that are interacting over the Internet. These devices typically include a server and a user's computer. These two types of encryption take normal information and place it into unique codes that are unknown to an outside user.

How does SSL impact ecommerce businesses?

SSL is a standard security technology for protecting encrypted communications between a server and the recipient of its stored information. SSL security typically establishes a secure link between a Web server, or an ecommerce website in this case, and the browser.

The same type of technology exists for email between mail servers and a mail client. Most Internet browsers support SSL. Ecommerce business owners must comply with SSL security standards because it

is the protocol that protects the transfer of important customer information, such as credit card numbers, social security numbers and login credentials. A website domain that begins with "https:" is compliant, whereas "http:" is not.

Why is it important?

Without this layer of protection, ecommerce store owners don't have extra security when it comes to accessing and storing sensitive information. With SSL security protocol, hackers have difficulty obtaining and reusing information illegally. Information transferred between a server and a browser without SSL protection is not encrypted, meaning it is visible in plain sight or not coded. Data that isn't coded is much more vulnerable to theft than encrypted information.

Unit-3: Introduction to Cyber Crimes

What is Cyber Crime?

Cybercrime is any criminal activity that involves a computer, networked device or a network Cybercrime refers to criminal conduct committed with the aid of a computer or other electronic equipment connected to the internet. Individuals or small groups of people with little technical knowledge and highly organized worldwide criminal groups with relatively talented developers and specialists can engage in cybercrime.

Cybercriminals or hackers who want to generate money, commit a majority of cybercrimes. Individuals and organizations are both involved in cybercrime. Aside from that, cybercriminals might utilize computers or networks to send viruses, malware, pornographic material, and other unlawful data. To make money, cybercriminals engage in a range of profit-driven criminal acts, including stealing and reselling identities, gaining access to financial accounts, and fraudulently utilizing credit cards to obtain funds.

A primary effect of cybercrime is financial. Cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial account, credit card or other payment card information

Examples of Basic Cybercrimes

Stolen credit card information:

The most common cybercrime is when a person's credit card information is stolen and used unlawfully to acquire or purchase goods or services over the internet.

Hacking into a government website:

Another type of cybercrime is tampering with sensitive government data.

Theft of user accounts:

Yahoo experienced a serious data breach from 2013 to 2016 that resulted in the theft of three billion user accounts. The attackers gained access to private information and passwords that were used to access user accounts in other online services. Most of this data is available even today on the dark web.

Compromised IoT devices:

In 2016, over one million connected devices in the IoT were compromised by attackers who took advantage of existing software vulnerabilities. It is the largest DDoS attack to date and one that caused outages in the global DNS affecting popular services including Netflix, PayPal, Twitter, and many more.

Loss of control and access to content:

The WannaCry attack, which was allegedly launched by North Korea, in 2017, unleashed ransomware that locked down content on user devices. This ransomware rapidly spread itself and infected 300,000 computers worldwide. The victims had to pay hundreds of dollars to restore their data.

Phishing campaigns:

The phishing campaigns infiltrate corporate networks by sending authentic-looking fraudulent emails to users in an organization and tricking them into performing actions such as downloading attachments or clicking on links. The viruses or malware then spreads to the systems, and, eventually, ends up in the organizations' networks.

3.1 Category of Cyber Crimes

Cybercrimes are broadly categorized into three fields:

Individual: It is a cybercrime that entails a single individual disseminating malicious or unlawful material via the internet. For example, distributing pornography, human trafficking, and online stalking.

Property: This cybercrime involves obtaining access to individuals' bank or credit card information, accessing their funds, making online transactions, or executing phishing schemes to persuade individuals to give away personal information.

Government: While these cybercrimes are uncommon, they are nevertheless considered significant offenses. It entails breaking into government databases and hacking official websites.

What are the Different Types of Cyber Crime?

There are several types of cybercrimes; the most common ones are email frauds, social media frauds, banking frauds, ransomware attacks, cyber espionage, identity theft, clickjacking, spyware, etc. Let us now see how these crimes are executed.

Malware

Malware is a broad phrase that encompasses a wide range of cyberattacks such as Trojans, viruses, and worms. Malware can simply be described as code written to steal data or destroy things on a computer.

How malware causes harm can assist us to classify the type of virus that we are dealing with. So, let us talk about it!

Viruses: Viruses, like their biological namesakes, attach themselves to clean files and infect other clean files. Viruses can spread uncontrollably, causing damage to the core functionality as well as deleting and corrupting files. Viruses usually appear as executable files downloaded from the internet.

Trojan: This type of malware masquerades as legitimate software that can be hacked. It prefers to function invisibly and creates security backdoors that allow other viruses to enter the system.

Worms: Worms use the network's interface to infect a whole network of devices, either locally or via the internet. Worms infect more machines with each successive infected machine.

Phishing

Phishing frequently poses as a request for information from a reputable third party. Phishing emails invite users to click on a link and enter their personal information.

In recent years, phishing emails have become much more complex, making it impossible for some users to distinguish between a real request for information and a fraudulent one. Phishing emails are sometimes lumped in with spam, but they are far more dangerous than a simple advertisement.

Man-in-the-middle Attack

A man-in-the-middle attack can obtain information from the end-user and the entity with which they are communicating by impersonating the endpoints in the online information exchange.

Drive-by Download Attack

To become infected, we no longer need to click to accept a download or install a software update. Simply opening a compromised webpage may now allow dangerous code to be installed on our device. We only need to visit or drive by a website by clicking accept for any software, and malicious code will be downloaded in the background on our device.

3.2 Technical Aspects of Cyber Crimes

3.2.1 Unauthorized access & Hacking

Unauthorized Access or Hacking is nothing but unauthorized attempts to bypass the security mechanisms of an information system or network. It is the most popularize form and commonly known cybercrime. The legal definition of 'Hacking' in India is of the widest amplitude. Like other criminal offences, hacking also requires men's rea i.e. intent or knowledge for causing wrongful loss or damage
.

With hackers becoming more organized and increasingly motivated by profit, theft of secured data and leakage of sensitive information have stimulated the corporates as well as individuals to cyber security. In recent trends anyone can become a hacker and hacking is largely possible because of free tools disguised as network tools available on the Internet. In data security, a hacker is a person who specializes in work with the security mechanisms for computer and network systems.

Mobile Phones and Smart Phones are the latest and largest targets of the hackers in recent trends. Indications are that these attacks on Smart Phones had proven even more prolific than those against computer or laptops because there are so many mobile phones than the computer**s.**

3.2.2 Trojan, Virus and Worm Attacks

What is a Virus?

A virus is malicious software (malware) made up of little bits of code attached to legitimate programs. When that software is launched, the virus is launched as well.

Viruses are malicious programs that infect computer files and spread without the user's knowledge. The most common virus infections are spread via e-mail attachments that activate when opened. As infected e-mails are forwarded to multiple people, the virus's vicious cycle continues. Viruses can also be propagated through shared media, such as USB flash drives.

Viruses are responsible for widespread and major computer systems and file loss. They were initially intended as pranks. Anti-virus software can assist prevent, block, or delete viruses that have already been installed.

What is a Worm?

A worm is a harmful software (virus) that replicates itself as it moves from computer to computer, leaving copies of itself in each computer's memory.

A worm finds a computer's vulnerability and spreads like an illness throughout its associated network, constantly looking for new holes. Worms, like viruses, are spread by e-mail attachments from seemingly trustworthy senders. Worms then spread through an e-mail account and address book to a user's contacts.

Some worms reproduce and then go dormant, while others inflict harm. The Worm's code is referred to as payload in such circumstances.

What is a Trojan Horse?

A Trojan horse is malware that disguises itself as a genuine program and downloads it onto a computer. A Trojan horse gets its name from how it's delivered: an attacker often uses social engineering to disguise malicious code within genuine software.

One of the critical characteristics of a Trojan is that it cannot replicate itself, and a user has to install it themselves. It produces a chance for another PC to fully control the infected PC and replicate to harm the host computer systems or steal data. A Trojan horse will damage your computer once it is installed or used, but it will look to be helpful software at first glance.

A Trojan virus spreads by spamming genuine-looking e-mails and attachments to the inboxes of a large number of users. Trojans can also infect devices when cybercriminals persuade people to download malicious software. The malicious software could be disguised in banner advertisements, pop-up ads, or website links.Beast, Zeus, The Blackhole Exploit Kit, and Back Orifice are example of some famous Trojan horses.

Difference between Virus, Worm and Trojan Horse

Virus	Worm	Trojan Horse
A Virus is a computer program or software loaded, either deliberately or unknowingly by the user. It connects to another software/program to execute unanticipated tasks when the system's actual program is running.	A Worm is a computer program similar to a virus that does not communicate with other system programs but multiplies and runs itself to slow down and damage the performance of the system.	Trojan Horse is a hidden piece of malware that steals sensitive information/data from a user's system and sends it to another location across the network.

Viruses cannot be operated remotely since they are installed on the target machine or by the user inadvertently.	Worms can be controlled by the remote because they can open a back door to the host.	Trojan Horse can also be operated remotely, much like worms via the network.
Viruses, like worms, cannot replicate themselves. Viruses also propagate at a moderate rate.	Worms replicate themselves in the system and propagate quicker than viruses and Trojan horses.	In comparison to viruses and worms, a Trojan Horse spreads slowly.
The primary goal of a virus is to alter or erase system data.	Worms aim to degrade system performance and slow it down by eating system resources.	The Trojan horse virus, much like in the story, disguises itself as normal software and steals crucial information
Viruses use executable files to spread.	Worms take use of system flaws to carry out their attacks.	Trojan horse is a type of malware that runs through a program and is interpreted as utility software.

