

Name: Cheerala Rohith
Project Name: STREET'S KITCHEN

Introduction

Streets kitchen is a eatery project build on HTML, JAVASCRIPT, CSS. This project is involved with building a flexible, open-ended design for eatery management system that integrates well-known design patterns and a coherent design style using UML diagrams. Our eatery Management System consists of two users customers and admin.

SCOPE AND OBJECTIVES

Focus of this project is to develop an web application which offers course of action to the diner owners to flourish their business by moving menus at no cost and will always provoke higher customer support and obtainment rates.

Specific Requirements:

Equipment AND SOFTWARE REQUIREMENTS

Equipment Requirement:

- Hardware - Pentium
- Speed - 1.1 GHz
- RAM - 2GB
- Hard Disk - 2 GB
- Keyboard - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

Software Requirements:

- Operating System : Windows / Linux / Mac
- Technology : Visual studio.
- Web Technologies : Html, JavaScript, CSS
- IDE : Notepad++
- Web Server : WAMP / XAMPP / LAMP / MAMP (anyone)

Software Used

HTML:

By definition, HTML is a uniform, text-based markup language. It consists of simple markup elements, the so-called "tags", as well as empty elements such as `
`. HTML is an abbreviation for "Hypertext Markup Language". It enables browsers to interpret, display and link web pages. In the current standard, XHTML and HTML 5 are used to create search engine-optimized and user-oriented websites with all the necessary elements. The responsive design and various awards within the code are also relevant for search engine ranking.

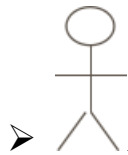
CSS: The real benefit of cascading style sheets is only apparent when you look at larger websites. The cascading effect of CSS can help here, because it becomes possible to outsource a style sheet. Style sheets can be imported to incorporate into another document. This procedure is the basis for the cascading style sheets. Looking at the style sheet hierarchy, there is a core style sheet at the top. In this, basic things such as font, background and text colors, etc. are defined. The core style sheet applies to all subsequent style sheets. All subordinate style sheets can import content from the core style sheet and expand it with format instructions such as a table or instructions for displaying color-coded product names. Theoretically, this chain can be continued indefinitely, with every change in a style sheet "rubs off" on all subsequent style sheets, which represents an increase in effectiveness.

JAVA SCRIPT: JavaScript is a scripting/programming language that allow you to implement intricate feature on web pages every time a web page does more than just sit there and display static info for you to look at showing timely content informs, interactive-maps, animated 2D or 3D graphics, scrolling-video juke-boxes, many more. It is the third layer of the layer cake of standard web technologies, two of which (HTML and CSS) we have covered in much more detail in above.

Visual Studio: Microsoft Visual Studio is an integrated development environment from Microsoft. It is used to develop computer programs, as well as websites, web apps, web services and mobile apps.

UML DIAGRAMS:

Entertainer:



- A contemplated set of jobs that clients of utilization cases play while communicating with the utilization cases.

USE CASE:

A depiction of activities, including variations that a framework plays out that yields a visual aftereffect of estimation of an on-screen character.

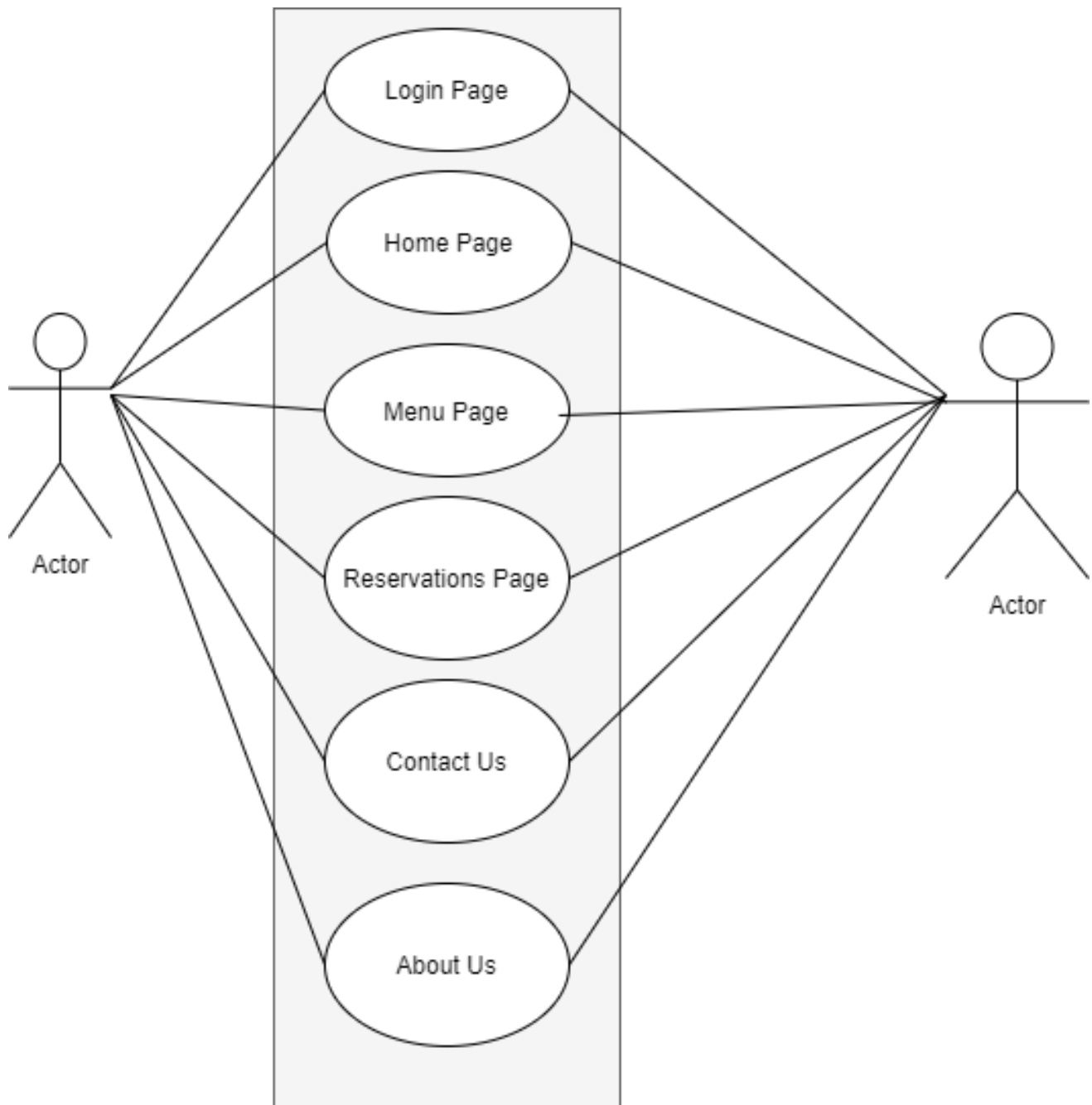


- UML speaks to Unified Modelling Language. UML is a language for deciding, envisioning, and revealing the system. This is the movement while developing anything after assessment. This goal is to model the substances related to the endeavor that later ought to be created. The depiction of the components to be used in the thing being made ought to be arranged.

