Scanning & Reconnaissance:

Scanning in ethical hacking is a network exploration technique used to identify the systems connected to an organization's network. It provides information about the accessible systems, services, and resources on a target system.

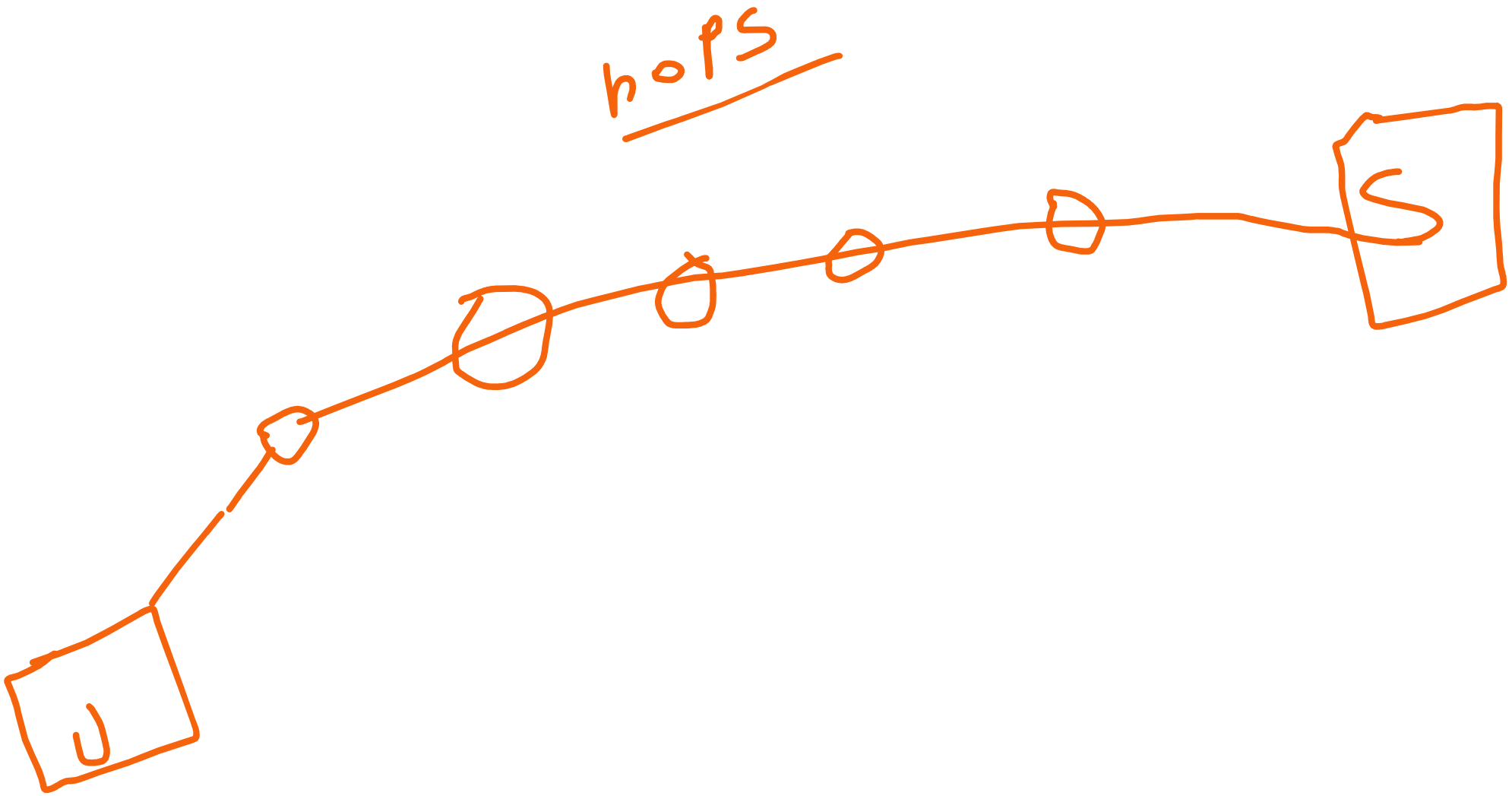
Some may refer to this type of scan as an active scan because it can potentially disrupt services on those hosts that are susceptible. Scanning is often used during vulnerability assessment when probing weaknesses in existing defenses.

Reconnaissance is the practice of covertly discovering and collecting information about a system. This method is often used in ethical hacking or penetration testing.

Like many cybersecurity terms, reconnaissance derives from military language, where it refers to a mission with the goal of obtaining information from enemy territory.

Footprinting

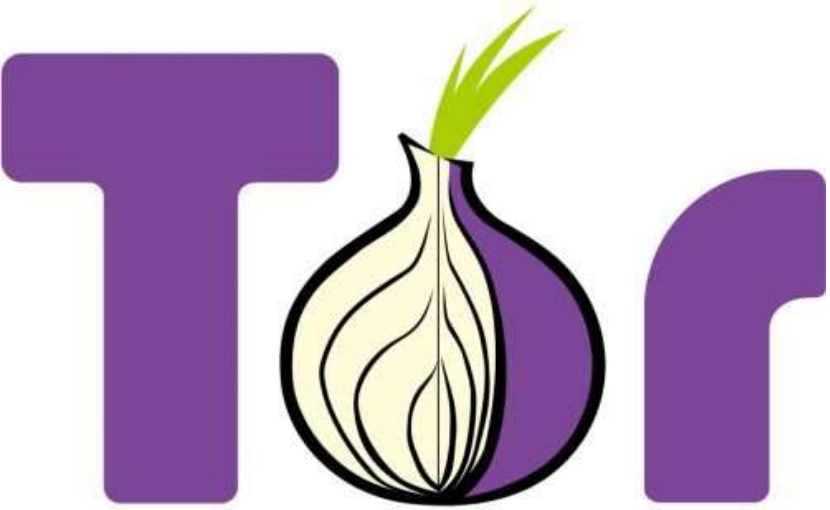
Footprinting is the technique to collect as much information as possible about the targeted network/victim/system. It helps hackers in various ways to intrude on an organization's system. This technique also determines the security postures of the target. Footprinting can be active as well as passive. Passive footprinting/pseudonymous footprinting involves collecting data without the owner knowing that hackers gather their data. In contrast, active footprints are created when personal data gets released consciously and intentionally or by the owner's direct contact.