3.2.3 E-Mail related Crimes: Spoofing, Spamming, And Bombing

Email is one of the most useful forms of electronic communication. Of course, its popularity is dwindling with the rise of texting. But it is still common to use email for communicating with individuals and staying up to date with subscriptions to websites.

As with any form of online communication, email is prone to scams and criminal activity. Here are some of the most common ways that people misuse email for criminal purposes.

1. Email Spoofing

A spoof email is an email that seems like it is from a legitimate source but is actually from an unreliable one. Usually, the sender falsifies the name or address of the originator in order to appear valid. For example, someone may send an email pretending to be a close friend or a trustworthy website in order to scam the recipient. Spoofing is often committed with the intention of defrauding the recipient of money.

2. Email Spamming

Spamming is the annoying and dangerous act of sending unsolicited bulk emails or other types of messages over the Internet. Spam is often used to spread malware and phishing and can come your way in the form of emails, social media, instant messages, comments, etc. In this article, we are going to focus on email spam

It may seem like spam email, or junk email, is merely a nuisance in your inbox, but it has the potential to be dangerous. Many cyber criminals deliver viruses via email that once opened or clicked on, deposit dangerous files onto your computer. Criminals can then gain access to your system and personal files or even disable your computer this way. Ransomware and malware are two common types of malicious software that can infect your system or even disable your access to your own data until you pay a "ransom."

3. Email Bombing

An email bomb is a form of Internet abuse which is perpetrated through the sending of massive volumes of email to a specific email address with the goal of overflowing the mailbox and overwhelming the mail server hosting the address, making it into some form of denial of service attack.

3.2.4 Denial of Service Attacks

A denial-of-service (DoS) attack focuses on disrupting network service. Attackers transmit a large amount of data traffic via the network until it becomes overloaded and stops working. A DoS attack can be carried out in a variety of ways, but the most common is a distributed denial-of-service (DDoS) attack. It involves the attacker sending traffic or data, by utilizing several machines that will overload the system. An individual may not recognize that their computer has been hijacked and is helping to the DoS attack in many cases. Disrupting services can have major ramifications for security and internet access; many large-scale DoS attacks have occurred in the past. Many instances of large-scale DoS attacks have been implemented as a single sign of protests toward governments.

A denial-of-service attack is a type of cyber-attack where the perpetrator tries to make a network resource unavailable to its intended users by stopping the services of a host connected to the Internet for a certain length of time or indefinitely. Denial of service is often accomplished by flooding a targeted computer or resource with unnecessary requests that could cause systems to become overburdened, preventing any or all genuine requests from being fulfilled.

In a distributed denial-of-service (DDoS) attack, the incoming traffic flooding the target comes from various places. This renders stopping the attack by just preventing a single source. In a distributed denial-of-service (DDoS) attack, the incoming traffic overwhelming the target comes from several sources. This effectively stops the assault by blocking a single source of the attack.

DoS attack is analogous to a swarm of individuals jamming a store's front entrance, making it difficult for legitimate customers to enter and disrupting commerce.

Attackers attempting to prevent legitimate consumers from using a service are denial-of- service attacks. There are two forms of denial-of-service attacks

- Those that crash services
- Those that flood services

The most dangerous assaults are spread out

3.2.5 Distributed Denial of Service Attack

A distributed denial-of-service (DDoS) attack happens when many computers exceed a targeted system's bandwidth or resources, usually one or more web servers. A DDoS assault uses many distinct IP addresses or computers, sometimes tens of thousands of compromised hosts. A distributed denial of service attack generally requires 3–5 nodes across many networks; however, fewer nodes may not qualify as a DDoS attack.

A group of attack machines can generate more attack traffic than a single attack machine. Turning off multiple attack machines is more challenging than a single assault machine. Each attack machine's activity can be stealthier, making monitoring and shutting down more challenging. Because the incoming traffic that overwhelms the target comes from various sources, ingress screening will not be enough to stop the attack. It's also difficult to distinguish between regular user and attack traffic when distributed across numerous origins.

3.3 Various crimes

3.3.1 IPR Violations (Software piracy, Copyright Infringement, Trademarks Violations, Theft of Computer source code, Patent Violations)

IPR Viloations (Intellectual Property Rights)

In IPR violation, generally, people rob the ideas, inventions, expressions, creativity etc. to gain money, by exploiting the same. In this era of digital technology, such types of wrongdoings are not uncommon. The most popular remedy for IPR infringement is a permanent injunction order from the court which is a civil remedy. As we know, IPR infringement is a violation of the IP rights in personam, which means violation of rights of a particular person/entity and that particular rights holder can take an action against the infringer. But crime is an offence against rem i.e. against the state or nation.

Software Piracy

Software piracy is the act of stealing software that is legally protected. This stealing includes copying, distributing, modifying or selling the software.Software piracy is the unauthorized downloading, copying, use, or distribution of software. Downloading and using software without paying for it is a common tactic of pirated software users. However, software piracy also includes distributing software on multiple machines when a license was only purchased for one, as well as copying software and redistributing it.

Copyright laws were originally put into place so that the people who develop software (programmers, writers, graphic artists, etc.) would get the proper credit and compensation for their work. When software piracy occurs, compensation is stolen from these copyright holders.

Copyright Infringement

Copyright infringement is the use or production of copyright-protected material without the permission of the copyright holder. Copyright infringement means that the rights afforded to the copyright holder, such as the exclusive use of a work for a set period of time, are being breached by a third party. Music and movies are two of the most well-known forms of entertainment that suffer from significant amounts of copyright infringement.

3.3.2 Cyber Squatting, Cyber Smearing, Cyber Stacking

Cyber Squatting

The term cybersquatting refers to the unauthorized registration and use of Internet domain names that are identical or similar to trademarks, service marks, company names, or personal names. Cybersquatting registrants obtain and use the domain name with the bad faith intent to profit from the goodwill of the actual trademark owner. Both the federal government and the Internet Corporation for Assigned Names and Numbers have taken action to protect the owners of trademarks and businesses against cybersquatting abuses.

The primary example of anti-cybersquatting legislation is the Anti-cybersquatting Consumer Protection Act (ACPA). The ACPA is a federal law that prohibits domain name registrations that are identical or similar to trademarks or personal names. An unauthorized user may be found liable to a trademark owner for intending to profit from a distinctive mark. Other U.S. laws, such as the Lanham Act and the Trademark Dilution Revision Act, govern additional trademark and service mark issues. State laws also can provide protection for owners

Cyber Smearing

Defamation is injury to the reputation of a person. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet.

The three essentials of defamation are:

The statement must be false and defamatory,
The said statement must refer to the victim, and
The statement must be published.

A person's reputation is his or her property and sometimes even more valuable than physical property.

Cyber criminals may also disclose victims' personal data (e.g. real name, address, or workplace/ schools) on various immoral websites.

Cases of piggy-backing on victim’s identity are now common. This could be used to publish objectionable material in their name that defames or ridicules a person.

Cyber Stacking

Cyberstalking is the act of persistent and unwanted contact from someone online. It may involve any number of incidents including threats, libel, defamation, sexual harassment, or other actions in which to control, influence, or intimidate their target. Stalking a person online may also involve stalking the person in real life. In many states and countries it is illegal, and could result in criminal charges as a named offence or under harassment and stalking laws.

There have been a number of prominent cases involving cyberstalking, including the incident involving actress Patricia Arquette. In 2011, she deactivated her Facebook account on the advice of her security people due to problems with an online stalker. She decided to only communicate with fans through Twitter and advised fans in her last post to only accept friend requests from people they know.

Cyberstalking doesn’t only affect the rich and famous. According to a 2014 study by the Pew Research Center (Duggan, 2014), 18% of those surveyed said that they had seen someone stalked, while 8% reported that they had been stalked. It also found that women are more likely to experience online sexual harassment or cyberstalking then men. Of these, women aged 18–24 experienced a disproportionately high number of incidents, with 26% having been cyberstalked, and 25% being the target of sexual harassment. This isn’t to say that men aren’t targeted by this type of behavior. The survey found that 7% of men aged 18–24 reported being stalked online, and 13% experienced sexual harassment.

Because cyberstalking could ultimately result in violence, if you’re a target it’s important that you take action as soon as possible. Contact the police and report the crime(s) that have been committed. Gather as much evidence as you can about the incidents. This would include printouts or screenshots of posts and messages, documenting dates and times of incidents, and any other information you might have. You should also evaluate your privacy and security settings, and change the passwords for any email and social media accounts, in case the person has gained access to them. As we’ll see in this and other chapters, many sites also have features to report harassment and other problems, possibly resulting in the person’s account being disabled or removed.

3.3.3 Financial Crimes: (Banking, credit card, Debit card related)

Definition of Financial Crime

According to globally accepted definition it is crime which generates the benefit illicitly or preserve the illicit benefit already generated and obtained. It includes fraud (cheque fraud, credit card fraud, mortgage fraud, medical fraud, corporate fraud, securities fraud (including insider trading), bank fraud, insurance fraud, market manipulation, payment (point of sale) fraud, health care fraud); theft; scams or confidence tricks; tax evasion; bribery; sedition; embezzlement; identity theft; money laundering; and forgery and counterfeiting, including the production of counterfeit money and consumer goods.