USE CASE DIAGRAMS:

- Use case plots model lead inside a structure and empowers the planners to understand of what the customer requires. The stick man addresses what's called a performer.
- Use case diagram can be useful for getting a general viewpoint on the structure and clarifying who can do and even more essentially what they can't do.

- Use case chart includes usage cases and on-screen characters and shows the participation between the use case and performers.
- The configuration is to show the relationship between the use case and performer.
- To address the structure essentials from customer's perspective.
- An on-screen character could be the end-customer of the system or an external

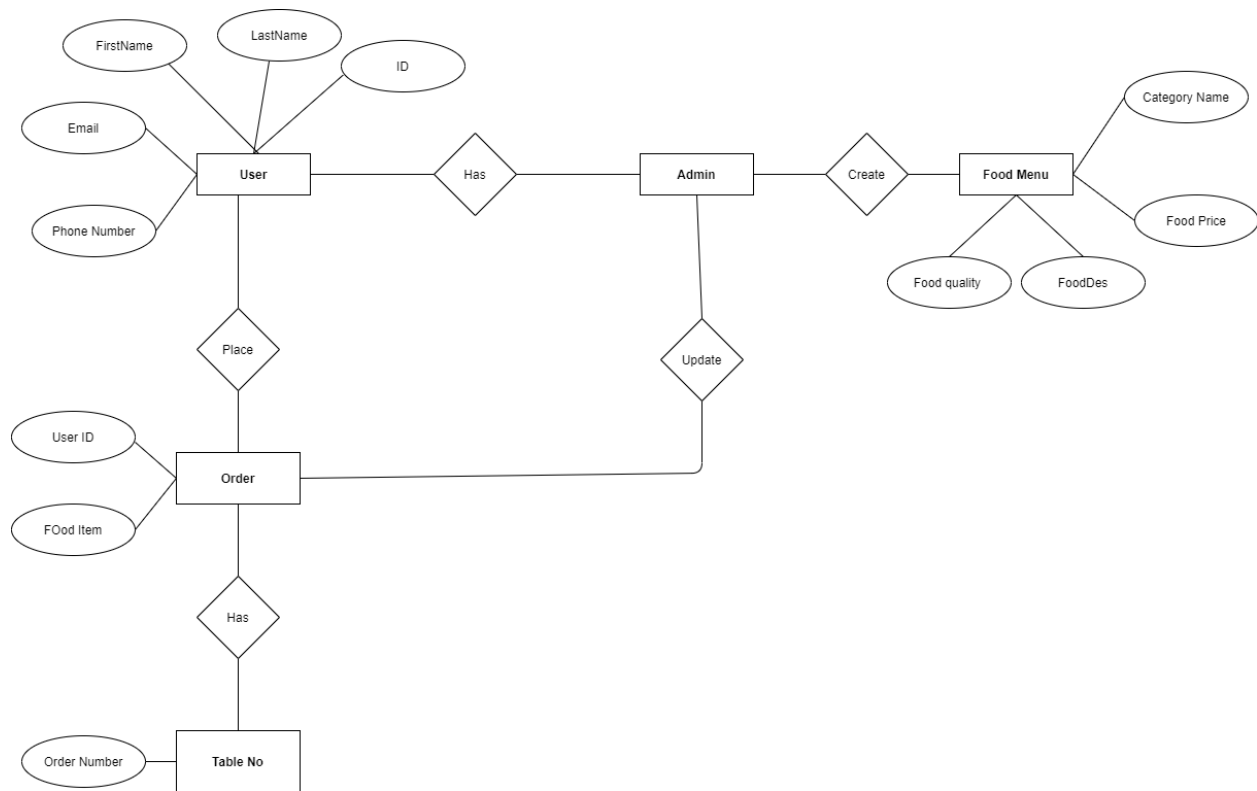


➤

E-R DIAGRAMS :-

The Entity-Relationship (ER) model was initially proposed by Peter in 1976 as a manner to bring together the system and social database sees. Just expressed the ER model is a calculated information model that perspectives this present reality as elements and connections. A fundamental segment of the model is the Entity-Relationship outline which is utilized to outwardly speaks to information objects. Since he composed his paper the model has been expanded and today it is normally utilized for database plan for the database fashioner, the utility of the ER model is:

- It maps well to the social model.
- It is basic and straightforward with at least preparing. In this manner, the model can be utilized by the database architect to correspondence.
- In expansion, the model can be utilized as a structure plan by the database engineer to actualize an information model in a particular database the executives programming.