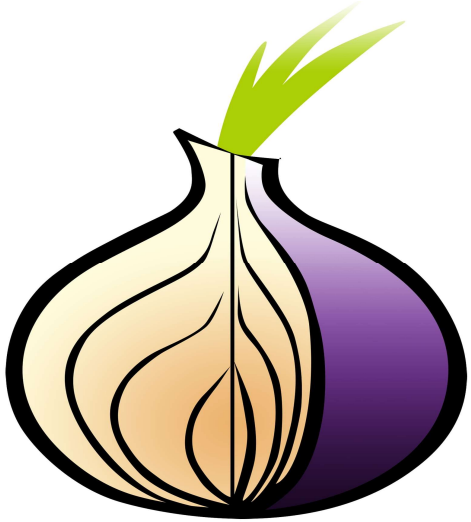

hops
U
S

TOR Network & Its use.

The Tor (the onion routing) browser is a web browser designed for anonymous web surfing and protection against traffic analysis. Although Tor is often associated with the darknet and criminal activity, law enforcement officials, reporters, activists, whistleblowers and ordinary security-conscious individuals often use the browser for legitimate reasons.

The Tor browser enables people to have access to the dark web. While many associate the dark web with illegal activities, the Tor network also has a number of legitimate uses. These include communicating or browsing in countries implementing internet censorship.

