18th\_feb: Penetration Testing

Contents for the Day:

Part1:

1.How does the Internet work?  
2.What is TCP/IP?  
3.Denial of Service (DoS) Attacks Explained  
4.What is Cross-Site Scripting (XSS)?  
5.How Data Moves Through the Internet  
6.VPN (Virtual Private Network)  
7.Public vs Private IP Address  
8.SSL, TLS, HTTP, HTTPS  
9.How does Email work?  
10.DNS (Domain Name System) and How It Works  
11.Firewall and Its Role in Network Security  
12.Man-in-the-Middle (MITM) Attacks Explained  
13.Phishing Attacks and How to Prevent Them

Part2:

1. What is Vulnerability Scanning vs. Penetration Testing?
2. Phases of Penetration Testing
3. Types of Penetration Testing (Black-box, White-box, Gray-box)
4. Exploration & Installation of Tools: Burp Suite – Web application security testing Nessus – Vulnerability scanning Acunetix – Automated web vulnerability scanning PenTest Tools – Online security testing tools HostScan – Scanning hosts for vulnerabilities Nmap – Network scanning and port discovery
5. Scanning Various URLs Using These Tools

**How does Internet work?**  
 **How Data Travels Over the Internet?**

Data transmission over the internet involves several key components and processes:

**IP Addresses**: Every device on the internet has a unique IP address, which acts like a postal address, ensuring that data packets reach the correct destination.

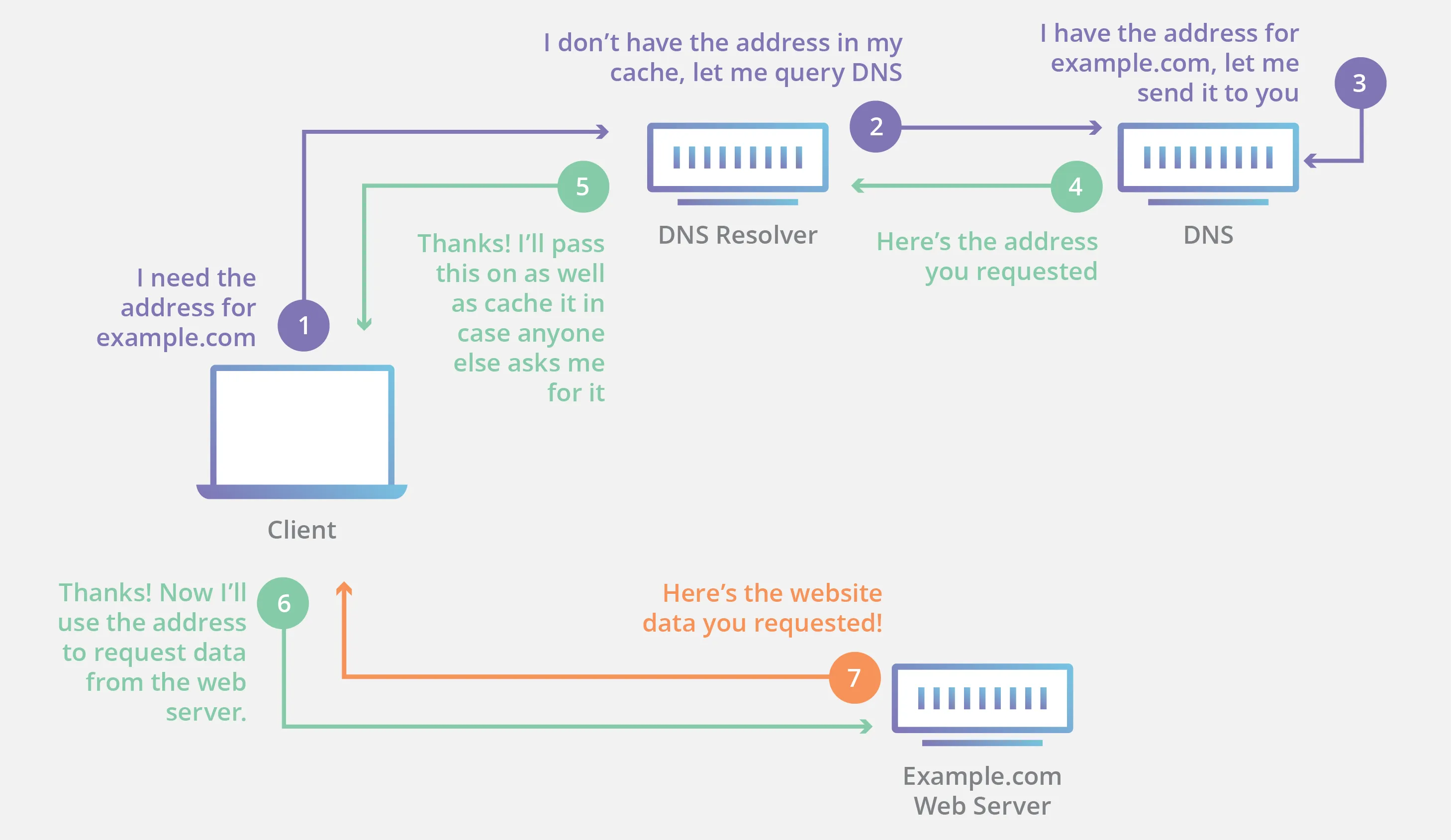
**Packets**: Data is broken down into smaller chunks called packets. Each packet contains both the data being sent and routing information.