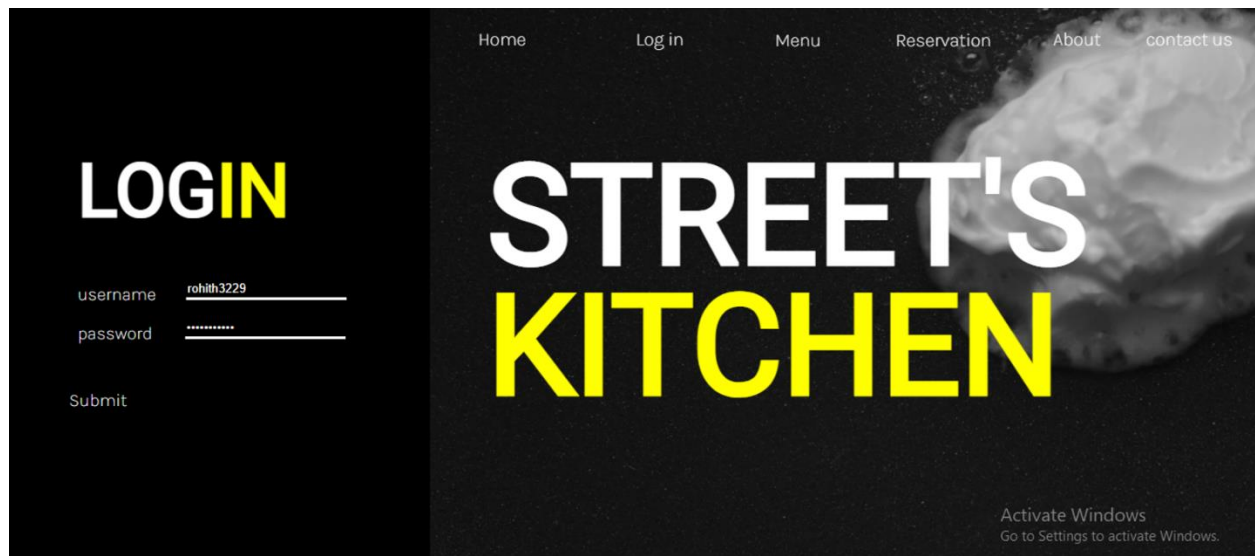


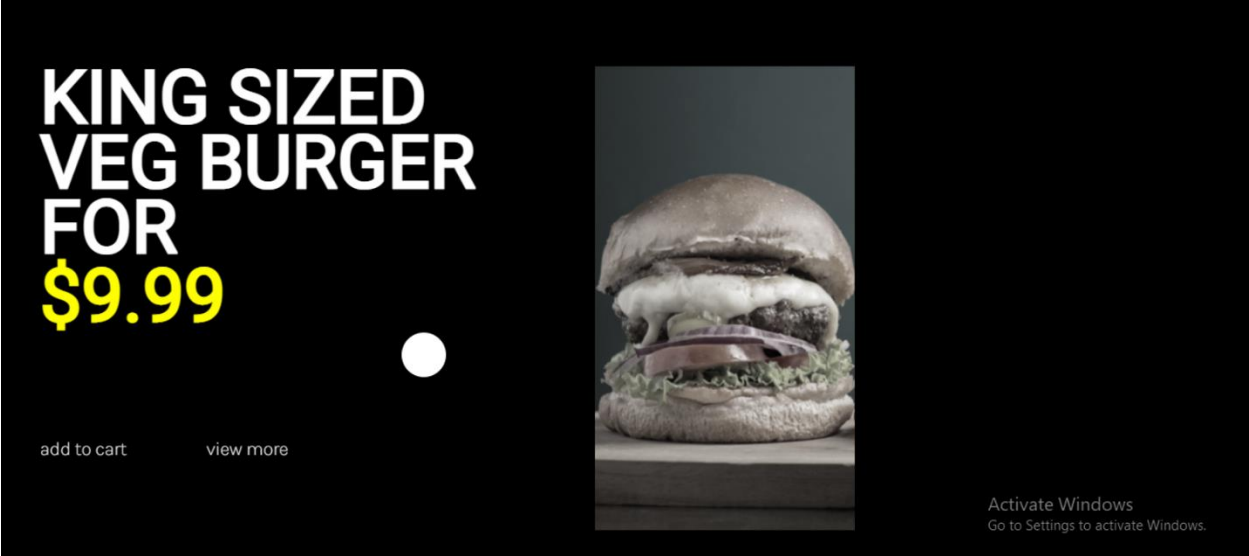
NETWORK AND CARDINALITY :-

- The essential sorts of network for relations are coordinated, one-to-many, and many-to-many. A balanced (1:1) relationship is when at most one occurrence of a substance A is related with one occasion of element B. For instance, "workers in the organization are each doled out their very own office. For every worker there exists a one of a kind offices and for every office there exists a one of a kind representative.
- A one-to-many (1: N) connections is when for one occurrence of element A, there are zero, one, or numerous examples of substance B, however for one occasion of element B, there is just one case of element A. A case of a 1: N connections is

- a office has numerous workers every representative is allocated to one division
- A many-to-many (M: N) relationship, now and then called vague, is when for one occurrence of substance A, there are zero, one, or numerous examples of element and for one occasion of element B there are zero, one, or numerous cases of element A. The availability of a relationship portrays the mapping of related

Output






desserts

noodles

pasta


seafood

beverages




add to cart

\$9.99




add to cart

\$14.99




add to cart

\$19.99




add to cart

\$11.99



\$9.99



add to cart

\$16.99

Activate Windows

Go to Settings to activate Windows.

OUR MENU


desserts

noodles

pasta


seafood

beverages




add to cart

\$9.99




add to cart

\$14.99



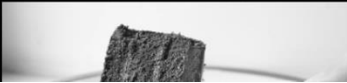
add to cart

\$19.99




add to cart

\$11.99



\$9.99

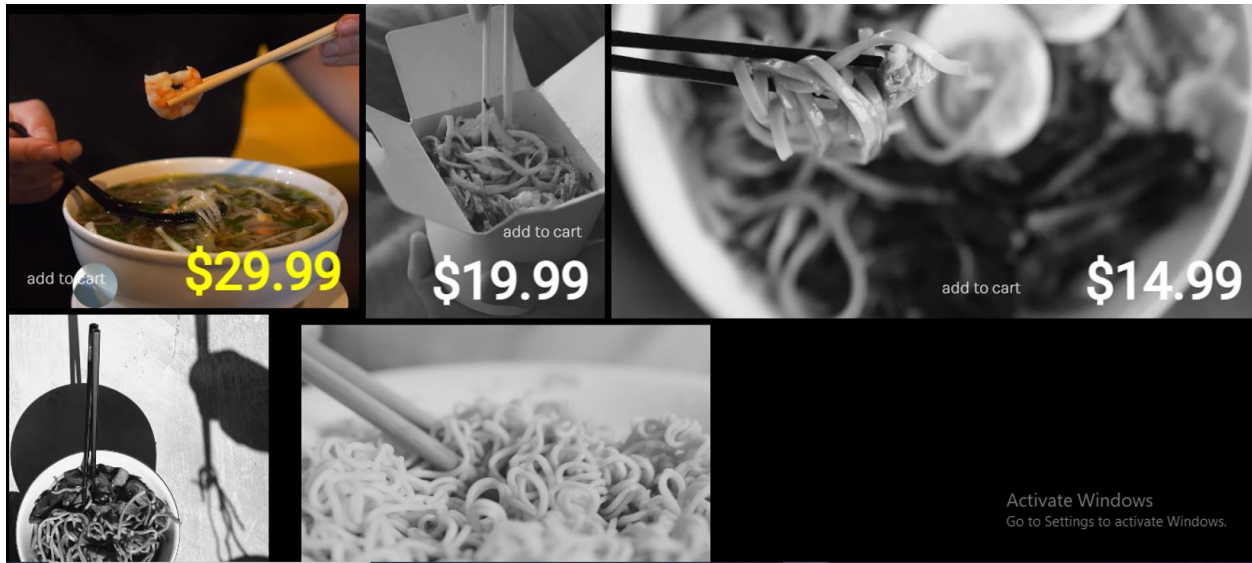


add to cart

\$16.99

Activate Windows

Go to Settings to activate Windows.



