18/02/2025

What is the Internet?

The **Internet** is a giant network that connects computers, phones, and other devices worldwide. It helps us send messages, watch videos, browse websites, and more.

How Does It Work?

Step 1: Your Device Connects to the Internet

- You use **Wi-Fi**, **mobile data**, or a **cable** to connect to the internet.
- This connection is provided by an **Internet Service Provider (ISP)** like Jio, Airtel, or BSNL.

Step 2: Asking for Information (Request)

- When you type a website like www.google.com, your device **asks** a special computer (called a **server**) for that website's data.
- This request is sent as tiny pieces of data called **packets**.

Step 3: Finding the Website (DNS & IP Address)

- Computers don't understand names like google.com; they understand numbers called **IP addresses** (e.g., 142.250.190.46).
- A system called **DNS (Domain Name System)** translates website names into IP addresses, like a phonebook matching names to phone numbers.

Step 4: Sending the Data Back (Response)

- The server hosting the website finds the requested page and sends it back to your device in **packets**.
- Your device **reassembles** these packets to display the website.

Step 5: You See the Website!

- Your browser (Chrome, Firefox, etc.) puts everything together and shows the website as you expect.

What is TCP/IP?

TCP/IP (Transmission Control Protocol / Internet Protocol) is the foundation of how the internet works. It is a set of rules (protocols) that allow computers and devices to communicate over the internet.

1. IP (Internet Protocol) – The Address System

- Think of **IP** like a home address. Every device on the internet has a unique **IP address** (e.g., 192.168.1.1).
- It helps **identify where data should be sent** and ensures it reaches the correct destination.

2. TCP (Transmission Control Protocol) – The Delivery System

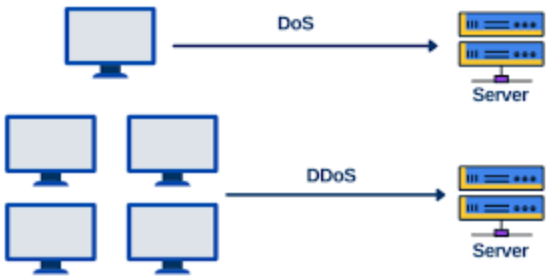
- Think of **TCP** like a **delivery truck** that ensures data is sent, received, and reassembled correctly.
- It **breaks data into small packets**, sends them, and ensures they arrive **in the correct order** without errors.

How TCP/IP Works Together

- **Step 1:** You request a webpage (e.g., google.com).
- **Step 2:** TCP **breaks** the webpage data into small packets.
- **Step 3:** IP **routes** these packets across the internet.
- **Step 4:** TCP **reassembles** the packets when they reach your device.
- **Step 5:** The webpage appears on your screen!

Denial of Service (DoS) Attack

A **Denial of Service (DoS) attack** is an attempt to make a computer, network, or service unavailable to its intended users by overwhelming it with a flood of traffic or requests. The goal is to **disrupt** normal service, making it slow or completely inaccessible.



How Does It Work?

In a typical DoS attack, the attacker:

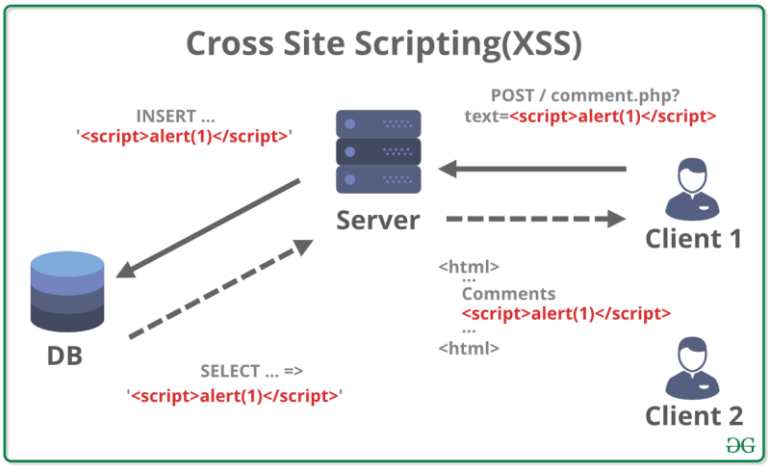
1. **Floods the server or network** with an overwhelming amount of traffic.
2. **Consumes all resources** (e.g., memory, processing power, bandwidth) so that the target cannot respond to legitimate users.
3. **Crashes or slows down the system**, preventing users from accessing the website or service.