**Routers**: Routers are devices that direct packets across the internet. They determine the most efficient path for data to travel from sender to receiver.

**Protocols (TCP/IP)**: The Transmission Control Protocol/Internet Protocol (TCP/IP) governs how data packets are transmitted and ensures accurate delivery, dividing data into packets and reassembling them at the destination.

### **The Role of Servers and Clients**

In the **client-server model**, servers host resources, such as websites and applications, while clients access these resources using browsers or applications. Servers respond to requests from clients, facilitating the sharing of information over the internet. This model is fundamental for efficient communication and resource management.



**TCP/IP:**

-It is a set of protocol that support network communication  
-The TCP/IP model is structured into layers, each responsible for specific functions within the communication process.

At its core, -TCP/IP encompasses two fundamental protocols: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). While IP operates at the network layer, TCP functions at the transport layer, as per the OSI model.

**How TCP/IP Works**  
Data transmission in TCP/IP begins with packetization, where information is divided into manageable packets. Each packet contains essential headers that include the source and destination IP addresses, along with port numbers that facilitate communication between applications.  
  
**Key Components:**

* **IP Addresses:** Uniquely identify devices on the network, ensuring each packet reaches the correct destination.
* **Ports:** Facilitate multiple applications running on a device to communicate simultaneously without interference.

TCP guarantees reliable delivery by establishing a connection and using techniques such as error-checking and acknowledgment for each packet transmitted, ensuring data integrity and order.

### **Applications of TCP/IP**

TCP/IP supports a wide range of applications essential for modern internet functionality. Notable examples include:

* **Web Browsing:** Utilizes HTTP/HTTPS protocols to transfer data for loading webpages.
* **Email Communication:** Employs SMTP for sending emails and IMAP for retrieving them.
* **File Transfer:** Relies on FTP for the exchange of files across networks.

The importance of TCP/IP lies in its ability to facilitate these critical operations, serving as the backbone of internet infrastructure.  
  
**Denial of Service (DOS):**  
*When an* ***attacker prevents authorized users from accessing computer systems****, networks, services, or other information technology (IT) resources, this is known as a* ***denial-of-service (DoS) attack****.*

***XSS: (Cross-Site Scripting)***  
Cross-Site Scripting (XSS) is a prevalent web application vulnerability that occurs when an attacker injects malicious code, usually in the form of JavaScript, into a vulnerable web application.  
  
There are three types of XSS  
Stored XSS, Reflected XSS, and DOM-based XSS.  
  
Stored XSS:  
Stored XSS attacks occur when a malicious script is injected into a web application’s data store, such as a database or content management system. This script is then served to users when they request the affected web page, leading to its execution in the context of their browser. Stored XSS is particularly dangerous because the injected script can be executed by any user who visits the affected page, potentially leading to a wide range of damaging consequences, including data theft and session hijacking.  
  