Financial Crimes in Banking Sector

A Financial Crime in Banking sector (Banking Fraud) can be defined as potentially used illegal means to obtain money, assets, the property owned by any financial institution, by obtaining money from the depositor and fraudulently posing as any bank or financial institute. Banking fraud is regarded as the criminal offence in India. In the case of legal purposes credit unions and banks are also included that are federally insured. This includes Federal Reserve banks, the Federal Deposit Insurance Corporation (FDIC), mortgage lending agencies, and other institutions that accept deposits of money or other financial assets. Bank frauds are involved basically to defraud the financial institution. From a simple cheque fraud to credit card skimming, it has a wide range.

Unit-4:

4.1 Concepts of Cyber Security

4.1.1 Types of Threats

What are Cyber Security Threats?

Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems. Common categories of cyber threats include malware, social engineering, man in the middle (MitM) attacks, denial of service (DoS), and injection attacks—we describe each of these categories in more detail below.

Cyber threats can originate from a variety of sources, from hostile nation states and terrorist groups, to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts.

Common Sources of Cyber Threats

Nation states— hostile countries can launch cyber-attacks against local companies and institutions, aiming to interfere with communications, cause disorder, and inflict damage.

Terrorist organizations— terrorists conduct cyber-attacks aimed at destroying or abusing critical infrastructure, threaten national security, disrupt economies, and cause bodily harm to citizens.

Criminal groups— organized groups of hackers aim to break into computing systems for economic benefit. These groups use phishing, spam, spyware and malware for extortion, theft of private information, and online scams

.

Hackers— individual hackers target organizations using a variety of attack techniques. They are usually motivated by personal gain, revenge, financial gain, or political activity. Hackers often develop new threats, to advance their criminal ability and improve their personal standing in the hacker community

.

Malicious insiders— an employee who has legitimate access to company assets, and abuses their privileges to steal information or damage computing systems for economic or personal gain. Insiders may be employees, contractors, suppliers, or partners of the target organization. They can also be outsiders who have compromised a privileged account and are impersonating its owner.

4.1.2 Advantages of Cyber Security

In simple words, Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Cyber security is very important for today’s life. Cyber safety provides enhanced cyberspace security, improves cyber resilience, speeds up cyber, data & information protection for businesses it protects individual private information, it protects networks & resources & tackles computer hackers and theft of identity. There are a few advantages & disadvantages of cyber security.

ADVANTAGES

- Cyber security will defend us from critical cyber- attacks.
- It helps us to browse the safe website.
- Cyber security will defend us from hacks & virus.
- The application of cyber security used in our PC needs to update every week.
- Internet security processes all the incoming & outgoing data on our computer.
- It helps to reduce computer chilling & crashes.
- Gives us privacy.

DISADVANTAGES

- It was expensive; most of the users can’t afford this.
- A normal user can’t use this properly, requiring special expertise.
- Lack of knowledge is the main problem.
- It was not easy to use.
- It makes the system slower.
- It could take hours to days to fix a breach in security.

4.2 Basic Terminologies:

4.2.1 IP Address, MAC Address

IP Address:

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

MAC Address:

A MAC address (media access control address) is a 12-digit hexadecimal number assigned to each device connected to the network. Primarily specified as a unique identifier during device manufacturing, the MAC address is often found on a device's network interface card (NIC).

A Media Access Control (MAC) address is a string of characters that identifies a device on a network. It’s tied to a key connection device in your computer called the network interface card, or NIC. The NIC is essentially a computer circuit card that makes it possible for your computer to connect to a network. A NIC turns data into an electrical signal that can be transmitted over the network.

Every NIC has a hardware address that's known as a MAC address. Whereas IP addresses are associated with a networking software called TCP/IP, MAC addresses are linked to the hardware of network adapters.

Manufacturers assign a MAC address to a network adapter when it is produced. It is hardwired or hard-coded onto your computer's NIC and is unique to it. Something called the Address Resolution Protocol (ARP) translates an IP address into a MAC address. Think of the ARP as a passport that takes data from an IP address through an actual piece of computer hardware.

Both MAC Address and IP Address are used to uniquely define a device on the internet. NIC Card's Manufacturer provides the MAC Address, on the other hand, Internet Service Provider provides IP Address.

The main difference between MAC and IP address is that MAC Address is used to ensure the physical address of the computer. It uniquely identifies the devices on a network. While IP addresses are used to uniquely identify the connection of the network with that device takes part in a network.

MAC Address	**IP Address**
MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
MAC Address is a six byte hexadecimal address.	IP Address is either a four-byte (IPv4) or a sixteen-byte (IPv6) address.
A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
NIC Card's Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
MAC Address is used to ensure the physical address of a computer.	IP Address is the logical address of the computer.
MAC Address operates in the data link layer.	IP Address operates in the network layer.
MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
MAC Addresses can't be found easily by a third party.	IP Addresses can be found by a third party.
No classes are used for MAC addressing.	IPv4 uses A, B, C, D, and E classes for IP addressing.

MAC Address sharing is not allowed.	In IP address multiple client devices can share the IP address.
MAC address help to solve IP address issue.	IP addresses never able to solve MAC address issues.
MAC addresses can be used for broadcasting.	The IP address can be used for broadcasting or multicasting.
MAC address is hardware oriented.	IP address is software oriented.

4.2.2 Domain name Server (DNS)

What is DNS?

Every website on the Internet has its own unique address. It's called an IP address. But unlike the physical street address for a house or building, an IP address consists of a set of numbers strung together and separated by periods. A typical IP address in the IPv4 address space looks like: 123.123.123.2. If customers had to memorize the IP addresses of every website they visited, they wouldn't spend much time on the Internet. Thankfully, we use URLs instead. And behind the scenes, there's an "address book" of sorts that helps convert these user-friendly URLs and web addresses into the IP addresses that computers understand. It's called a Domain Name System, or DNS.

In the simplest form, a DNS is a directory of domain names that align with IP addresses. They bridge the gap between computer language and human language – keeping both servers and people happy.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.

What is DNS Security?

When most people use the Internet, they use domain names to specify the website that they want to visit, for instance checkpoint.com. These domain names are user-friendly addresses which are mapped by the Domain Name System (DNS) to Internet Protocol (IP) addresses that computers and other network infrastructure components use to identify different devices connected to the Internet. In sum, the Domain Name System is the protocol that makes the Internet usable by allowing the use of domain names.

DNS is widely trusted by organizations, and DNS traffic is typically allowed to pass freely through network firewalls. However, it is commonly attacked and abused by cybercriminals. As a result, the security of DNS is a critical component of network security.

4.2.3 DHCP, Router, Bots

DHCP

Dynamic Host Configuration Protocol, or DHCP, is used to provide quick and centralized management of IP addresses and other TCP/IP settings on your network. These are things like host IP address, subnet mask, DNS settings, default gateway address, and so on (I call these “IP configuration settings”). When you power on your computer, a DHCP server likely provides these IP configuration settings to you. Even if you don’t have a stand-alone DHCP server, your default gateway likely has its own DHCP server feature.

DHCP really makes network management a lot easier. DHCP eliminates the need for manually assigning IP addresses to our devices. And with this benefit, we decrease the chances of two devices having the same IP address. The following steps describe how DHCP works step-by-step.

Step 1: DHCP Discover: - This first step is a discovery process performed by the workstation. The workstation here refers to the system that currently does not have an IP address. The purpose of this step is to discover any DHCP servers on the network that can hand out IP configuration settings. The workstation accomplishes this task by sending out a broadcast over UDP port 67 that essentially asks, “Hello, are there any DHCP servers available to help me?” This message is referred to as a DHCP Discover message. Importantly, it’s a great idea to have multiple redundant DHCP servers on your network. But, this raises an important question: Since routers don’t forward broadcasts, will we need to install a DHCP server on every broadcast domain? The answer is no. Routers can forward DHCP broadcast messages if they’re configured to do so. Features like “DHCP Relay” and “IP Helper” ensure that DHCP broadcasts can reach other subnets. A relay agent will take a DHCP broadcast and forward it through a router as a unicast transmission to the DHCP server on the other subnet.

Step 2: DHCP Offer: - After step 1 is accomplished and one or more DHCP servers are discovered somewhere on the network, the DHCP servers all reply to the workstation with a broadcast offer to the workstation over UDP port 68. This broadcast contains available IP configuration settings. This message is called a “DHCP Offer.”

Step 3: DHCP Request: - In this third step, the workstation receives all the broadcast offers in step 2, and picks one. Whichever IP configuration settings it chooses, the workstation sends another broadcast back out on UDP port 67. Every DHCP server receives this broadcast. This message is called a DHCP Request.

Step 4: DHCP Acknowledgement: - In this final step, the DHCP server that was responsible for the DHCP request responds with one last broadcast to the workstation and all other DHCP servers over UDP port 68. This DHCP Acknowledgement Message tells the other DHCP servers that the new IP configuration settings are owned by this particular workstation and cannot be reused for anyone else.

Benefits of DHCP.

Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

Reduced network administration. DHCP includes the following features to reduce network administration:

- Centralized and automated TCP/IP configuration.
- The ability to define TCP/IP configurations from a central location.
- The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable devices that move to different locations on a wireless network.
- The forwarding of initial DHCP messages by using a DHCP relay agent, which eliminates the need for a DHCP server on every subnet.