Cross Site Scripting

Cross-Site Scripting (XSS) is a type of **security vulnerability** found in web applications where an attacker injects malicious scripts (usually JavaScript) into webpages viewed by other users. The malicious script runs in the context of the victim's browser, allowing the attacker to steal sensitive information, hijack accounts, or perform actions on behalf of the user.

How Does XSS Work?

1. **Injection**: The attacker injects malicious code (usually JavaScript) into a web page, typically through input fields like search boxes, comment sections, or URL parameters.
2. **Execution**: When a victim visits the page, the browser **executes** the injected script as if it were part of the legitimate webpage.
3. **Impact**: The script can steal cookies, session tokens, or redirect the user to malicious websites.



Types of XSS Attacks

1. Stored XSS (Persistent XSS)

- The attacker injects the malicious script into a **server-side resource**, like a database, which is then served to all users who access the page.
- Example: Posting a malicious comment on a blog. Anyone who views the comment will have the script executed in their browser.

2. Reflected XSS (Non-Persistent XSS)

- The attacker injects a script through a **URL** or a request, and it is immediately reflected back by the web server.
- Example: Sending a malicious link to someone, and when they click it, the script runs in their browser.

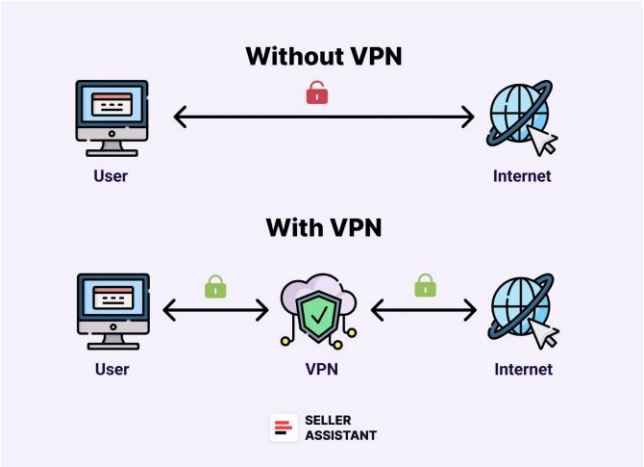
3. DOM-based XSS

- The attack occurs entirely within the **browser's Document Object Model (DOM)**, where the malicious script manipulates the page after it has been loaded.
- Example: An attacker manipulates a URL fragment (#) or other client-side inputs to execute malicious JavaScript.

VPN:

A **VPN (Virtual Private Network)** is a tool that helps you stay **private and secure** while using the internet. It creates a **safe, encrypted connection** between your device (like a phone or

computer) and the internet, even when you're using a public or untrusted network (like public Wi-Fi).



How Does It Work?

1. **Encryption**: When you connect to a VPN, it **encrypts** (locks) your internet data, so no one can see what you're doing online (like hackers or your internet provider).
2. **Masking Your Location**: The VPN connects to a **remote server** in a different location, which makes it seem like you are browsing the internet from that location instead of your actual one.
3. **Secure Connection**: All your internet traffic is routed through this secure server, protecting your data from being stolen or spied on.

What Does a VPN Do?

- **Protects Your Privacy**: It hides your real IP address, making it harder for websites or hackers to track you.
- **Keeps Your Data Safe**: It prevents others (like hackers on public Wi-Fi) from seeing your personal information, passwords, or credit card details.
- **Bypasses Geo-Restrictions**: It can make it look like you're browsing from another country, allowing you to access websites and services that might be blocked in your country.
- **Helps with Online Security**: It protects you when using unsecured networks (like public Wi-Fi in cafes or airports).