**Reflected XSS**, also known as Non-Persistent XSS, is a type of Cross-Site Scripting attack in which a malicious script is included as a parameter in a URL or form submission. When a user clicks on a malicious link or submits a form containing the script, it is sent to the server and then “reflected” back to the user’s browser, where it is executed. Unlike Stored XSS, the malicious script is not stored on the server, making Reflected XSS attacks often harder to detect. These attacks typically rely on social engineering tactics, such as phishing emails, to trick users into clicking malicious links.  
  
DOM-based XSS: Its a client-side vulnerability that involves manipulating the Document Object Model (DOM) of a web page to inject malicious scripts. Unlike Stored or Reflected XSS attacks, DOM-based XSS does not involve sending a malicious payload to the server. Instead, the attack exploits client-side JavaScript code, typically by manipulating variables, URL fragments, or other elements of the DOM. The malicious script is then executed in the user’s browser, potentially leading to data theft, session hijacking, or other malicious activities.

**What is VPN( Virtual Private Network) ?**  
A **Virtual Private Network (VPN)** is a technology that creates a secure, encrypted connection over the internet, enabling users to safely access online resources. By masking a user's IP address, a VPN enhances **online privacy** and ensures that sensitive data remains protected from potential threats. With increasing concerns about data security, a VPN becomes essential for maintaining anonymity while browsing, especially on public Wi-Fi networks, allowing individuals to enjoy a safer online experience.

### **Types of VPNs** **Remote Access VPNs**

* **Definition**: Allows individual users to connect securely to a private network from anywhere.
* **Use Case**: Ideal for employees working from home or traveling, as it enables access to company resources securely.

#### **Site-to-Site VPNs**

* **Definition**: Connects entire networks, allowing multiple users in different locations to communicate securely.
* **Use Case**: Used by organizations with multiple offices to share resources and collaborate effectively, ensuring secure data exchange between sites.

**Public vs Private IP Address:**  
**Public IP Address**:- It is the IP address which is used to identify a device over the internet.   
It is assigned by ISP(Internet Service provider) and it’s unique over the internet.  
public IP are not secured as anyone can trace back to you using the Public IP.

**Private IP Address: -** It is the IP address used to establish communication within a local network.  
It is assigned by your router and it’s not unique.  
Private IP are secured as they are used in local network  
  
What is SSL,HTTP,HTTPS,TLS:  
**1. HTTP (Hypertext Transfer Protocol)**

* HTTP is the foundation of the web that allows browsers and servers to communicate.
* It defines how requests and responses are sent over the Internet.
* **Example:** When you enter [http://example.com](http://example.com/), your browser requests the website using HTTP.
* **Security:** HTTP is **not** encrypted, making it vulnerable to attacks like **man-in-the-middle (MITM)**.

### **2. HTTPS (Hypertext Transfer Protocol Secure)**

* HTTPS is the **secure** version of HTTP.
* It uses **TLS (or SSL)** encryption to protect data between your browser and the server.
* **Example:** [https://google.com](https://google.com/) ensures a secure connection.
* **Security Benefits:**
  + Encrypts data, preventing hackers from stealing sensitive information.
  + Helps prevent MITM attacks.
  + Google ranks HTTPS websites higher for security reasons.

### **3. SSL (Secure Sockets Layer)**

* SSL was the **original** security protocol used for encrypted connections over the web.
* It secures HTTP, email, and other data transfers.
* **Versions:** SSL 2.0 and SSL 3.0 (now deprecated due to vulnerabilities).
* **Replaced by:** **TLS** (Transport Layer Security) because SSL had security flaws.

### **4. TLS (Transport Layer Security)**

* TLS is the modern replacement for SSL.
* It provides **encryption, authentication, and data integrity**.
* **Versions:**
  + **TLS 1.0, TLS 1.1** (Deprecated)
  + **TLS 1.2, TLS 1.3** (Most secure and widely used today)
* **How it Works:**
  + Uses cryptographic techniques like **AES (Advanced Encryption Standard)** for secure communication.
  + Ensures data is not tampered with or intercepted.

### **1. HTTP (Hypertext Transfer Protocol)**

* HTTP is the foundation of the web that allows browsers and servers to communicate.
* It defines how requests and responses are sent over the Internet.
* **Example:** When you enter [http://example.com](http://example.com/), your browser requests the website using HTTP.
* **Security:** HTTP is **not** encrypted, making it vulnerable to attacks like **man-in-the-middle (MITM)**.