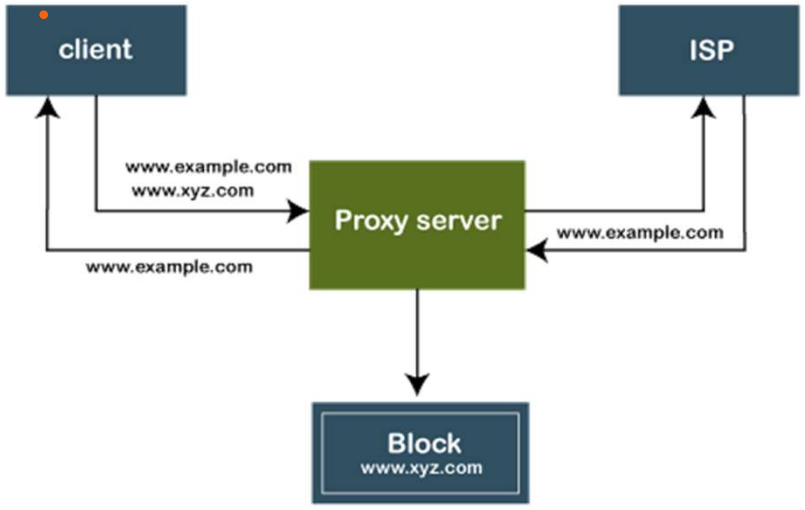




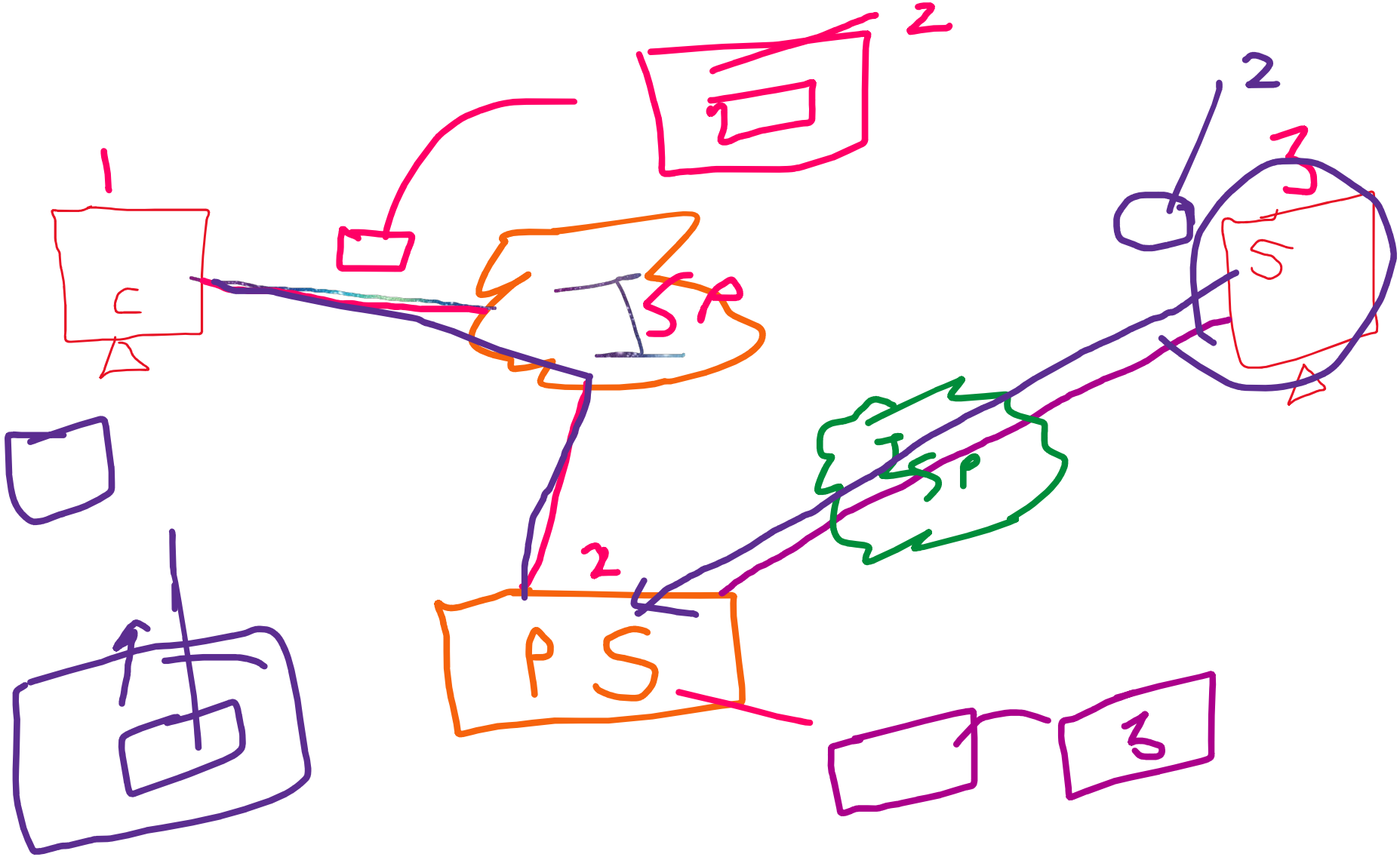
Proxy server & work & use

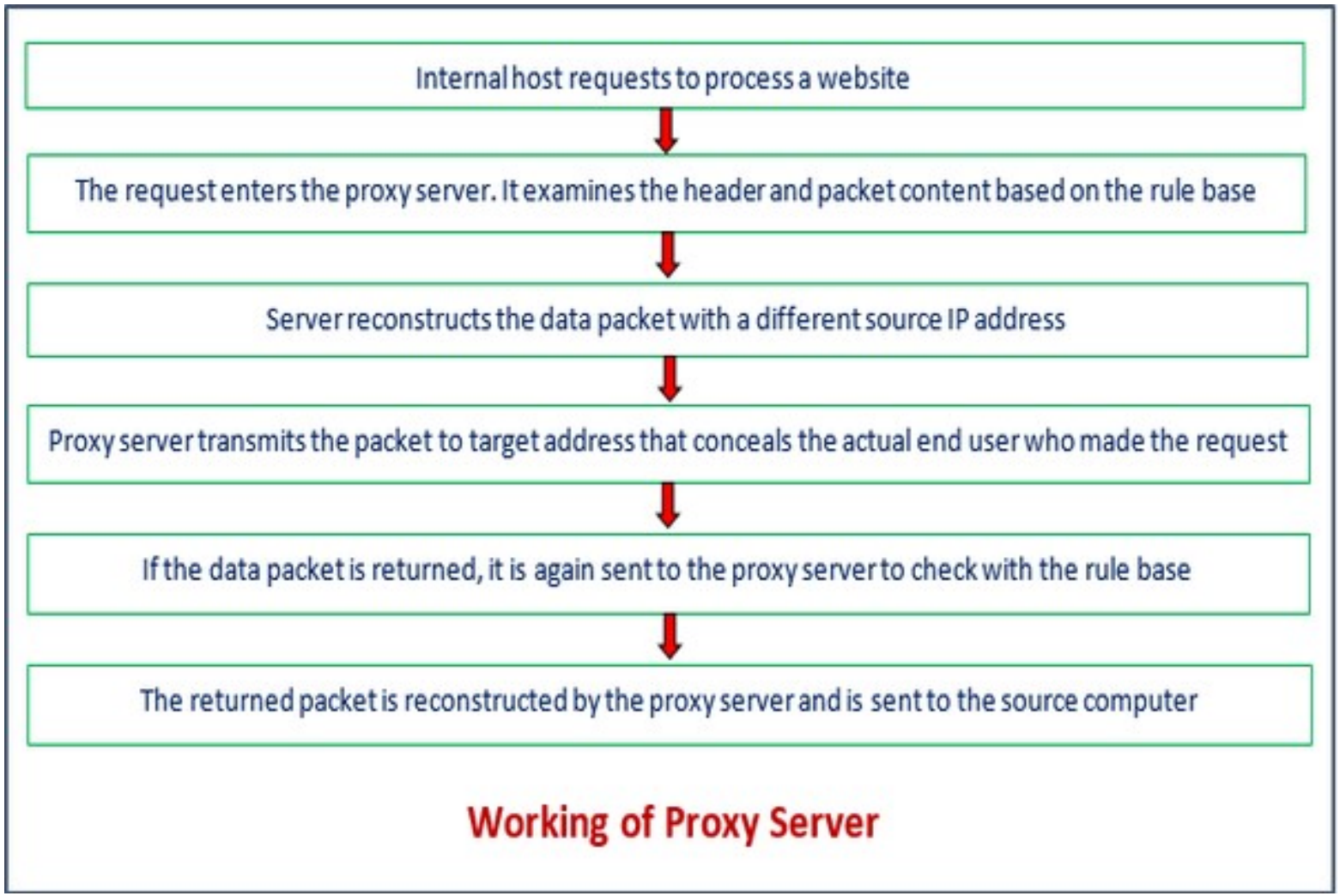
Proxy Server
The proxy server is a computer on the internet that accepts the incoming requests from the client and forwards those requests to the destination server. It works as a gateway between the end-user and the internet. It has its own IP address. It separates the client system and web server from the global network.