MAKE RESERVATIONS

call us leave a message

Home Log in Menu Reservation About contact us

CONTACTUS

Street's Kitchen India,
Tower-999, Plot No. 5,
1st Floor, Logic Techno Park,
Road 127, Bangalore - 560023, KA.
Phone 0123-211121

STREET'S KITCHEN

ATTACKS ON THE LOCAL HOST NETWORK.

DENIAL OF SERVICE (DOS): -

- Service Denial (DoS) is a digital assault on a PC or site planned to refuse any assistance to proposed clients. Their motivation is to upset the network activities of an association by denying access to their clients. Forswearing of administration is usually performed by overpowering the focused-on gadget or resource with abundance solicitations to overpower frameworks and stop a few or the entirety of the legal.
- For the model, if a bank site can deal with 10 individuals every second by tapping the Login button, the aggressor must send only 10 phony solicitations for each second so no real clients can sign in.
- The Ping of Death is the most mainstream DoS method. The Ping of Death assault works by making and sending extraordinary network messages (explicitly, non-standard size ICMP bundles) that reason issues for accepting frameworks. This assault could make powerless Internet servers crash quickly in the beginning of the Web.

POSSIABILITY OF DOS ATTACKS INVOLVE:

- Flooding a network with pointless movement as to avoid certifiable traffic. The assaults on TCP/IP SYN and smurf are two normal models.
- wireless over-burdening the CPU of a framework to anticipate the treatment of authentic solicitations.

- Switch authorizations or break get to the rationale to keep clients from signing into a program. One regular model is to trigger a fast arrangement of phony login endeavors to bolt out records from signing in.
- Remove or meddle with specific basic applications or administrations to dodge typical activity (regardless of whether the procedure and network are operational when all is said and done).
- Smurf assault is another variation of the DoS. This incorporates programmed reactions to messages. In the event that somebody sends several email messages to many individuals in an association with an autoresponder in their email with a bogus return email address, the first sent messages could transform into thousands sent to the phony email address. On the off chance that somebody belongs to that phony email address, this can occur

DOS ATTACKS CAN CAUSE THE FOLLOWING PROBLEMS:

- Ineffective services
- Inaccessible services
- Interruption of network traffic
- Connection interference

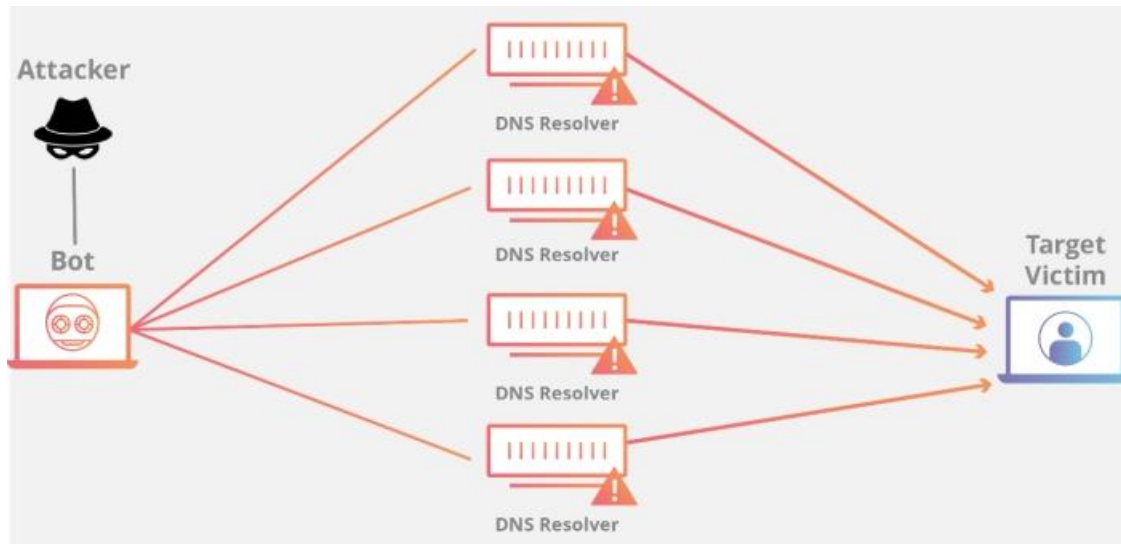


Figure: -3.1 Denial of Service (DOS).

COUNTERACTIVE ACTION FOR DOS ATTACK

In perspective on the expanding recurrence of Denial of Service (DoS) assaults, it's an extraordinary time to survey the basics and how we can battle back.

CLOUDMITIGATION PROVIDER: -

- Cloud assurance merchants are authorities in conveying cloud-based DDoS moderation. This implies they've developed monstrous measures of network transfer speed and DDoS moderation assets at numerous Internet locales that can take on any type of network traffic, regardless of whether you're utilizing different ISPs, your own server farm, or any number of cloud suppliers. The street can be scoured for you and just send "clean" server farm traffic.

FIREWALL : -

- This is the strategy that is most straightforward and least compelling. As a rule, somebody keeps in touch with some Python contents that endeavor to sift through awful traffic or an organization will attempt to utilize its current firewalls to square traffic

NET SERVICE PROVIDER (ISP): -

- many organizations are utilizing their ISP to moderate DDoS. These ISPs have more transfer speed than an organization would have, which can help with the huge volumetric assaults
- To keep away from such assaults, you should utilize secure coding and construct solid design to avoid such assaults and update your site's customary answer for bug.

DISTRIBUTED DENIAL OF SERVICE (DDOS): -

- Imagine a situation where you visit a few sites and one of them will in general be somewhat moderate. You may censure their servers for improving their adaptability since they may get a great deal of client traffic on their page. A few locales as of now mull over this issue ahead of time. Odds are, they could be an objective of the supposed DDoS assault, Distributed Denial of Service Attack. Allude – Service and Prevention Denial.
- In DDoS assault, by managing constant and gigantic traffic from a few end frameworks, the aggressor attempts to make a specific assistance out of reach. In light of this monstrous traffic, the assets of network are utilized to help the requirements of these bogus end frameworks with the goal that an authentic customer can't utilize the assets for himself.