### **2. HTTPS (Hypertext Transfer Protocol Secure)**

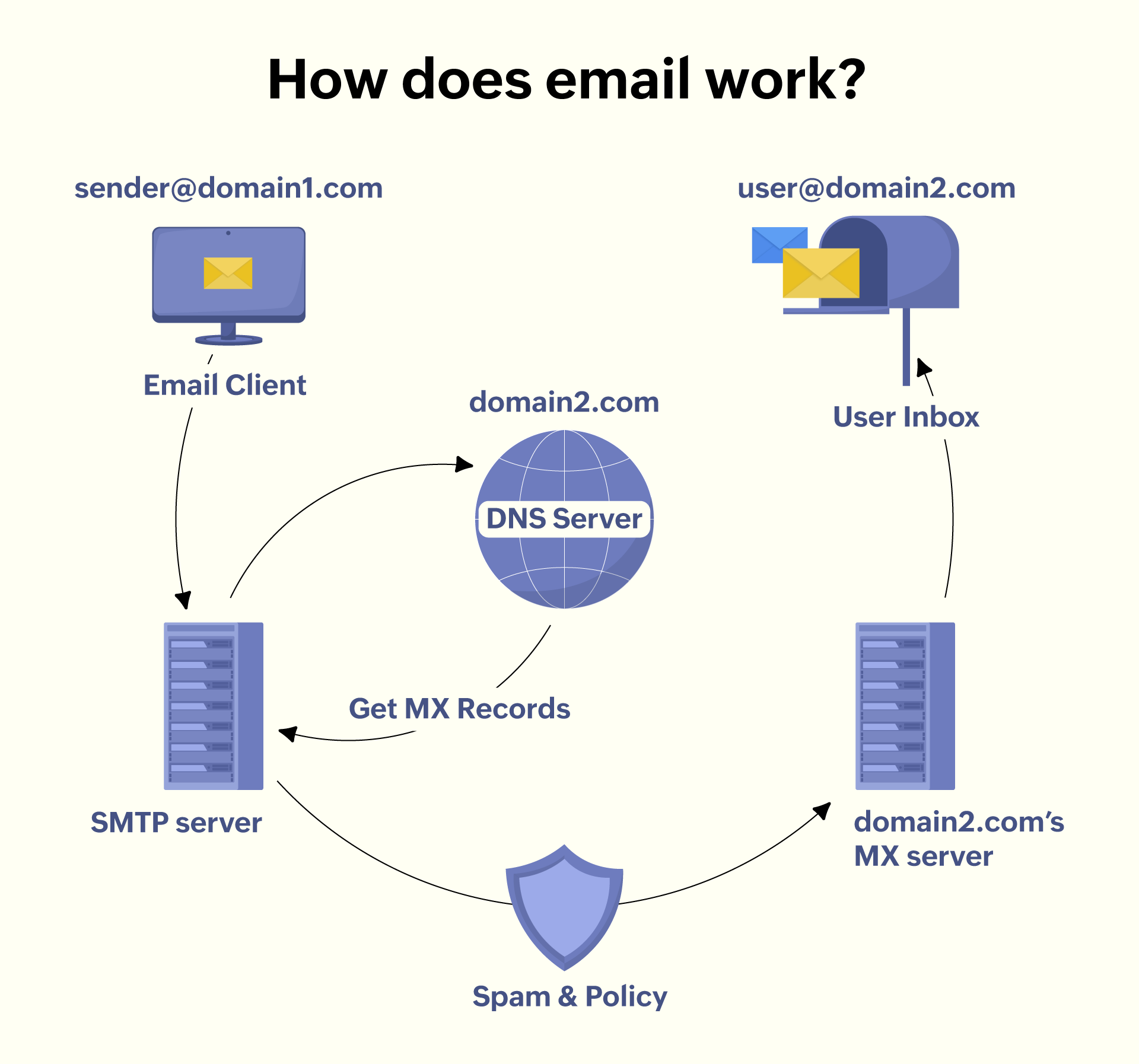
* HTTPS is the **secure** version of HTTP.
* It uses **TLS (or SSL)** encryption to protect data between your browser and the server.
* **Example:** [https://google.com](https://google.com/) ensures a secure connection.
* **Security Benefits:**
  + Encrypts data, preventing hackers from stealing sensitive information.
  + Helps prevent MITM attacks.
  + Google ranks HTTPS websites higher for security reasons.