Router

What is a router?

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

There are several types of routers, but most routers pass data between LANs (local area networks) and WANs (wide area networks). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router.

A WAN, by contrast, is a large network spread out over a vast geographic area. Large organizations and companies that operate in multiple locations across the country, for instance, will need separate LANs for each location, which then connect to the other LANs to form a WAN. Because a WAN is distributed over a large area, it often necessitates multiple routers and switches.

How does a router work?

Think of a router as an air traffic controller and data packets as aircraft headed to different airports (or networks). Just as each plane has a unique destination and follows a unique route, each packet needs to be guided to its destination as efficiently as possible. In the same way that an air traffic controller ensures that planes reach their destinations without getting lost or suffering a major disruption along the way, a router helps direct data packets to their destination IP address.

In order to direct packets effectively, a router uses an internal routing table — a list of paths to various network destinations. The router reads a packet's header to determine where it is going, then consults the routing table to figure out the most efficient path to that destination. It then forwards the packet to the next network in the path.

Bots

A ‘bot’ – short for robot – is a software program that performs automated, repetitive, pre-defined tasks. Bots typically imitate or replace human user behavior. Because they are automated, they operate much faster than human users. They carry out useful functions, such as customer service or indexing search engines, but they can also come in the form of malware – used to gain total control over a computer.

Internet bots can also be referred to as spiders, crawlers, or web bots.

A bot is a software application that is programmed to do certain tasks. Bots are automated, which means they run according to their instructions without a human user needing to manually start them up every time. Bots often imitate or replace a human user's behavior. Typically they do repetitive tasks, and they can do them much faster than human users could.

A bot is a small piece of software that automates web requests with various goals. Bots are used to perform tasks without human intervention, including everything from scanning website content to testing stolen credit card numbers to providing customer service support. A bot can be used in both helpful and harmful ways, while “bot attack” always refers to an attacker with a fraudulent goal.

A bot attack is the use of automated web requests to manipulate, defraud, or disrupt a website, application, API, or end-users. Bot attacks started out as simple spamming operations and have branched into complex, multinational criminal enterprises with their own economies and infrastructures.

Bot attacks are automated, ranging from individual cyber criminals to vast hacking organizations. Sophisticated attackers write custom code to vary frequency and length of an automated attack, designed to circumvent security monitoring.

Bots usually operate over a network; more than half of Internet traffic is bots scanning content, interacting with Webpages, chatting with users, or looking for attack targets. Some bots are useful, such as search engine bots that index content for search or customer service bots that help users. Other bots are "bad" and are programmed to break into user accounts, scan the web for contact information for sending spam, or perform other malicious activities. If it's connected to the Internet, a bot will have an associated IP address.

Bots can be:

Chatbots: Bots that simulate human conversation by responding to certain phrases with programmed responses

Web crawlers (Googlebots): Bots that scan content on WebPages all over the Internet

Social bots: Bots that operate on social media platforms

Malicious bots: Bots that scrape content, spread spam content, or carry out credential stuffing attacks

4.3 Common Types of Attacks:

4.3.1 Distributed Denial of Service

DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

Motivations for carrying out a DDoS vary widely, as do the types of individuals and organizations eager to perpetrate this form of cyberattack. Some attacks are carried out by disgruntled individuals and hacktivists wanting to take down a company's servers simply to make a statement, have fun by exploiting cyber weakness, or express disapproval.

Other distributed denial-of-service attacks are financially motivated, such as a competitor disrupting or shutting down another business's online operations to steal business away in the meantime. Others involve extortion, in which perpetrators attack a company and install hostageware or ransomware on their servers, then force them to pay a large financial sum for the damage to be reversed.

DDoS attacks are on the rise, and even some of the largest global companies are not immune to being "DDoS'ed". The largest attack in history occurred in February 2020 to none other than Amazon Web Services (AWS), overtaking an earlier attack on GitHub two years prior. DDoS ramifications include a drop in legitimate traffic, lost business, and reputation damage.

How DDoS Attacks Work

A DDoS attack aims to overwhelm the devices, services, and network of its intended target with fake internet traffic, rendering them inaccessible to or useless for legitimate users.

DoS vs. DDoS

A distributed denial-of-service attack is a subcategory of the more general denial-of-service (DoS) attack. In a DoS attack, the attacker uses a single internet connection to barrage a target with fake requests or to try and exploit a cybersecurity vulnerability. DDoS is larger in scale. It utilizes thousands (even millions) of connected devices to fulfill its goal. The sheer volume of the devices used makes DDoS much harder to fight.

Botnets

Botnets are the primary way distributed denial-of-service-attacks are carried out. The attacker will hack into computers or other devices and install a malicious piece of code, or malware, called a bot. Together, the infected computers form a network called a botnet. The attacker then instructs the botnet to overwhelm the victim's servers and devices with more connection requests than they can handle.

Types of DDoS Attacks

Volume-Based or Volumetric Attacks

This type of attack aims to control all available bandwidth between the victim and the larger internet. Domain name system (DNS) amplification is an example of a volume-based attack. In this scenario, the attacker spoofs the target's address, then sends a DNS name lookup request to an open DNS server with the spoofed address.

When the DNS server sends the DNS record response, it is sent instead to the target, resulting in the target receiving an amplification of the attacker’s initially small query.

Protocol Attacks

Protocol attacks consume all available capacity of web servers or other resources, such as firewalls. They expose weaknesses in Layers 3 and 4 of the OSI protocol stack to render the target inaccessible.

A SYN flood is an example of a protocol attack, in which the attacker sends the target an overwhelming number of transmission control protocol (TCP) handshake requests with spoofed source Internet Protocol (IP) addresses. The targeted servers attempt to respond to each connection request, but the final handshake never occurs, overwhelming the target in the process.

Application-Layer Attacks

These attacks also aim to exhaust or overwhelm the target's resources but are difficult to flag as malicious. Often referred to as a Layer 7 DDoS attack—referring to Layer 7 of the OSI model—an application-layer attack targets the layer where web pages are generated in response to Hypertext Transfer Protocol (HTTP) requests.

A server runs database queries to generate a web page. In this form of attack, the attacker forces the victim's server to handle more than it normally does. An HTTP flood is a type of application-layer attack and is similar to constantly refreshing a web browser on different computers all at once. In this manner, the excessive number of HTTP requests overwhelms the server, resulting in a DDoS.

DDoS Attack Prevention

Even if you know what a DDoS attack is, It is extremely difficult to avoid attacks because detection is a challenge. This is because the symptoms of the attack may not vary much from typical service issues, such as slow-loading web pages, and the level of sophistication and complexity of DDoS techniques continues to grow.

Further, many companies welcome a spike in internet traffic, especially if the company recently launched new products or services or announced market-moving news. As such, prevention is not always possible, so it is best for an organization to plan a response for when these attacks occur.

4.3.2 Man in the Middle, Email Attack

A MITM attack is a form of cyber-attack where a user is introduced with some kind of meeting between the two parties by a malicious individual, manipulates both parties and achieves access to the data that the two people were trying to deliver to each other. A man-in-the-middle attack also helps a malicious attacker, without any kind of participant recognizing till it's too late, to hack the transmission of data intended for someone else and not supposed to be sent at all. In certain aspects, like MITM, MitM, MiM or MIM, MITM attacks can be referred.

If an attacker puts himself between a client and a webpage, a Man-in-the-Middle (MITM) attack occurs. This form of assault comes in many different ways.

For example, In order to intercept financial login credentials, a fraudulent banking website can be used. Between the user and the real bank webpage, the fake site lies "in the middle."

How does MITM work

There are several reasons and strategies for hackers to use a MITM attack. Usually, like credit card numbers or user login details, they try to access anything. They also spy on private meetings, which may include corporate secrets or other useful information.

Types of Attacks

Although ARP poisoning is commonly known as a MitM attack, other forms of data interception also give attackers the ability to read private communications between two parties.

Email hijacking:

Email messages sent in clear text are open to eavesdropping, but an attacker can also read messages should they obtain a targeted user’s username and password to the email account. The attacker may wait silently reading messages until sensitive information is transferred such as a financial transaction, and then use the targeted user’s email address to send a message that will reroute money transfers to the attacker’s bank account.

Wi-Fi eavesdropping:

A poorly secured Wi-Fi connection could be subject to a MitM using a method called ARP poisoning. The attacker’s device is used as the default gateway between the sender and the Wi-Fi router where data can be intercepted and read. Attackers also use malicious hotspots of their own to trick users into connecting and routing communication through the attacker-controlled hotspot.

Session hijacking:

When users connect to a server, a unique session is created that identifies the user on the server. Attackers with access to this session token can impersonate the user and read data on a web application.

IP spoofing:

Using a fraudulent IP address, an attacker can reroute traffic from an official site to an attacker-controlled server.

DNS spoofing:

Similar to IP spoofing, DNS spoofing alters a website’s address record to divert traffic to an attacker-controlled server. Any information sent to this server is intercepted by the attacker unbeknownst to the tricked users.

How to Prevent MitM Attacks

Because MitM attacks are invisible and silent to the targeted user, it’s essential that users take the necessary precautions to prevent them. It’s also the responsibility of the application developer to ensure that their software is not vulnerable to MitM attacks. In some cases, users would be unable to prevent a man-in-the-middle attack due to the way an application is coded.