In other words, we can say that the proxy server allows us to access any websites with a different IP address. It plays an intermediary role between users and targeted websites or servers. It collects and provides information related to user requests. The most important point about a proxy server is that it does not encrypt traffic.



Mechanism of Proxy Server


2
2
1
C
SP
S
ISP
2
PS
1
3


Internal host requests to process a website
The request enters the proxy server. It examines the header and packet content based on the rule base
Server reconstructs the data packet with a different source IP address
Proxy server transmits the packet to target address that conceals the actual end user who made the request
If the data packet is returned, it is again sent to the proxy server to check with the rule base
The returned packet is reconstructed by the proxy server and is sent to the source computer
Working of Proxy Server

Advantages of Proxy Server

There are the following benefits of using the proxy server:

It improves the security and enhances the privacy of the user.
It hides the identity (IP address) of the user.
It controls the traffic and prevents crashes.
Also, saves bandwidth by caching files and compressing incoming traffic.
Protect our network from malware.
Allows access to the restricted content.

Communication without proxy server

Communication with proxy server

https://www.duplichecker.com/ → to check links inside a URL.

https://lookup.icann.org/ → CHECK DETAILS OF A DOMAIN NAME

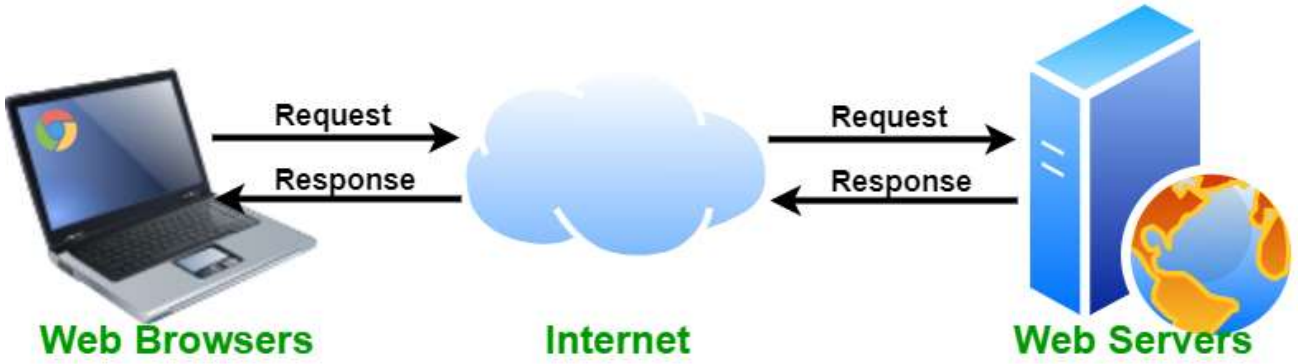
Nmap tool to find the details inside a netwok

https://www.site24x7.com/find-website-location.html SITE LOCATION

Web server & Applications

What is a Web Server?
A Web Server is defined as a server which accepts a request for data and sends the relevant document in return. In other words, it is a computer program that accepts a request for a specific document and sends it to the client machine.

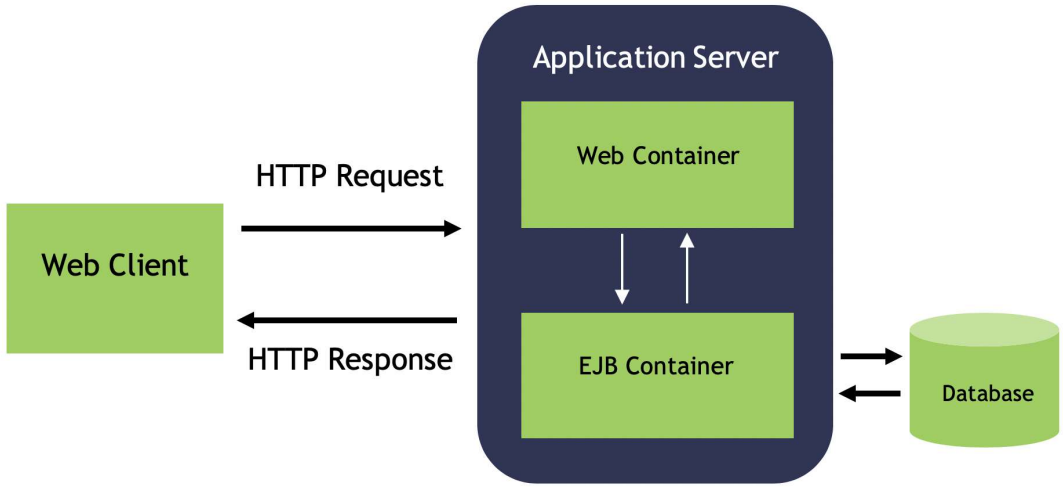
Web servers are designed to serve HTTP content to the client computer. In most cases, the web servers are the integral parts of the application servers. Web servers accept the HTTP requests and interpret them to serve the requested content.



What is an Application Server?

An application server is one that is designed to generate dynamic content. It is a software framework that transforms the data to provide specialized functionalities offered by a business, service, or application. Application servers enhance the interactive parts of a website depending on the context of the request.