### **3. SSL (Secure Sockets Layer)**

* SSL was the **original** security protocol used for encrypted connections over the web.
* It secures HTTP, email, and other data transfers.
* **Versions:** SSL 2.0 and SSL 3.0 (now deprecated due to vulnerabilities).
* **Replaced by:** **TLS** (Transport Layer Security) because SSL had security flaws.

### **4. TLS (Transport Layer Security)**

* TLS is the modern replacement for SSL.
* It provides **encryption, authentication, and data integrity**.
* **Versions:**
  + **TLS 1.0, TLS 1.1** (Deprecated)
  + **TLS 1.2, TLS 1.3** (Most secure and widely used today)
* **How it Works:**
  + Uses cryptographic techniques like **AES (Advanced Encryption Standard)** for secure communication.
  + Ensures data is not tampered with or intercepted.

How does Email Works?  


Process at the backend while sending the mail:  
-A user sends the email.

-The outgoing SMTP server validates the authenticity of the sender.

-SMTP server checks the domain details in the recipient's email address.

-SMTP server sends the email to the recipient server based on the [MX Record](https://www.zoho.com/mail/glossary/mx-records.html) found in the recipient's [Domain Name Server (DNS)](https://www.zoho.com/mail/glossary/what-is-dns.html).

-The recipient server validates the email address and delivers the mail.

## How does DNS work?

### **Domain resolution**

When a query for a domain (www.zoho.com) is made from a web browser, it's forwarded to the DNS resolver.

### **Fetching the IP address of the domain**

The DNS resolver checks its cache to resolve the query. If it finds the IP address of the requested domain in the cache, the query is resolved and www.zoho.com is displayed on the web browser.

### **DNS resolver to Root Nameserver**

If the requested domain is not stored in the cache of the DNS resolver, the query is forwarded to the Root Nameserver. The Root Nameserver looks for the domain's extension like '.com', '.net', or '.org' and shares the IP address of the TLD Nameserver with the DNS resolver. It then stores information about the requested extension in its cache.

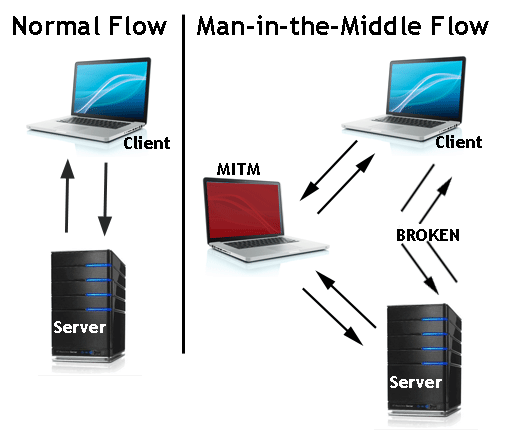
### **Root Nameserver to TLD Nameserver**

The TLD Nameserver then runs a query and shares the IP address of the Authoritative Nameserver that stores the IP address of the requested domain (www.zoho.com).

### **TLD Nameserver to Authoritative Nameserver**

The Authoritative Nameserver resolves the domain query and the website is displayed on the web browser

## **What is a Firewall?** A fire wall is a network security device that observes and filters incoming and outgoing network traffic. A firewall 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 in order to block malicious traffic like viruses and hackers. Role in **Network Security**

A firewall sits as a barrier between an internal an and external network . A firewall prevents unauthorized access and protects your network from hackers and malicious activities.  
  
Man-In-The-Middle Attack:  


**How can be prevented:**

-Avoiding WiFi connections that aren’t password protected.

-Paying attention to browser notifications reporting a website as being unsecured.

-Immediately logging out of a secure application when it’s not in use.

-Not using public networks (e.g., coffee shops, hotels) when conducting sensitive transactions.

# **What is Phishing ?** Phishing is a type of cyber-attack in which attackers attempt to trick people into disclosing sensitive information such as usernames, passwords, credit card numbers, or other personal information*.*

# **How Can we prevent:**

***-Educate:*** Use phishing microlearning and security awareness training to educate, teach, and alter behaviour.

***-Monitor:*** Use phishing simulation tools to assess employee knowledge and identify who in the organization is most vulnerable to phishing attacks.