Some methods to prevent becoming a victim of a MitM attack:

Use two-factor authentication on email accounts. Should an attacker obtain email credentials for your account, successful authentication would not be possible as the attacker would not have access to the 2FA PIN.

Use traffic analytical tools on the network. These tools help administrators identify suspicious traffic and provides analytics into ports and protocol usage across users and devices.

Use certificate pinning on mobile apps. Certificate pinning whitelists approved certifications, which blocks any attacker-controlled certificates from being used with the application. Certificate pinning is the responsibility of the application developer.

Use VPN on public Wi-Fi networks. With VPN, an attacker may intercept data but would be unable to read data or downgrade to a weaker encryption protocol as the VPN uses its own encryption algorithm to package data and transfer it across the internet.

Educate employees about the dangers of phishing. Some MitM and malware attacks start with phishing attacks. Educate employees to identify phishing attacks so that they do not install malware or send credentials to attackers.

Integrate email security. Email filters will detect a majority of phishing emails or messages with malicious attachments and send them to a safe quarantine storage where they can be reviewed by an administrator.

Never connect to an unknown Wi-Fi hotspot. Attackers use malicious hotspots with names similar to an official source. Users should never connect to a public Wi-Fi without first verifying that it is indeed owned by the official provider.

4.3.3 Password Attack, Malware

Password attacks involve exploiting a broken authorization vulnerability in the system combined with automatic password attack tools that speed up the guessing and cracking passwords. The attacker uses various techniques to access and expose the credentials of a legitimate user, assuming their identity and privileges. The username-password combination is one of the oldest known account authentication techniques, so adversaries have had time to craft multiple methods of obtaining guessable passwords. Additionally, applications that use passwords as the sole authentication factor are vulnerable to password attacks since the vulnerabilities are well understood.

Password attacks have far-reaching consequences since malicious users only require unauthorized access to a single privileged account or a few users accounts to compromise the web application. Depending on the data hosted by the application, compromised passwords can pave the way for the exposure of sensitive information, distributed denial-of-service, financial fraud, and other sophisticated attacks.

.

4.4 Hackers:

The basic definition of a hacker is someone who uses a computer system to gain unauthorized access to another system for data or who makes another system unavailable. These hackers will use their skills for a specific goal, such as stealing money, gaining fame by bringing down a computer system, or making a network unavailable -- even sometimes destroying them. However, there are three different types of hackers, each with a particular goal, and not all are the bad guys.

A hacker is a person who breaks into a computer system. The reasons for hacking can be many: installing malware, stealing or destroying data, disrupting service, and more. Hacking can also be done for ethical reasons, such as trying to find software vulnerabilities so they can be fixed.

4.4.1 Various Vulnerabilities:

Vulnerabilities are flaws in a computer system that weaken the overall security of the device/system. Vulnerabilities can be weaknesses in either the hardware itself, or the software that runs on the hardware. Vulnerabilities can be explorrited by a threat actor, such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions) within a computer system. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerabilities are also known as the attack surface.

In Short, security vulnerability is an unintended characteristic of a computing component or system configuration that multiplies the risk of an adverse event or a loss occurring either due to accidental exposure, deliberate attack, or conflict with new system components.
The Difference among Vulnerabilities, Threats and Risks

Many people may use the terms vulnerability, threat and risk interchangeably. However, in the cybersecurity world, these terms have distinct and specific meanings.

As noted above, a vulnerability is a weakness that can be exploited by a malicious actor. For example, unpatched software or overly permissive accounts can provide a gateway for cybercriminals to

access the network and gain a foothold within the IT environment.
A threat is a malicious act that can exploit a security vulnerability.
A risk is what happens when a cyber threat exploits a vulnerability. It represents the damage that could be caused to the organization in the event of a cyberattack.

4.4.1.1 Injection attacks, Changes in security settings

Injection attacks: Injection attacks refer to a broad class of attack vectors. In an injection attack, an attacker supplies untrusted input to a program. This input gets processed by an interpreter as part of a command or query. In turn, this alters the execution of that program.

Injections are amongst the oldest and most dangerous attacks aimed at web applications. They can lead to data theft, data loss, loss of data integrity, denial of service, as well as full system compromise. The primary reason for injection vulnerabilities is usually insufficient user input validation.

Types of Injection Attacks

SQL injection (SQLi) and Cross-site Scripting (XSS) are the most common injection attacks but they are not the only ones. The following is a list of common injection attack types.

Injection attack	Description	Potential impact
Code injection	The attacker injects application code written in the application language. This code may be used to execute operating system commands with the privileges of the	Full system compromise

Injection attack	Description	Potential impact
	user who is running the web application. In advanced cases, the attacker may exploit additional privilege escalation vulnerabilities, which may lead to full web server compromise.	
CRLF injection	The attacker injects an unexpected CRLF (Carriage Return and Line Feed) character sequence. This sequence is used to split an HTTP response header and write arbitrary contents to the response body. This attack may be combined with Cross-site Scripting (XSS).	Cross-site Scripting (XSS)
Cross-site Scripting (XSS)	The attacker injects an arbitrary script (usually in JavaScript) into a legitimate website or web application. This script is then executed inside the victim's browser.	Account impersonation Defacement Run arbitrary JavaScript in the victim's browser
Email Header Injection	This attack is very similar to CRLF injections. The attacker sends IMAP/SMTP commands to a mail server that is not directly available via a web application.	Spam relay Information disclosure
Host Header Injection	The attacker abuses the implicit trust of the HTTP Host header to poison password-reset functionality and web caches.	Password-reset poisoning Cache poisoning
LDAP Injection	The attacker injects LDAP (Lightweight Directory Access Protocol) statements to execute arbitrary LDAP commands. They can gain permissions and modify the contents of the LDAP tree.	Authentication bypass Privilege escalation Information disclosure
OS Command Injection	The attacker injects operating system commands with the privileges of the user who is running the web application. In advanced cases, the attacker may exploit additional privilege escalation vulnerabilities, which may lead to full system compromise.	Full system compromise
SQL Injection (SQLi)	The attacker injects SQL statements that can read or modify database data. In the case of advanced SQL Injection attacks, the attacker can use SQL commands to write arbitrary files to the server and even execute OS commands. This may lead to full system compromise.	Authentication bypass Information disclosure Data loss Sensitive data theft Loss of data integrity Denial of service Full system compromise.
XPath injection	The attacker injects data into an application to execute crafted XPath queries. They can use them to access unauthorized data and bypass authentication.	Information disclosure Authentication bypass

Changes in security settings: Security misconfiguration is the lack of proper security in server or web apps, opening up your business to cyber threats. This kind of misconfiguration runs rampant, commonly occurring when levels of the application stack are upgraded while others are left untouched, as the default settings may have included insecurities that go unaddressed.

- Running an application with debug enabled in production
- Having directory listing (which leaks valuable information) enabled on the server
- Running outdated software (think WordPress plugins, old PhpMyAdmin)
- Running unnecessary services
- Not changing default keys and passwords (which happens more frequently than you'd believe)
- Revealing error handling information (e.g., stack traces) to potential attackers

4.4.1.2 Expouser of Sensitive Data

Exposure of Sensitive Data: Sensitive data exposure can happen in several ways. Sheer human negligence can cause data to be uploaded to a public website or a commonly accessed database. Inappropriate access controls might lead to a single employee owning control over a huge database of sensitive information. Unlike a data breach, there isn't always malicious intent behind such scenarios. Human errors or system misconfigurations cause sensitive data (intellectual property, user credentials, personally identifiable information, payment details, etc.) to end up in the wrong place where it is vulnerable to exploitation.

This web security vulnerability is about crypto and resource protection. Sensitive data should be encrypted at all times, including in transit and at rest. No exceptions. Credit card information and user passwords should never travel or be stored unencrypted, and passwords should always be hashed. Obviously, the crypto/hashing algorithm must not be a weak one. When in doubt, web security standards recommend AES (256 birts and up) and RSA (2048 bits and up).

It cannot be overemphasized that session IDs and sensitive data should not travel in URLs. Cookies with sensitive data should have the "secure" flag on.

4.4.1.3 Breach in authentication protocol

Breach in authentication protocol: Broken authentication is an umbrella term for several vulnerabilities that attackers exploit to impersonate legitimate users online. Broadly, broken authentication refers to weaknesses in two areas: session management and credential management. Both are classified as broken authentication because attackers can use either avenue to masquerade as a user: hijacked session IDs or stolen login credentials.

Attackers employ a wide variety of strategies to take advantage of these weaknesses, ranging from huge credential stuffing attacks to highly targeted schemes aimed at gaining access to a specific person's credentials

Session Management Flaws Open the Door to Attacks. Session management is part of broken authentication, but the two terms are often listed side by side so people don't assume that "authentication" refers only to usernames and passwords. Since web applications use sessions and credentials to identify individual users, attackers can impersonate them using either mechanism.

Attackers Exploit Weak and Compromised Credentials. Malicious actors use various methods to steal, guess, or trick users into revealing their passwords. It includes various ways such as password spraying, Phishing Attacks etc. Password spraying is a little like credential stuffing, but instead of working off a database of stolen passwords, it uses a set of weak or common passwords to break into a user's account. Attackers typically phish by sending users an email pretending to be from a trusted source and then tricking users into sharing their credentials or other related information. It can be a broad-based attempt that hits everyone at an organization with the same phony email, or it can take the form of a “spear phishing” attack tailored to a specific target.