SORTS OF DDOS ATTACKS:

There are numerous sorts of DDoS assaults. Basic assaults incorporate the accompanying:

- Traffic attacks: traffic flooding assaults give the objective a tremendous volume of parcels from TCP, UDP and ICPM. Real demands are lost, and malware abuse can go with these assaults.
- Bandwidth assaults: With huge measures of garbage information, this DDos assault overburdens the objective. This outcomes in an absence of data transmission and assets for network hardware and may prompt a total disavowal of administration.
- Application assaults: Application-layer information messages in the application layer that exhaust assets, making framework administrations of the objective inaccessible.

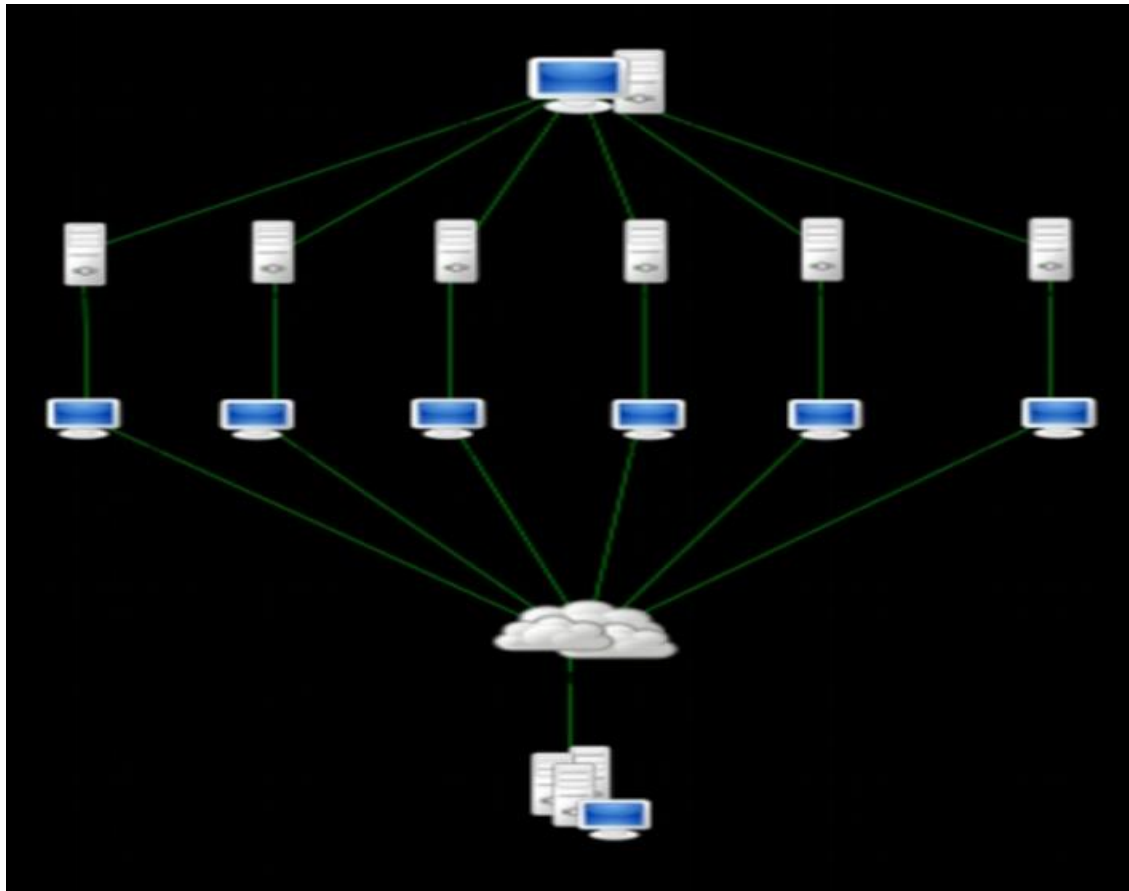


Figure: -3.2 Distributed Denial of Service (DDoS).

ANTICIPATION FOR DDOS ATTACK:

1. PURCHASE MORE BANDWIDTH: -

- The most important thing you can take to make your "DDoS" organize resistant is to ensure you have enough data transfer capacity to oversee traffic spikes that can be activated by pernicious development.
- In previously, it was possible to avoid DDoS attacks by guaranteeing that you had a bigger number of information move limit open than any aggressor may have. In any case, this is never again reasonable with the development in improvement attacks. Or maybe, buying more transmission limit by and by expands present desires that attackers need to overcome

before they can dispatch a powerful DDoS ambush anyway without any other individual, purchasing more information move limit isn't a DDoS attack game plan.

2. REDUNDANCY INTO YOUR INFRASTRUCTURE: -

- To Make sure that you spread them over numerous server farms with a decent burden adjusting framework to circulate traffic between them to make it as hard as feasible for an assailant to effectively dispatch a DDoS assault against your servers. Such server farms must be in various nations, or if nothing else in various areas of a similar nation, if conceivable.
- To be genuinely successful, it is important to guarantee that server farms are associated with different networks and that there are no clear network bottlenecks or single disappointment focuses on these networks.
- Distributing the cuts off geologically and geographically would make it hard for an aggressor to target in excess of a segment of your servers adequately, leaving different servers immaculate and ready to take on probably a portion of the additional traffic that would typically be taken care of by the influenced servers.

3. DESIGN YOUR NETWORK HARDWARE AGAINST DDOS ATTACKS :-

- There are various straightforward enhancements to equipment setup that you can take to help anticipate an assault on DDoS.
- For model, setting up your firewall or switch to drop approaching ICMP bundles or blocking DNS reactions from outside your network (by blocking UDP port 53) can help avert some volumetric assaults on DNS and ping based.

PHISHING ATTACK: -

- Phishing is a kind of assault that is regularly used to take client information, including login certifications and Mastercard numbers. It happens when an assailant hoodwinks an objective into opening an email, text, or instant message, taking on the arrival of a confided in element. The beneficiary is then fooled into clicking a malevolent connection that can result in malware establishment, framework solidifying as a major aspect of a ransomware assault, or delicate data uncovering.
- An assault can bring about pulverizing results. This incorporates unapproved purchasing, taking assets, or distinguishing robbery for people.
- In expansion, phishing is regularly utilized as a major aspect of a bigger assault, for example, a progressed diligent danger (APT) occasion, to increase and a dependable balance in corporate or administrative networks. Representatives are undermined in this last situation so as to sidestep security edges, spread malware inside a shut domain, or get special access to ensured information.
- An association that surrenders to such an assault commonly has extreme money related misfortunes notwithstanding declining piece of the pie, notoriety, and customer certainty. Contingent upon the extension, a phishing endeavour could grow into a security occurrence that makes it hard for a business to recoup.