***-Communicate:*** Maintain open lines of communication and run campaigns regarding phishing emails, social engineering, and cyber security.

***-Incorporate:*** Make cyber security awareness campaigns, training, support, education, and project management a part of your company’s culture.

***-Apply:*** Use this understanding regarding phishing email attacks in your daily activities as an end user. Be aware of the dangers and take the time to carefully examine emails, messages, and webpages.

**What is Vulnerability Scanning?**  
Vulnerability Scanning is a systematic review of security weaknesses within an information system. It involves identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. The process includes:

**-Scanning Systems and Networks:** Automated tools are used to scan for known vulnerabilities.

**-Identifying Vulnerabilities:** These could range from outdated software, missing patches, or faulty configurations.  
**Reporting:** This process culminates in a detailed report outlining the found vulnerabilities.  
Use Case: An e-commerce website wants to identify potential **security risks** in its platform before launching.

**What is Penetration Testing?**  
Penetration Testing, also known as pen testing or ethical hacking, is more aggressive than VA. It simulates a cyber-attack against your computer system to check for exploitable vulnerabilities.   
The primary goal is to identify vulnerabilities that could be exploited by malicious hackers   
Key aspects include:

**-Exploitation:** Unlike VA, PT involves the exploitation of found vulnerabilities.

**-Simulated Attacks:** These mimic the actions of potential attackers, using tools and techniques that real-world attackers would employ.

**-Analysis and Reporting:** The results offer insights into the potential damage and ways to remediate the vulnerabilities.  
Use Case: A bank launches a new mobile banking app and wants to ensure hackers can't steal user credentials.   
  
**Phases of Penetration Testing:**  
There are 5 phases of penetration testing which includes:

1. Planning  
   Goal Setting: Understand the client’s objectives, whether it’s to discover vulnerabilities in a new software product, adhere to regulatory requirements, or validate existing security measures.

Gathering Intelligence: Collect as much information as possible about the target system. This could involve identifying IP addresses, domain names, and network services. Tools like Nmap and Whois can be useful in this phase.

1. Scanning  
   Static Analysis: Examine the codebase without executing it. Tools like Checkmarx or Veracode can be utilized.

Dynamic Analysis: Analyze the codebase while it’s running. Tools such as OWASP ZAP or Burp Suite are often used here.

1. Access Gaining  
   This is where the actual hacking takes place.   
   The tester tries to exploit potential vulnerabilities discovered in the previous phase.  
   The methods can range from SQL injection, buffer overflow, to cross-site scripting.   
   It’s essential to understand that the goal is not to cause harm but to identify if unauthorized access or actions are possible.   
   Tools like Metasploit or Hydra can be invaluable in this phase.
2. Maintaining Access  
   To understand how deep a vulnerability goes, testers try to stay inside the system for a long time—just like a **trojan virus or advanced malware**. They check if an attacker can **stay hidden, maintain access, and steal data** without being detected. This helps determine how much damage a hacker could cause if they got in. It’s similar to how **Advanced Persistent Threats (APTs)** work, where hackers remain unnoticed for a long time, slowly extracting sensitive information.
3. Analysis and Reporting  
   Post-intrusion, a detailed report is crucial. This report usually includes:

Summary of Assessment: The scope, objectives, and methodologies used.

Vulnerabilities Found: Detailed descriptions of vulnerabilities discovered, the data accessed, and the duration of the tester’s presence.

Data Exfiltrated: Information on any data that was accessed during the test.

Recommendations: Strategies to secure vulnerabilities, often categorized by priority.

**Types of penetration testing:**  
  
**Black-box testing:** The tester has no prior knowledge of the system or network being tested. This simulates a real-world attack scenario where an attacker has no insider information.

**White-box testing:** The tester has complete access to the system’s source code, network diagrams, and other internal documentation. This allows for a more in-depth analysis of vulnerabilities.

**Gray-box testing:** The tester has limited knowledge of the system, such as public-facing information or access to certain network segments. This simulates a scenario where an attacker has gained some initial foothold within the system.