Application servers contain web containers and EJB containers. Application servers are entirely responsible for creating an environment for enterprise applications. These servers are capable of supporting HTTP as well as RPC/PMI protocols. Application servers consume more resources like CPU, memory as compared to web servers



Enterprise JavaBeans Containers

What is Web Server Hacking?

Web server hacking is a type of cyber attack that targets web servers, the computers that host websites. It is a malicious attempt to gain unauthorized access to a web server, either to steal data, disrupt services, or gain control of the server. Web server hacking is a serious threat to businesses, as it can lead to data breaches, financial losses, and reputational damage.

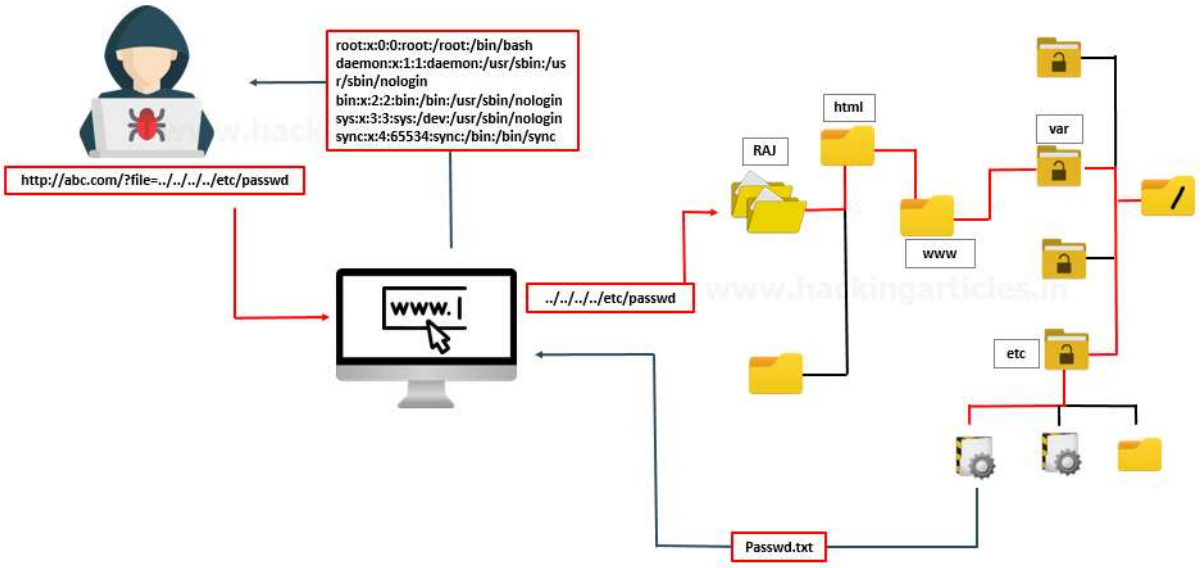
The Impact of Web Server Hacking

Web server hacking can have serious consequences for businesses. It can lead to data breaches, financial losses, and reputational damage. Data breaches can result in the theft of sensitive information, such as customer data, financial records, and intellectual property. Financial losses can occur due to the cost of repairing the damage caused by the attack, as well as the cost of lost business due to the disruption of services. Finally, reputational damage can occur due to the negative publicity associated with a data breach.

Directory traversal attacks

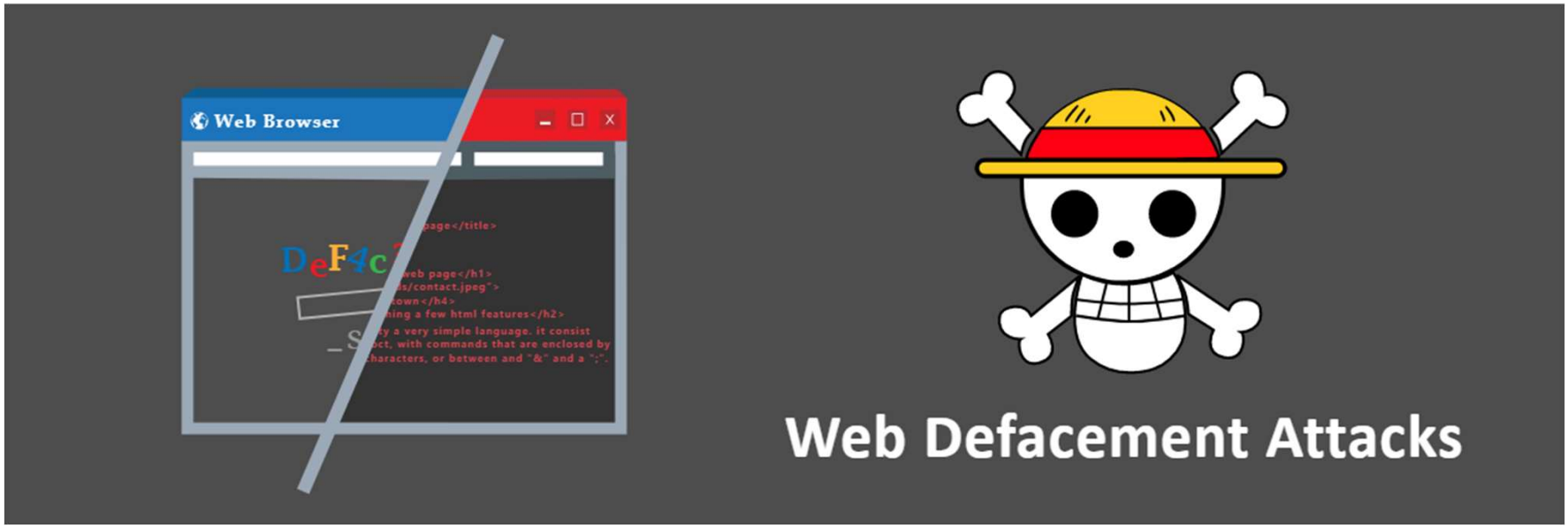
What Is Directory Traversal?
Directory traversal, or path traversal, is an HTTP exploit. It exploits a security misconfiguration on a web server, to access data stored outside the server's root directory. A successful directory traversal attempt enables attackers to view restricted files and sometimes also execute commands on the targeted server.