PHISHING ATTACK EXAMPLES:

The following illustrates a common phishing scam attempt:

- Mass-circulated to however many staff individuals as could reasonably be expected is a ridiculed email supposedly from myuniversity.edu.

- The email says the secret word of the client will terminate. Guidelines are given to go to myuniversity.edu/recharging inside 24 hours to refresh your code.

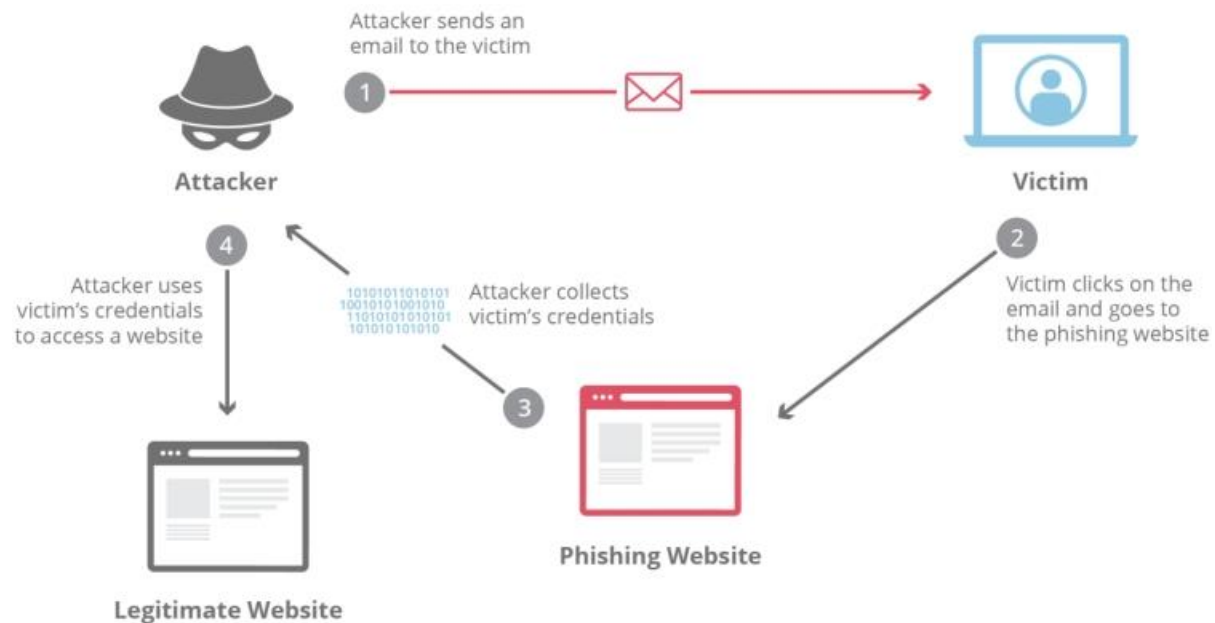


Figure: -3.3 Using Spoofing for Phishing Attack.

HERE ARE A FEW STEPS TO PROTECT ITSELF AGAINST PHISHING:

- Educate the staff and complete recreated phishing situations practice sessions.
- Use a SPAM channel to follow malware, void senders, etc.
- Hold the latest security fixes and invigorates on all stages.
- Install an antivirus game plan, plan signature updates and screen all devices for antivirus status.

- Create a security game plan that incorporates yet isn't compelled to expiry and intricacy of the code.
- To square toxic destinations, present a web firewall.
- Encrypt every single fragile datum about the association.
- Convert simply email messages from HTML to content or weaken HTML email messages.
- Require affirmation for telecommuting workers.
- Multiple steps can be taken by an organization to secure against phishing. They have to keep up a heartbeat on current phishing systems and affirm their security approaches, and as they advance, they can dispense with dangers.
- It is similarly essential to guarantee that their workers comprehend the kinds of assaults they face, the dangers they face, and how to manage them. Key to shielding your organization from phishing assaults are educated representatives and appropriately verified frameworks.

SESSION HIJACKING: -

- The Hijacking Session assault comprises of abusing the control system of the web session, which is typically overseen for a session token.
- When http correspondence utilizes a wide range of TCP associations, a system is required for the web server to perceive the associations of every client. After fruitful customer

verification, the most valuable strategy relies upon a token that the Web Server sends to the customer program. A session token typically comprises of a variable width string and can be utilized in different ways, for example, in the URL. In the http demand header as a treat, in different pieces of the http demand header, or in the http demand body.

- The Session Hijacking assault endangers the session token by taking or foreseeing a legitimate session token to increase unapproved Web Server get to.

The session token could be undermined in various manners; the most widely recognized are:

- Predictable session token
- Session Sniffing
- Client-side assaults (XSS, malignant JavaScript Codes, Trojans, and so forth)
- Man-in-the-middle assault
- Man-in-the-middle assault

Example 1:

SESSION SNIFFING:

- The commandeering of a TCP session is a security assault on a client session over an ensured network. The most well-known technique for session seizing is called IP satirizing when an aggressor utilizes source-steered IP parcels to embed directions into a functioning correspondence on a network between double hubs and mask themselves as one of the

verified clients. This kind of assault is conceivable because of confirmation Normally it is performed distinctly toward the start of a TCP session.

- Another type of session commandeering is known as a man-in - the-middle assault where the assailant can follow the collaboration between gadgets utilizing a sniffer and catch the transmitted data.
- As we find in the model, the assailant first uses a sniffer to get a bona fide token session called "Session ID" and a brief span later uses the critical token session to augment unapproved access to the Web Server.