4.4.2 Types of Hackers: White hat and Black hat

Main types of hackers: Black hat hacker, White hat hacker and Gray hat hacker.

1) **Black Hat Hacker - Evil Doer**

The black hat hacker is the one who hacks for malicious intent - he is the bad guy. This type of hacker uses his or her skills to steal money or data, knock a computer system offline, or even destroy them. Some of these hackers love to see their work and name in the news, so they would try to target big name organizations and companies. For instance, they might change the front page of a company website.

Black hats also try to break into computer systems to steal credit card information and possibly steal valuable information to sell on the black market. They may even lock out the computer and network system from the owners and then hold them for ransom.

The black hat works outside of the law. This is the hacker that we as a society are most familiar with. Some black hats have cost companies hundreds of millions of dollars in damages for credit card and social security information theft. They can work alone, in that case known as a lone wolf, or with a team. They work slowly and methodically, since the black hat knows it takes patience to compromise a computer or a network system in order to a hit a big payoff and not be caught.

2) **White Hat Hacker – Ethical Hacker**

White hat hackers are cyber security professionals who are authorized or certified to hack organizational networks and computer systems. They use their expertise and skills to find vulnerabilities in systems. A white hacker is also known as Ethical Hacker.

Typically, large organizations, businesses, and governments hire white hat hackers to identify security vulnerabilities before black hat hackers can. White hat hackers spot and fix the weaknesses in the security systems and safeguard them against external attacks and data breaches. They are also known as ethical hackers.

Ethical hackers, thus, do not intend to harm a system. Instead, they find loopholes in a system as a part of penetration testing and vulnerability assessments.

White hat hackers usually have a good degree of technical expertise and broad skills in programming, networking, and IT.

3) **Gray hat hackers**

Gray hat hackers may not have the criminal or malicious intent of a black hat hacker, but they also don’t have the prior knowledge or consent of those whose systems they hack into. Nevertheless, when gray hat hackers uncover weaknesses such as zero-day vulnerabilities, they report them rather than fully exploiting them. But gray hat hackers may demand payment in exchange for providing full details of what they uncovered

Unit-5:

5.1 Ethical Hacker

An ethical hacker, also referred to as a white hat hacker, is an information security (infosec) expert who penetrates a computer system, network, application or other computing resource on behalf of its owners -- and with their authorization. Organizations call on ethical hackers to uncover potential security vulnerabilities that malicious hackers could exploit.

The purpose of ethical hacking is to evaluate the security of and identify vulnerabilities in target systems, networks or system infrastructure. The process entails finding and then attempting to exploit vulnerabilities to determine whether unauthorized access or other malicious activities are possible.

What is ethical hacking?

An ethical hacker needs deep technical expertise in infosec to recognize potential attack vectors that threaten business and operational data. People employed as ethical hackers typically demonstrate applied knowledge gained through recognized industry certifications or university computer science degree programs and through practical experience working with security systems.

Ethical hackers generally find security exposures in insecure system configurations, known and unknown hardware or software vulnerabilities, and operational weaknesses in process or technical countermeasures. Potential security threats of malicious hacking include distributed denial-of-service attacks in which multiple computer systems are compromised and redirected to attack a specific target, which can include any resource on the computing network.

An ethical hacker is given wide latitude by an organization to legitimately and repeatedly attempt to breach its computing infrastructure. This involves exploiting known attack vectors to test the resiliency of an organization's infosec posture.

What do ethical hackers do?

Ethical hackers can help organizations in a number of ways, including the following:

Finding vulnerabilities. Ethical hackers help companies determine which of their IT security measures are effective, which need updating and which contain vulnerabilities that can be exploited. When ethical hackers finish evaluating an organization's systems, they report back to company leaders about those vulnerable areas, which may include a lack of sufficient password encryption, insecure applications or exposed systems running unpatched software. Organizations can use the data from these tests to make informed decisions about where and how to improve their security posture to prevent cyber attacks.

Demonstrating methods used by cybercriminals. These demonstrations show executives the hacking techniques that malicious actors could use to attack their systems and wreak havoc on their businesses. Companies that have in-depth knowledge of the methods the attackers use to break into their systems are better able to prevent those incursions.

Helping to prepare for a cyber attack. Cyber attacks can cripple or destroy a business -- especially a smaller business -- but most companies are still unprepared for cyber attacks. Ethical hackers understand how threat actors operate, and they know how these bad actors will use new information and techniques to attack systems. Security professionals who work with ethical hackers are better able to prepare for future attacks because they can better react to the constantly changing nature of online threats.

5.1.1 Roles and Responsibilities

There seems to be a general misconception that a person with an ethical hacking career is only responsible for penetration testing of systems and applications. This is not true, and an ethical hacker is responsible for much more.

- Scanning open and closed ports using Reconnaissance tools like Nessus and NMAP
- Engaging in social engineering methodologies
- Examining patch releases by performing vigorous vulnerability analysis on them
- An ethical hacker will see if he/she can evade IDS (Intrusion Detection systems), IPS (Intrusion Prevention systems), honeypots and firewalls
- Ethical hackers can employ other strategies like sniffing networks, bypassing and cracking wireless encryption, and hijacking web servers and web applications

An ethical hacker strives to replicate the working of a black hat hacker by analyzing the defence protocols and social-engineering aspects of an organization. His job is to make sure the organization reacts to these situations well enough if they are already not doing so.

When you think about a ‘hacker,’ you probably envision a person who loves a good puzzle and likes to go about breaking into computer systems. Someone who knows how to slither their way in and out so as to obtain the information and data they need or want. Many individuals are hackers and are actually paid by enterprises to exactly figure out how a criminal could hack into the organization’s computer system.

These folks are referred to as ethical hackers and are entrusted with the exact determination of how a typical criminal hacker could break into an establishment’s computer systems. Ethical hacking is a growing discipline for persons that are interested in computers; the caveat is that you do not necessarily need a diploma or degree. Nevertheless, any type of post-secondary education is definitely considered an asset to any individual looking to pursue ethical hacking

.

5.1.2 Benefit of Ethical Hacking

Learning ethical hacking involves studying the mindset and techniques of black hat hackers and testers to learn how to identify and correct vulnerabilities within networks. Studying ethical hacking can be applied by security pros across industries and in a multitude of sectors. This sphere includes network defender, risk management, and quality assurance tester.

However, the most obvious benefit of learning ethical hacking is its potential to inform and improve and defend corporate networks. The primary threat to any organization's security is a hacker: learning, understanding, and implementing how hackers operate can help network defenders prioritize potential risks and learn how to remediate them best. Additionally, getting ethical hacking training or certifications can benefit those who are seeking a new role in the security realm or those wanting to demonstrate skills and quality to their organization.

You understood what is ethical hacking, and the various roles and responsibilities of an ethical hacker, and you must be thinking about what skills you require to become an ethical hacker. So, let's have a look at some of the ethical hacker skills

5.1.3 Skills require to become Ethical hacker

An ethical hacker must have a bachelor’s degree in information technology or an advanced diploma in network security. He needs extensive experience in the area of network security and a working knowledge of various operating systems. Areas of expertise include a sound working knowledge of Microsoft and Linux servers, Cisco network switches, virtualization, Citrix and Microsoft Exchange. A working knowledge of the latest penetration software is essential. The International Council of E-Commerce Consultants, or EC-Council, certifies professionals as certified ethical hackers and as certified network defense architects if they work for select agencies of the federal government.

Working as an ethical hacker can be one of the most creative and fulfilling jobs available in cybersecurity. Few other industry professionals are allowed the same degree of latitude in their work or encouraged to break the constraints of the working environment like white hat hackers.

Broadly speaking, the job of a white hat hacker is to find vulnerabilities before the black hats can do so. The ethical hacker uses many of the same tools and goes through the same steps:

Researching the intended target via both open-source and dark-web channels

Scanning target networks and systems with commercial, open-source, or custom vulnerability scanners

Designing a plan of attack that can include exploiting software vulnerabilities, systemic vulnerabilities, social manipulation, or any combination of those factors Many of these activities may happen at odd hours, conforming to times when the target may be least monitored and most vulnerable. Sometimes work is performed on-site at the client company, and other times remotely via the Internet.

But it’s not all fun and games. Ethical hacking is a job, not a joy ride through other people’s networks. Ethical hackers are expected to carefully document the steps taken to uncover vulnerabilities and detail exactly how they were able to compromise client security systems. Long hours can be spent writing up reports in clear and concise language for corporate executives. And, after breaching a target, the ethical hacker might be expected to spend time with the hapless IT group that was just compromised, helping to advise and train them to avoid future penetrations.

Not all ethical hacking is strictly confined to penetration testing, however. Many ethical hackers spend a great deal of time either writing or examining computer code, to either look for or exploit flaws. They attempt to push systems and devices to accomplish tasks that the creators may not have envisioned.

Ethical Hacker Qualification

An ethical hacker must have a bachelor’s degree in information technology or an advanced diploma in network security. He needs extensive experience in the area of network security and a working knowledge of various operating systems. Areas of expertise include a sound working knowledge of Microsoft and Linux servers, Cisco network switches, virtualization, Citrix and Microsoft Exchange. A working knowledge of the latest penetration software is essential. The International Council of E-Commerce Consultants, or EC-Council, certifies professionals as certified ethical hackers and as certified network defense architects if they work for select agencies of the federal government.