Typically, a directory traversal attack exploits web browsers. This means that all servers accepting unvalidated input data from web browsers are vulnerable to the attack. To launch this attack, threat actors often scan through a directory tree, which is where they can locate paths to restricted files on web servers.



Website defacement

Website defacements are the unauthorized modification of web pages, including the addition, removal, or alteration of existing content. These attacks are commonly carried out by hacktivists, who compromise a website or web server and replace or alter the hosted website information with their own messages. Website defacements are primarily orchestrated by unskilled actors using automated applications to test vulnerabilities of websites, such as SQL injection attacks. Websites that are unpatched or misconfigured are easily susceptible to simple probing tools used by these actors, which can lead to unauthorized access to websites. These attacks are often opportunistic; when a probing tool is successful they will initiate an attack.



password brute forcing

Brute force attacks occur when a bad actor attempts a large amount of combinations on a target. These attacks frequently involve multiple attempts on account passwords with the hopes that one of them will be valid. It's a bit like trying all of the possible combinations on a padlock, but on a much larger scale.

Passwords are not the only resource that can be brute forced: Links and directories, usernames, and emails are other common targets.

Common sense is important in identifying brute force attempts. Basically, if it appears someone is repeatedly and unsuccessfully trying to log in to an account, it's likely an attempted brute force attack.

Signs can include:

The same IP address unsuccessfully trying to log in multiple times.
Many different IP addresses unsuccessfully trying to log in to a single account.
Multiple unsuccessful login attempts from various IP addresses in a short time period.

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.

Types of SQLi

Though there are plenty of examples of SQL injection , the most common types of SQL injection are the following:

- **Hidden data retrieval**. Changing the SQL query such that it can access hidden database entries.
- **Logic subversion**. Manipulating application logic or using query to interfere with the expected use of application logic to return desired results.
- **Union attacks.** Changing SQL query such that it returns the expected results as well some additional query results, possibly from multiple databases.
- **Examining database**. The SQL query returns database metadata and details such as the structure and schema.
- **Inferential blind SQL injection.** These could be Boolean or time-based attacks ,where querying a series of questions or error-raising input can allow the attacker to determine information stored in the database.
- **Hexadecimal attack**. A variation of query input to evade signature-based detection systems. These queries may use one of the other SQL injection techniques such as logic subversion and union attacks to manipulate application behavior.

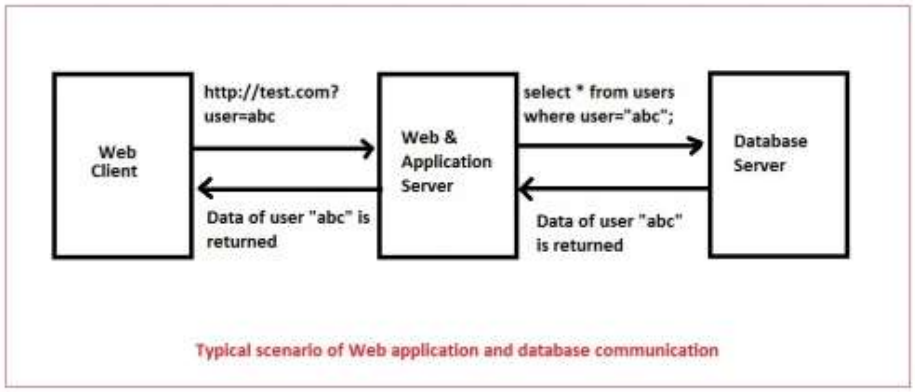
Consequences of SQL Injection:

Authentication bypass: If the authentication form of the application is vulnerable to SQL injection, the user may log into the application without providing proper credentials.

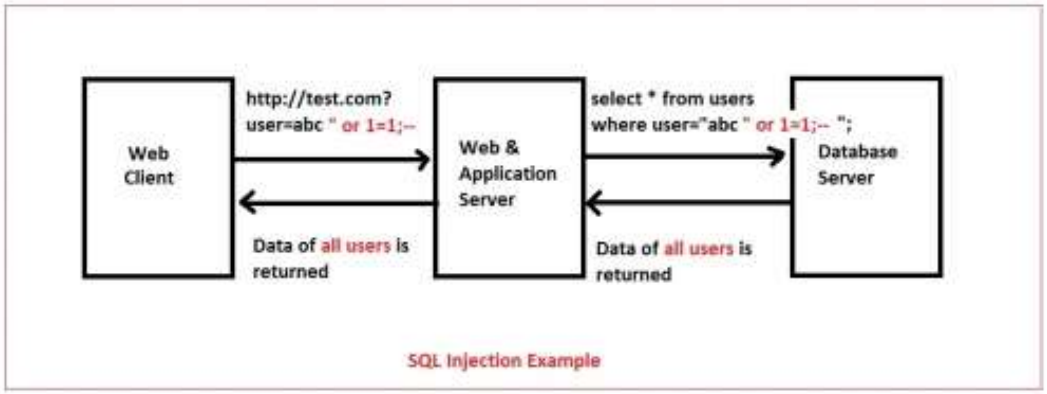
Gaining access to unauthorized data: Through SQL injection, a user may gain access to data which he is not entitled to.