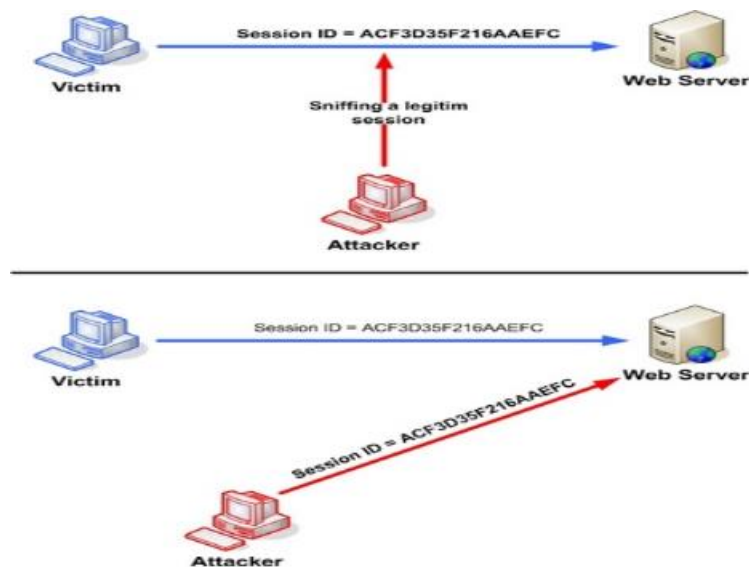


Figure: -3.4 Using Packet for Session Sniffing.

Example 2:

CROSS-SITE SCRIPT ATTACK:

- By utilizing noxious code or projects running on the customer side, the aggressor may bargain the session token. The model tells the best way to utilize a XSS assault to take the session token from the aggressor.
- In the event that an aggressor sends the noxious JavaScript with a created connection to the objective, the JavaScript will run and finish the assailant's guidelines when the objective taps on the link. The model in Figure 3.5 uses a XSS assault to show the treat estimation of the present session; an alternate JavaScript code can be produced utilizing a similar procedure to convey the treat to the aggressor.

<SCRIPT>alert(document.cookie);</SCRIPT>

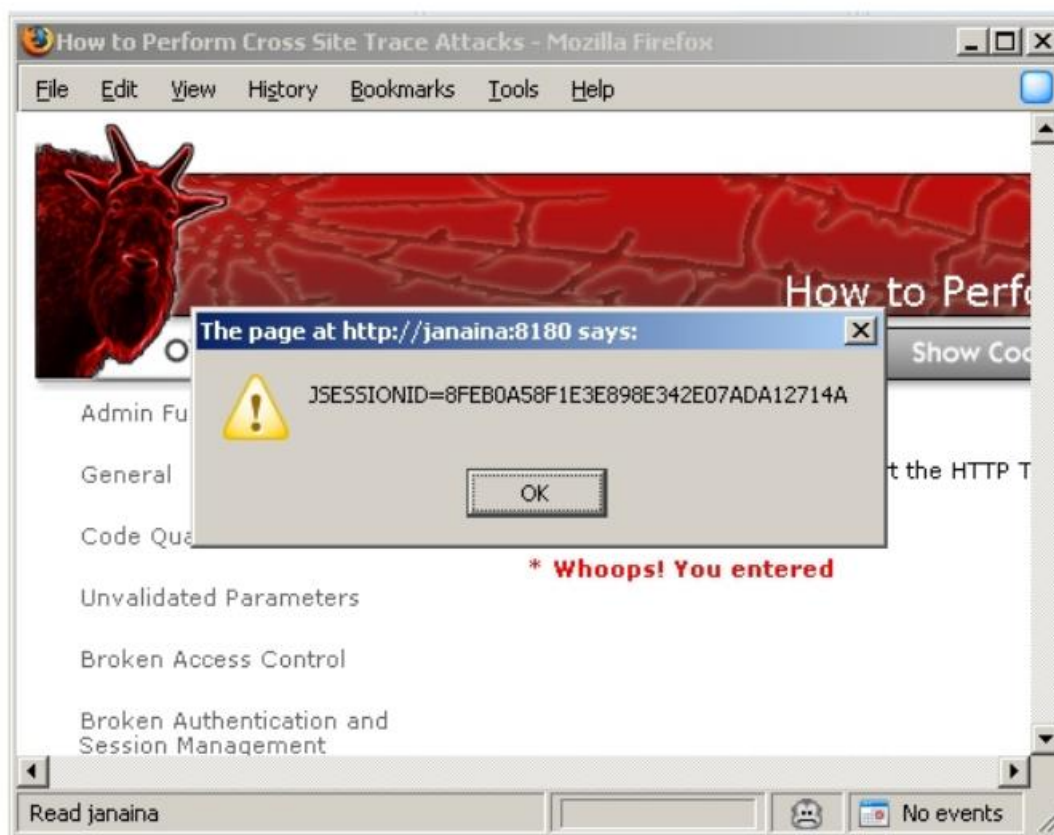


Figure: -3.5 Cross-site script attack.

COUNTERACTING THE SESSION HIJACKING: -

- As we have seen previously, the methodology regularly used to take the session ID is to download a noxious code on the organization site and afterward take the treat. Empowering security from the customer side is the most ideal approach to counteract session capturing. It is suggested that preventive measures be taken on the customer side for the session commandeering. Clients need an antivirus, hostile to malware performance Applications and the applications must be state-of-the-art.
- Engines were utilized to stand-out engraving all session demands. In spite of following the IP address and SSL session ID, the motors in like way screen the http headers. - Header change adds discipline focuses to the session and the session closes once the focuses have arrived at a specific total. This breaking point can be balanced. This is effective in light of the fact that there will be an impedance, it will have another http header
- These are the proposed preventive measures to be taken by both the client and server sides to avoid the catching ambush of the session.

MAN IN THE MIDDLE ATTACK (MITM): -

- Not to be mistaken for an assault from Meet-in - the-Middle.
- A man-in - the-middle assault (MITM) in cryptography and PC security is an assault wherein the assailant covertly transfers and likely changes messages between double gatherings that think they discuss straightforwardly with one another. A case of a MITM assault is forceful listening in, in which the aggressor speaks with the objectives autonomously and transfers messages between the targets to cause them to accept that they are conversing with one another legitimately through a private association, when the

assailant really controls the whole discussion. The aggressor must have the option to block and infuse new messages that move between the double targets. As a rule, this is clear; for instance, an interloper in the banquet room of a decoded remote purpose of access (Wi-Fi) could be embedded as a man in the middle.

- Since it is proposed to bypass common confirmation, a MITM assault can possibly succeed if the assailant imitates every endpoint all around ok to satisfy their desires. Most cryptographic conventions explicitly contain some type of endpoint confirmation to avoid MITM assaults. For instance, TLS can utilize a commonly confided in endorsement power to verify one or the two gatherings.

KEY CONCEPTS OF A MAN-IN-THE-MIDDLE ATTACK:

- Man-in - the-center is a sort of spying ambush that happens when a threatening performer places himself in a correspondence session between people or structures as a hand-off/middle person.
- A MITM attack misuses consistent trade planning, correspondence or other data move.
- Man-in - the-center ambushes empower attackers to get, send and get information that is never intended to be for them until it's past the final turning point.