In order to become an ethical hacker it's necessary to have a bachelor's degree in a related field, such as computer science. Ethical hackers need to have computer programming experience and familiarity with a range of different programming languages. It's common for employers to require ethical hackers to have Certified Ethical Hacker (CEH) certification and other recognized certifications, such as CompTIA, that prepare them to work as experts in cyber security.

Ethical hackers need to have strong analytical skills because their work involves reviewing a lot of data to identify potential issues with computer network security. Their work can involve consulting with clients, explaining their findings to managers or clients, and collaborating with other professionals who are involved with information security. They therefore need to have excellent customer service skills and strong interpersonal skills. Communication skills are also important so that they can effectively explain their test results to clients and coworkers. Exceptional problem-solving skills and attention to detail are fundamental since ethical hackers need to be thorough in their attempts to breech the security systems in place. They must also develop new and often innovative strategies that enable them to identify problems with the security systems they work on.

5.2 Penetration testing concepts

What is a penetration test? If you're struggling to understand the intricacies of penetration testing, you're not alone. To those unfamiliar with the world of cybersecurity and ethical hacking, a penetration test can be a very foreign concept.

Learn more about penetration testing, why it's so critical in cybersecurity, and how penetration testers play a role in exposing network security vulnerabilities.

Also known as a "pen testing" or "white-hat hacking," a penetration test is a simulated cyberattack against a computer system to find exploitable security vulnerabilities. Penetration testing helps organizations manage risk, protect clients from data breaches, and increase business continuity. This testing is essential for maintaining compliance in highly regulated industries such as banking and healthcare.

Basically, pen testing helps businesses answer the question, "Is my data easy to steal?" When it comes to protecting valuable data from cyberattacks, knowing the answer to that is critical. Data breaches are costly. In fact, IBM estimates that U.S. companies lose an average of $7.35 million per data breach!

5.2.1 Phases of Ethical hacking

Protecting against data breaches through pen testing requires a thorough approach. Penetration tests usually have five phase/stages:

1. Planning. The pen tester determines the goals for the test and does preliminary system reconnaissance. This is the information-gathering stage of the test. It often involves social engineering to gather the data needed to carry out the attack.

2. Scanning. Next, the tester analyzes or “scans” the system to determine how it will respond to their attack. They often use technical tools to help in this process. They perform vulnerability scanning and look for gateways to gain access.

3. Breaching. Here, the tester uses cross-site scripting, SQL injection, backdoors, or other strategies to pinpoint where they can bypass the firewall and break into the system. They then breach the system, take control of the network or devices and begin extracting the data.

4. Burrowing. Then, the penetration tester sees how long they can stay in the system, what data is compromised, and how much deeper they can burrow into it. They attempt to maintain access as long as possible by creating persistence, which entails planting rootkits and installing backdoors.

5. Analyzing. The tester creates a detailed configuration review and reports on the results. They often simulate how a hacker would cover their tracks to eliminate evidence that a cyberattack happened. At the end of the test, the ethical hacker gathers the information they obtained and takes note of where they found exploitable vulnerabilities.

Outside of network security testing, pen tests also challenge an organization’s incident response capabilities—i.e., how prepared they are to respond to an attack. The logic here is that the more practice companies get, the better they’ll cope with a real incident.

5.2.2 Areas of penetration testing

This leads to the different categories of testing that you might run as an ethical hacker. Five general services meet varying needs for web applications or software:

External Testing

An external penetration test targets company assets that are visible to external parties, such as websites, web applications, domain name servers (DNS), and emails. The goal of these tests is to see if hackers can gain access to and extract data from external systems. This type of penetration testing measures a system’s vulnerability to outside attackers.

Internal Testing

An internal penetration test simulates an attack by a malicious insider—someone with access to systems behind a company’s firewall. This pen testing method can also be used to screen employees on their vulnerability to external social engineering or phishing attacks in which their credentials can be stolen with an eye toward mitigation of potential risks.

Blind Testing

In a blind test, your role as a pen tester would be to target an enterprise using very limited information—hence the term “blind.” In a blind test, a pen-tester acts as a real hacker tasked with using only publicly accessible information to gain access to a system. While the tester is blind, in this type of test the target organization is generally not. Rather, the target is told what the pen-tester will attack, how they’ll attack, and when. A blind test provides a good level of vulnerability assessment, though it is not quite as informative as a double-blind test which will be discussed next.

Double-Blind Testing

Also called “zero-knowledge testing,” a double-blind test refers to a penetration test in which neither the pen tester nor the target is informed of the scope. Think of it like a fire drill in school where neither students nor teachers know about the event. In short, both the tester and the target are blind to the test. In this situation, security personnel have no advance knowledge of a simulated attack. This stops them from shoring up their defenses before an attempted breach and provides a more realistic picture as to what areas need to be addressed. Vulnerability is clear inside this penetration testing method because security personnel aren't ready for pen testers to hack, so they have to rely on their processes and strategies.

Targeted Testing

Lastly, in targeted testing, both the tester and security team work together—keeping each other apprised of their movements. This gives the entire pen test team invaluable real-time feedback from a hacker’s point of view. This type of penetration testing is less about vulnerability and more about understanding the best information security strategies to implement.

5.3 SQL Injection:

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.

5.3.1 Concepts of SQL Injection

SQL Injection (SQLi) is a popular attack vector that makes it possible for an attacker to perform malicious SQL statements for backend database manipulation or restrict the queries that an application makes to its database. Attackers take advantage of SQL Injection vulnerabilities to bypass login and other application security procedures. In simple words, SQL Injection permits an attacker to access data that they would normally be unable to recover. This data may comprise a few items, such as private details about a client, sensitive company data, or user lists.

An SQL Injection attack is based on an “injection” or insertion of a SQL query through input data from the customer to the application. SQL Injection is typically recognized as an attack vector for websites; however, it can be exploited to attack any number of SQL databases. The actions of a successful SQL Injection exploit can access delicate information from the database, amend the data from the database (Insert, Modify, and Delete), retrieve the content of a specified file available on the DBMS file system, become administrators of the database server (including shutting down the DBMS), and in some situations, send commands to the operating system.

Simply, a successful SQL attack can be carried out through the following methods:

- Adjusting or compromising data
- Exfiltrating or pinching data
- Sidestepping authentication
- Changing database permissions
- Removing data
- Running arbitrary code

What Is 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 successful SQL injection attack can badly affect websites or web applications using relational databases such as MySQL, Oracle, or SQL Server. In recent years, there have been many security breaches that resulted from SQL injection attacks.

How Does SQL Injection Work?

SQL is a query language intended to run data kept in functional databases. SQL queries are implemented to perform commands, like updates, data retrieval, and deletion of records. Diverse SQL essentials execute these tasks. Examples include, queries using the SELECT statement to recover data through user-offered strictures.

For an SQL Injection attack to be executed, the hacker must first discover defenseless user inputs in the web application or web page. SQL Injection is then exploited by unscrupulous hackers to locate the IDs of other users within the database, and these users are then impersonated by the attacker. The impersonated users are often people with data privileges such as the database administrator.

The web application or web page with an SQL Injection vulnerability exploits the user's input openly in an SQL query and generate input content. This type of content is usually referred to as a "malicious payload," and it represents the most significant aspect of the attack. The malicious SQL commands are performed in the database once the malicious hacker sends this content.

Since SQL makes it possible for you to choose and output data from the database, an SQL Injection vulnerability may permit the attacker to have full access to the entire data within a database server. SQL is designed in such a way that it allows you to modify or change the data in a database and insert new ones. An attacker can use SQL Injection in a financial application to make some transactions void, change balances, or move money from the user's account to another account.

5.3.2 Types of SQL Injection

SQL Injection types exist in different categories; however, they are all concerned with an attacker introducing random SQL into a web page or web application database query. The easiest method of SQL Injection is via user input. Typically, web apps receive user input using a form. So, the front end sends the user input to the back-end database for processing.

In the situation when the web application fails to sanitize user input, the attacker can introduce the SQL they select into the back-end database and duplicate, modify, or remove the contents of the database. SQL Injection types can be categorized into three main groupings, including In-band SQLi, Out-of-band SQLi, and Blind or Inferential SQLi.

1) In-band SQLi :-

In-band SQL Injection happens when an unscrupulous hacker can effectively apply the same communication channel for introducing an attack and collating the results. Attackers exploit the same channel of communication to introduce their attacks and to assemble their outcomes. In-band SQL Injection is one of the simplest and most popular SQL Injection attacks, making it easy to exploit. The two popularly known sub-categories of in-band SQL Injection include:

1. Error-based SQLi

This is an in-band SQL Injection practice where an attacker executes actions that lead to error messages. These error messages are cast by the database server to gain data regarding the structure of the database. Although errors are extremely valuable during the development stage of a web application, these should be logged to a file with limited access or deactivated on a live site.

2. Union-based SQLi

Union-based SQL Injection technique takes advantage of the UNION SQL operator to merge the results of multiple SELECT statements to get a single result that is afterward sent back as part of the HTTP response. This attacker leverages the data from this response.

2) Out-of-band SQLi

Unlike the in-band SQLi technique, the out-of-band SQLi technique is not as popular. The reason is that an attacker can only perform this type of attack when specified features are activated on the database server engaged by the web page. This type of attack is mostly used when an attacker is unable to use the same channel to introduce the attack and assemble results.