Unauthorized Data Manipulation: SQL injection may also allow an application user to inset, modify or delete data which he is not permitted to. This causes data integrity to be compromised.

Gain administrative privileges: SQL injection could allow an attacker or an malicious user to gain administrative privileges on the database or the database server and ultimately could perform actions like shutting down the database. This affects the availability of the database and consequently, unavailability of the application.



Typical scenario of Web application and database communication



SQL Injection Example

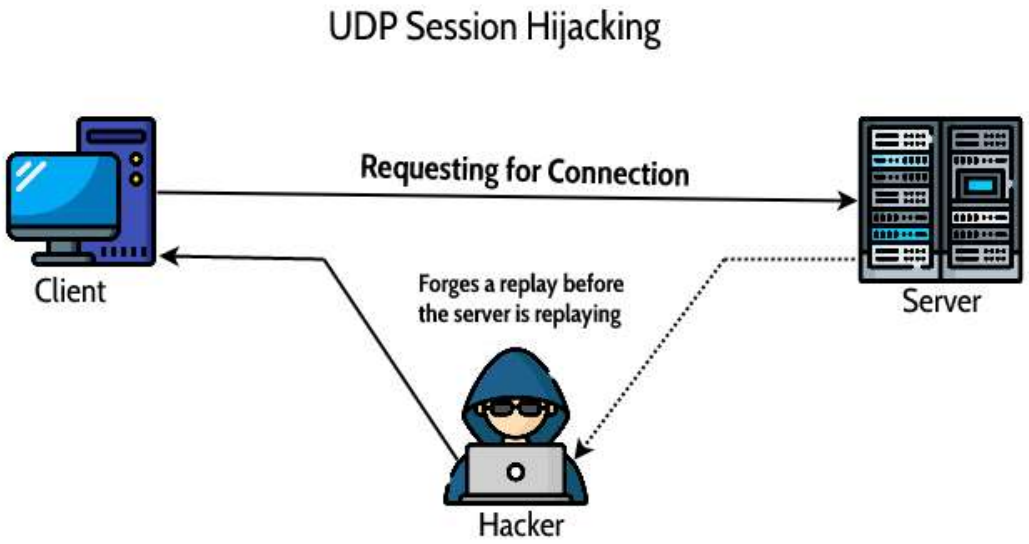
Sql injection detection tools,

- ✓ Netsparker
- ✓ SQLMap
- ✓ jSQL Injection
- ✓ Havij
- ✓ Burp
- ✓ BBQSQL
- ✓ Blisqy
- ✓ Acunetix Web Vulnerability Scanner
- ✓ Damn Small SQLi Scanner
- ✓ Leviathan
- ✓ NoSQLMap
- ✓ Tyrant SQL
- ✓ Whitewidow

Session Hijacking

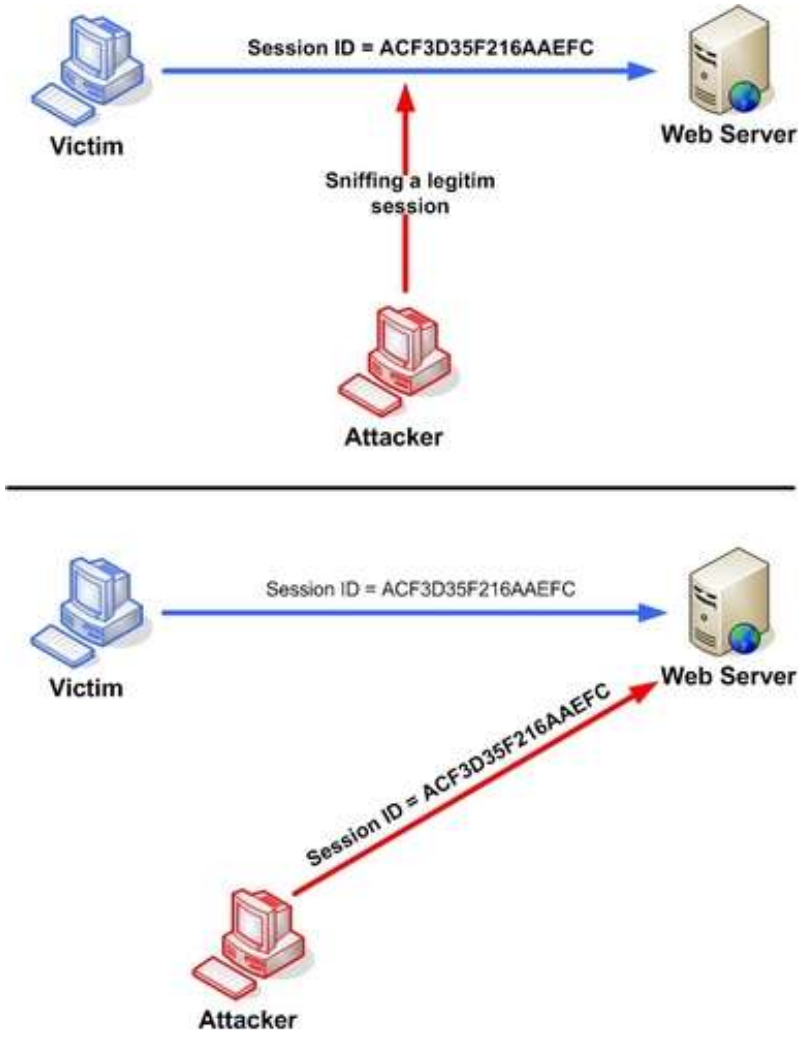
TCP session hijacking is a security attack on a user session over a protected network. The most common method of session hijacking is called IP spoofing, when an attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network and disguise itself as one of the authenticated users. This type of attack is possible because authentication typically is only done at the start of a TCP session.