Example

Imagine you're browsing on public Wi-Fi at a coffee shop. Without a VPN, someone could intercept your data and steal it. But with a VPN, your data is encrypted, and it's much safer from anyone trying to snoop on your activities.

In simple terms, a **VPN is like a secure tunnel** that protects your internet connection from hackers and helps you stay anonymous online.

IP Address

An IP address is like a home address for your device on the internet or a local network. But, there are two types of IP addresses: public and private.

Feature	Public IP Address	Private IP Address
Scope	Used on the internet	Used within a local network
Assigned by	Internet Service Provider (ISP)	Router or Network Administrator
Uniqueness	Must be unique across the internet	Can be used by multiple devices in different local networks
Visibility	Visible to the outside world	Not visible to the outside world

1. HTTP (Hypertext Transfer Protocol)

- **What it is**: HTTP is the basic protocol (set of rules) used for transferring data over the **web**. When you visit a website, your browser uses HTTP to request and receive data from the web server.
- **How it works**: HTTP sends data in **plain text**, meaning it’s not encrypted, and anyone can **intercept** and read the data sent between your device and the server.

Example: When you visit a website like http://example.com, your browser uses HTTP to get the content of that site.

2. HTTPS (Hypertext Transfer Protocol Secure)

- **What it is**: HTTPS is an **enhanced version** of HTTP that **adds security** by encrypting the data exchanged between your browser and the website server.
- **How it works**: HTTPS uses **SSL/TLS encryption** to protect data during transmission, preventing eavesdropping and tampering.

Example: Websites that use HTTPS (like https://example.com) show a padlock icon in the browser, indicating the connection is secure.

3. SSL (Secure Sockets Layer)

- **What it is**: SSL is an older **security protocol** that was originally used to establish secure connections between a browser and a web server. It uses **encryption** to keep data private.
- **How it works**: SSL was designed to create a secure, encrypted connection over the internet. However, SSL is now considered **obsolete** and has been replaced by TLS, though you might still hear people refer to "SSL" for secure connections.

Note: Websites that use SSL certificates still show the padlock icon in browsers, but they now use **TLS**.

4. TLS (Transport Layer Security)

- **What it is**: TLS is the modern, more secure version of SSL. It's the **protocol** that actually provides encryption and secure data transmission over the internet today.
- **How it works**: TLS ensures that the communication between your browser and the website is **private** and **secure** by encrypting the data. It also provides authentication, ensuring that the server you are connecting to is the one it claims to be.

Example: When you visit a site with HTTPS, it's actually using **TLS** encryption behind the scenes.

Basic Email Process:

When you send an email, it involves several steps and different servers to make sure it reaches the recipient.

1. Composing the Email:

- You start by writing an email on your device (phone, computer) using an **email client** (like Gmail, Outlook, or Apple Mail).

2. Sending the Email:

- When you click **send**, your email client connects to an **SMTP server** (Simple Mail Transfer Protocol).

- **SMTP** is a protocol used to send emails. It works as a mail "postman" that delivers your email to the recipient's mail server.

3. The Email Goes to Your Email Provider's Server:

- The SMTP server of your email provider (for example, Gmail's SMTP server) processes the email and checks:
  - If the recipient's email address is valid.
  - If your email isn't flagged as spam.

4. Email Routing and Delivery:

- Once the SMTP server sends the email, it looks up the **recipient's email server** using a **DNS (Domain Name System)** query to get the recipient's mail server's **IP address**.
  - For example, if you're sending an email to someone@example.com, the DNS system finds the email server for example.com.
- The email is then forwarded to the recipient's **MX (Mail Exchange) server**. **MX records** are DNS records that tell the system where to deliver the email.