It is an alternative to the Blind and in-band SQLi practices, particularly when the server responses are less steady. Out-of-band SQLi procedures matter based on the capability of the server to generate HTTP or DNS requests to transmit data back to an attacker

3) Blind or Inferential SQLi

Most situations of an SQL Injection attack are blind vulnerabilities. This is because applications do not send back SQL query results or the particulars of database errors within its responses. As an alternative, an attacker who can reconstruct the structure of the database by transmitting payloads monitors the response of the web application and the ensuing performances of the database server. This is often more complicated and difficult for an attacker to exploit, but it is as dangerous as any other form of SQL Injection available. Inferential or blind SQLi can be grouped into two sub–categories:

1. Time-Based

Using this blind technique, the attacker transfers a SQL query to the database, making the database hold for some seconds before responding. Time-based SQLi depends on transferring an SQL query to the database, which in turn influences the database to halt for a short period, usually in seconds, before it can react. The attacker can observe from the response time whether the ensuing query is true or false.

Depending on the result, an HTTP response is created immediately or after a delay. The attacker can, therefore, understand if the message they applied returned true or false, without depending on the data from the database. This type of attack is often time-consuming, particularly when large databases are involved because a requirement for an attacker is that they should itemize the database character by character.

2. **Boolean or Content-based**

This blind SQLi technique is used by an attacker to send a SQL query to the database, forcing the application to generate a result. Depending on whether the query is true or false, varying results would be generated. Also, depending on the returned result, the content within the HTTP response is altered or remains unaffected. Afterward, the attacker can determine whether the message created is a true or false result.

5.3.3 Case study of SQL Injection

There are several SQL Injection attacks, Vulnerabilities, and procedures that occur in diverse circumstances. An attacker that wants to perform an SQL Injection exploits a standard SQL query to manipulate unauthorized data Vulnerabilities in a database. This attack vector can be executed in several ways. However, a few of the common SQL Injection examples include the following:

Retrieving hidden data: This occurs by modifying an SQL query to recover further outcomes.
UNION attacks: Here, the attacker recovers data from diverse database tables.
Subverting application logic: Here, the attacker modifies a query to compromise the application's logic.
Blind SQL Injection: In this situation, the results of a query a user controls do not return in the application's responses.
Examining the database: Here, you can remove the information regarding the structure and version of the database.
Furthermore, let's consider two database tables for this SQL Injection example, that is, Users and Contacts. The User table does not necessarily have to be extremely technical; it can be as simple as entering just three fields. This field would include the User ID, username, and password. However, the Contacts table would require more information concerning the users, including the User ID, First Name, Last Name, First Address, Email, security code, and credit card information. So, the Users table would have the login information below:

wsmith,JusticeIsHere!
jsparks,Pow3rPassword$Secur3ed
kperry,P@$$w0rd
A solid password must be primed and hashed when placed in a database. Avoid using cleartext to avoid being compromised. When you want to log in, you would have to enter your username and passwords in the login page. The information you enter is sent to the website's server, which constructs a SQL query and that query is sent to the database server. This is what the query would look like:

Select ID from Users where username='kperry' and password='P@$$w0rd'

How SQL work is that each of the rows the query requests is assessed based on a true or false comparison. Using the above example as a guide, the query suggests that, for every row where the username is kperry and the password is P@$$w0rd, we check the Users table and give back the ID value. Usually, the web site's server realizes what is sent back via the database server. With our example, the website's server would get a '1' and allow the user to go past the login page.

However, if we want to get malicious with the query, we will have to trick the server into believing that we have authentication, considering that the database server executes a true-or-false check. This can be achieved by including an OR to our password. If we login with x' or a=a as our password, a new SQL query would be created:

Select ID from Users where username='kperry' and password='x' or a=a

We would successfully bypass being kicked off because even though x is not kperry's password, the database server will automatically verify the second option. It will check the alternative if x is not kperry's password, is an equal a? Since it does, the ID will be returned to the application, and the user will have a successful authentication. Moreover, the situation does not necessarily have to be an a=a situation. Once the two values are equal, then this command would work. You can have b=b, 1=1, or even 2452=2452.

If the webpage can display data, it might be able to print other data to the screen. To obtain the data, you can try chaining two SQL requests together. Furthermore, we can add a second statement to our ' or a=a, such as UNION SELECT LastName, security code from Contacts, and credit card details. Additional clauses such as this might require more input. Nevertheless, gaining access to data is the final objective of an SQL Injection attack.

Another procedure can be adapted for blind SQL Injection, the technique where no data is returned to the screen to inject other hints. Comparable to our ' or a=a situation, we can command the server to take a nap. We could include: " ' or nap(20) " and this executes what it appears to be. This commands the database server to snooze for 20-seconds, while other responses are deferred.

5.4 Firewall:

With the increasing number of cybercrimes with every passing day, individuals and companies must secure their information. However, there are many challenges to implementing the same. A firewall is one such security device that can help you safeguard your network and device from an outsider. In this tutorial on 'what is a firewall', you will learn all you need to know about a firewall and how it acts as a shield to protect your network.

Now, let's start by understanding what firewall is

Firewalls prevent unauthorized access to networks through software or firmware. By utilizing a set of rules, the firewall examines and blocks incoming and outgoing traffic.

Fencing your property protects your house and keeps trespassers at bay; similarly, firewalls are used to secure a computer network. Firewalls are network security systems that prevent unauthorized access to a network. It can be a hardware or software unit that filters the incoming and outgoing traffic within a private network, according to a set of rules to spot and prevent cyberattacks.

Firewalls are used in enterprise and personal settings. They are a vital component of network security. Most operating systems have a basic built-in firewall. However, using a third-party firewall application provides better protection. A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

5.4.1 Concepts of Firewall

Firewalls are designed with modern security techniques that are used in a wide range of applications. In the early days of the internet, networks needed to be built with new security techniques, especially in the client-server model, a central architecture of modern computing. That's where firewalls have started to build the security for networks with varying complexities. Firewalls are known to inspect traffic and mitigate threats to the devices.

Key Uses of Firewalls

- Firewalls can be used in corporate as well as consumer settings.
- Firewalls can incorporate a security information and event management strategy (SIEM) into cybersecurity devices concerning modern organizations and are installed at the network perimeter of organizations to guard against external threats as well as insider threats.
- Firewalls can perform logging and audit functions by identifying patterns and improving rules by updating them to defend the immediate threats.
- Firewalls can be used for a home network, Digital Subscriber Line (DSL), or cable modem having static IP addresses. Firewalls can easily filter traffic and can signal the user about intrusions.
- They are also used for antivirus applications.
- When vendors discover new threats or patches, the firewalls update the rule sets to resolve the vendor issues.
- In-home devices, we can set the restrictions using Hardware/firmware firewalls.

5.4.2 Types of Firewall

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:

Packet Filtering

A packet filtering firewall controls data flow to and from a network. It allows or blocks the data transfer based on the packet's source address, the destination address of the packet, the application protocols to transfer the data, and so on.

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.

5.4.3 Working, Advantages and Importance of Firewall

How Does a Firewall Work?

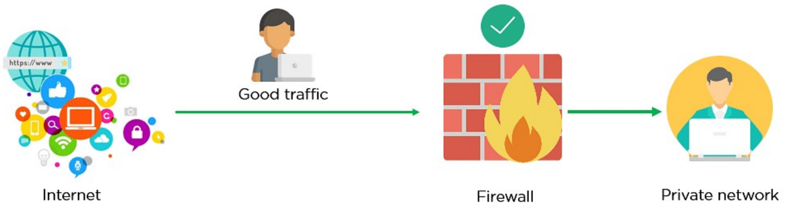
As mentioned previously, firewalls filter the network traffic within a private network. It analyses which traffic should be allowed or restricted based on a set of rules. Think of the firewall like a gatekeeper at your computer's entry point which only allows trusted sources, or IP addresses, to enter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

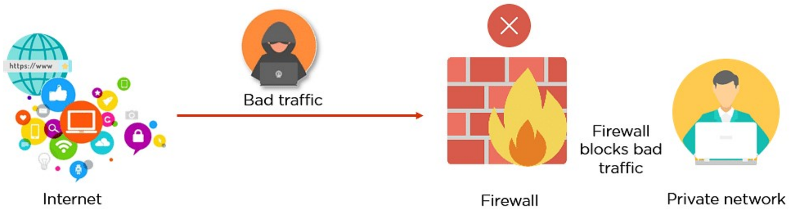
For example, the image depicted below shows how a firewall allows good traffic to pass to the user's private network.

Firewall_1.



However, in the example below, the firewall blocks malicious traffic from entering the private network, thereby protecting the user's network from being susceptible to a cyberattack.

Firewall_2.



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 Firewalls

Perhaps the strongest advantage of a firewall is that it effectively isolates your computer from external threats. According to various studies, Windows computers which did not have a firewall activated upon connecting to the internet were exposed to various forms of cyber threats within a matter of minutes. When using a firewall, network administrators can carefully select the specific ports which receive and transmit data for various operations, including web browsing, email communication, and so on. This can be immensely powerful in that it will allow you to customize your security protocols depending upon the specific situation at hand and create a tailored experience for each user on the network. Given the fact that a firewall is designed to protect a computer from unwanted intrusion, the advantages offered by this technology are priceless.

- Now that you have understood the types of firewalls, let us look at the advantages of using firewalls.
- 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.