In order to hijack a session, the attacker needs to have substantial knowledge of the user's cookie session. Although any session can be hacked, it is more common in browser sessions on web applications.



Session Sniffing

In the example, as we can see, first the attacker uses a sniffer to capture a valid token session called “Session ID”, then they use the valid token session to gain unauthorized access to the Web Server.



In order to protect a user's session from getting hijacked, organizations can incorporate certain encryptions. These encryptions are necessary to protect your consumers' sessions and are in the form of certificates.

SSL: SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details.

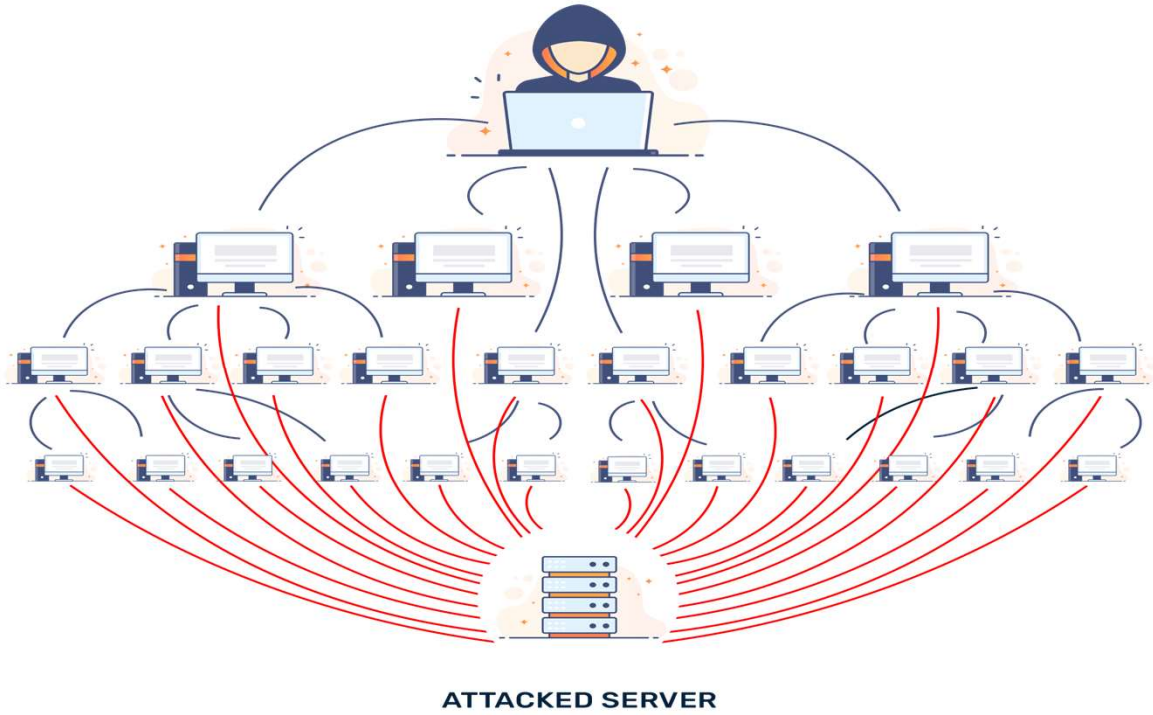
TLS: TLS (Transport Layer Security) is just an updated, more secure, version of SSL.

denial-of-service (DoS) attack

A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack.

The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests.

A DDoS attack is a malicious attempt to disrupt the normal operations of a network or server. It is typically achieved by flooding it with superfluous requests from multiple sources, crippling the handlebar capacity and hindering its ability to respond to legitimate requests. This type of attack differs from DoS (Denial-of-Service) attacks as DDoS involves multiple machines—known as bots—to launch the attack from different locations, thereby masking the identity of the culprit and making it more difficult for organizations to prevent or mitigate. In order to amplify the effect, some bots can even use thousands of machines in a single attack, making responding an arduous task.



If you’re experiencing one or more of these signs, you might be under DDoS attack:

- ✓ **A sudden influx of requests to a specific endpoint or page.**
- ✓ **A flood of traffic that originates from a single IP or range of IP addresses.**
- ✓ **A sudden spike of traffic that occurs at regular intervals or at unusual time frames.**
- ✓ **Problems accessing your website.**
- ✓ **Files load slowly or not at all.**
- ✓ **Slow or unresponsive servers, including “too many connections” error notices.**
- ✓ **A flood of traffic coming from a single device type, geolocation, or web browser version.**
- ✓ **500 internal server errors status codes.**
- ✓ **503 errors on your website.**
- ✓ **You receive a ransom or extortion demand from some attackers.**

503 error, it means that the server in question is unavailable. That could be because it's too busy, for example, or it's under maintenance.

A 500 internal server error is, as the name implies, a general problem with the website's server. More than likely, this means there's an issue or temporary glitch with the website's programming

Botnet

Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks. The term “botnet” is formed from the word’s “robot” and “network.” Assembly of a botnet is usually the infiltration stage of a multi-layer scheme. The bots serve as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution.

Botnets use your devices to scam other people or cause disruptions