MAN-IN-THE-MIDDLE ATTACK EXAMPLES:

- You will find in the picture over that the aggressor inserted him/herself between the movement of client server traffic. Since the attacker has hindered into the twofold

endpoints correspondence, he/she can mix counterfeit information and square the moved data between them.

- Below is another instance of what could happen once he/she has installed the man in the centre.

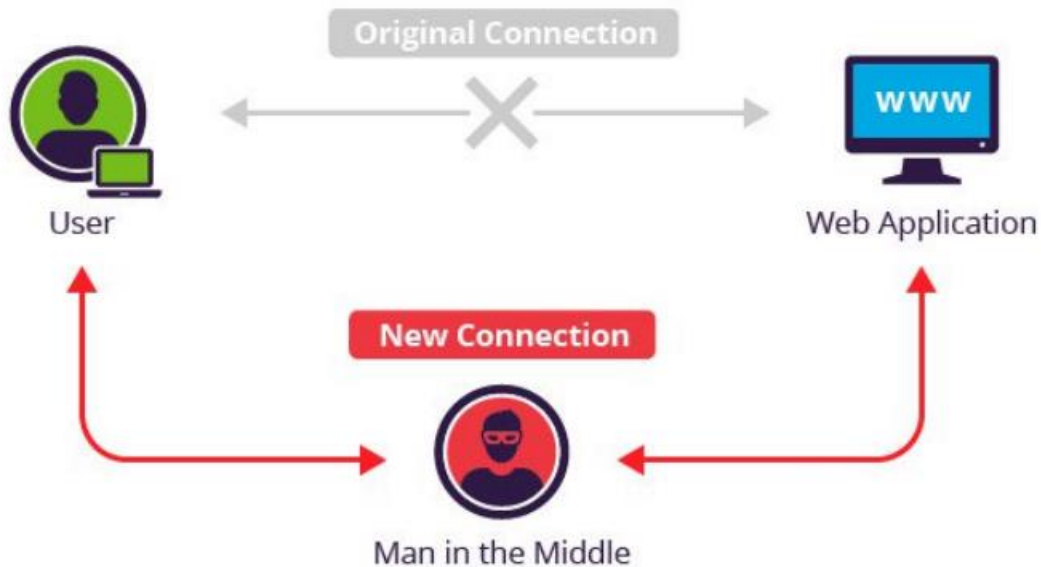


Figure: -3.6 Man in the middle attack (MITM).

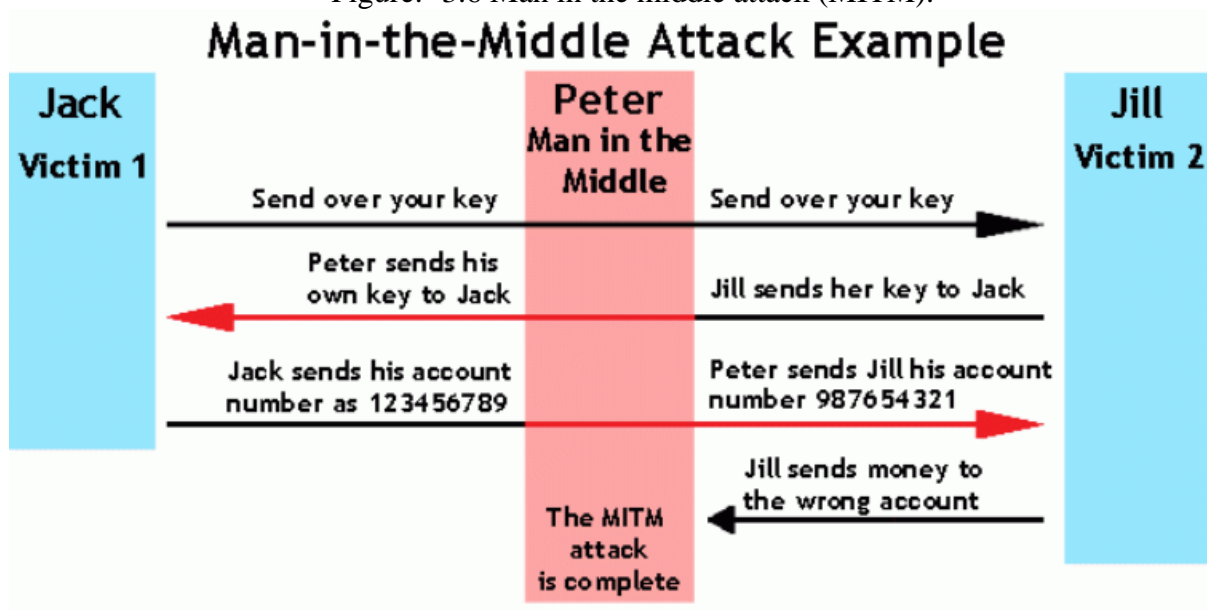


Figure: -3.7 Man in the middle attack (MITM).

- To access reserves, the programmer mimics all sides of the discussion. This model is valid for a customer and server discussion just as individual-to-individual discussions. The assailant catches an open key in the above model, and with that, he can transpose his very own accreditations to fool individuals into accepting that they are talking safely to one another.

BEST PRACTICES TO PREVENT MAN-IN-THE-MIDDLE ATTACKS: -

Strong WEP/WAP ENCRYPTION ON ACCESS POINTS: -

- Having a strong encryption framework on remote entries checks bothersome customers basically being close by from joining your system.
- A delicate encryption instrument can savage power an aggressor into a system and start man-in - the-middle ambush. The more grounded the execution of encryption, the more secure.

SOLID ROUTER LOGIN CREDENTIALS: -

- Making sure that your default switch login is changed is basic. Your secret word for Wi-Fi, however your qualifications for switch login. On the off chance that your switch login certifications are found by an assailant, your DNS servers can be changed to their pernicious servers. Or then again more regrettable yet, contaminate your switch with malware

POWER HTTPS: -

- Using open private key exchange, HTTPS can be used to confer securely over HTTP. It keeps a gate crasher from using the information that he can smell. Locales must use HTTPS just and not offer alternatives rather than HTTP. Customers can for the most part acquaint program modules with approve HTTPS on request .

OPEN KEY PAIR BASED AUTHENTICATION: -

- Usually man-in - the-center attacks fuse caricaturing something or something else. Open key pair-based encryption, for instance, RSA can be used in various stack layers to help ensure that the things you talk with are the things you have to talk with.