5. Recipient's Mail Server:

- The recipient's **email server** (like Yahoo, Outlook, or Gmail) receives the email. It uses the **POP3** or **IMAP** protocol to store the email in the recipient's inbox.
  - **POP3**: Downloads the email to the recipient's device, then deletes it from the server.
  - **IMAP**: Keeps the email on the server, so the recipient can access it from multiple devices.

6. Recipient Receives the Email:

- The recipient can now check their inbox using an email client (like Gmail or Outlook) or a mobile app. The email client uses **IMAP** or **POP3** to retrieve the email from the recipient's email server.

What is DNS?

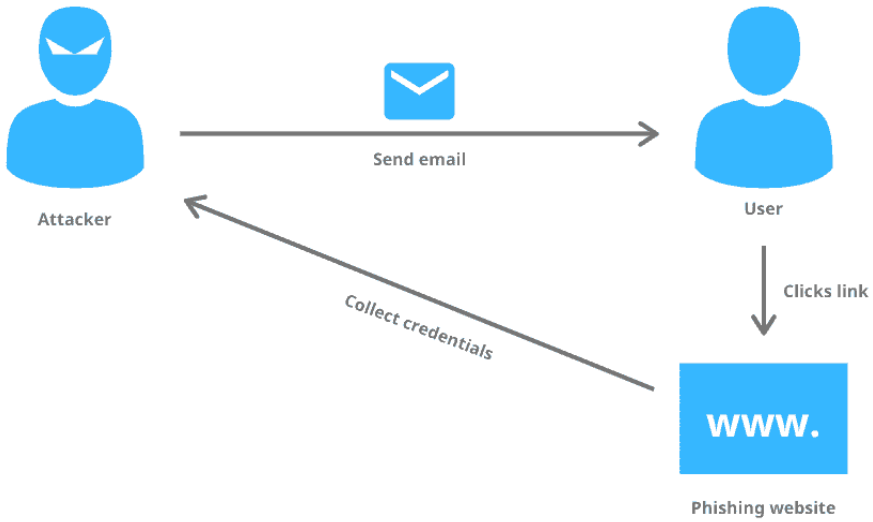
DNS (Domain Name System) is like the **phonebook of the internet**. It helps translate easy-to-remember domain names (like google.com) into **IP addresses** (like 172.217.11.46), which computers and servers use to identify each other on the internet.

What is a Man-in-the-Middle (MITM) Attack?

A **Man-in-the-Middle (MITM) attack** is a type of cyberattack where an attacker secretly **intercepts and alters communication** between two parties without their knowledge. The attacker acts as an **invisible third party** ("man in the middle"), eavesdropping or manipulating data.

What is a Phishing Attack?

A **phishing attack** is a type of cyberattack where hackers trick people into **giving away sensitive information** (like passwords, credit card details, or personal data) by pretending to be a **trusted entity** (such as a bank, social media site, or employer).



Phishing is usually done through **emails, messages, fake websites, or phone calls**, designed to look **legitimate** but actually lead to scams.

How to Prevent Phishing Attacks?

1. **Check the Sender's Email Address** – Phishing emails often use slight changes (e.g., support@paypa1.com instead of support@paypal.com).
2. **Hover Over Links Before Clicking** – If a link looks suspicious, hover your mouse over it to see the real URL before clicking.
3. **Use Multi-Factor Authentication (MFA)** – Even if attackers steal your password, MFA (e.g., a one-time code) makes it harder for them to log in.
4. **Avoid Clicking on Attachments from Unknown Sources** – They may contain malware.
5. **Verify Requests for Sensitive Information** – If you receive an unexpected request for login details or payments, contact the company directly.

6. **Look for HTTPS in Website URLs** – Secure sites start with https:// instead of http://.
7. **Use Security Software and Keep It Updated** – Antivirus and anti-phishing tools help detect and block phishing attempts.
8. **Be Wary of Urgent or Scary Messages** – Attackers often use fear tactics like "Your account will be suspended!" to pressure you into clicking.