# What is a denial-of-service 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.

# How does a DoS attack work?

The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests. The multiple attack vectors of DoS attacks can be grouped by their similarities.

**DoS attacks typically fall in 2 categories:**

## *Buffer overflow attacks*

An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in denial-of-service.

## *Flood attacks*

By saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service. In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

# What are some historically significant DoS attacks?

Historically, DoS attacks typically exploited security vulnerabilities present in network, software and hardware design. These attacks have become less prevalent as DDoS attacks have a greater disruptive capability and are relatively easy to create given the available tools. In reality, most DoS attacks can also be turned into DDoS attacks.

A few common historic DoS attacks include:

- Smurf attack - a previously exploited DoS attack in which a malicious actor utilizes the broadcast address of vulnerable network by sending spoofed packets, resulting in the flooding of a targeted IP address.

- Ping flood - this simple denial-of-service attack is based on overwhelming a target with ICMP (ping) packets. By inundating a target with more pings than it is able to respond to efficiently, denial-of-service can occur. This attack can also be used as a DDoS attack.

- Ping of Death - often conflated with a ping flood attack, a ping of death attack involves sending a malformed packet to a targeted machine, resulting in deleterious behavior such as system crashes.

# How can you tell if a computer is experiencing a DoS attack?

While it can be difficult to separate an attack from other network connectivity errors or heavy bandwidth consumption, some characteristics may indicate an attack is underway.

Indicators of a DoS attack include:

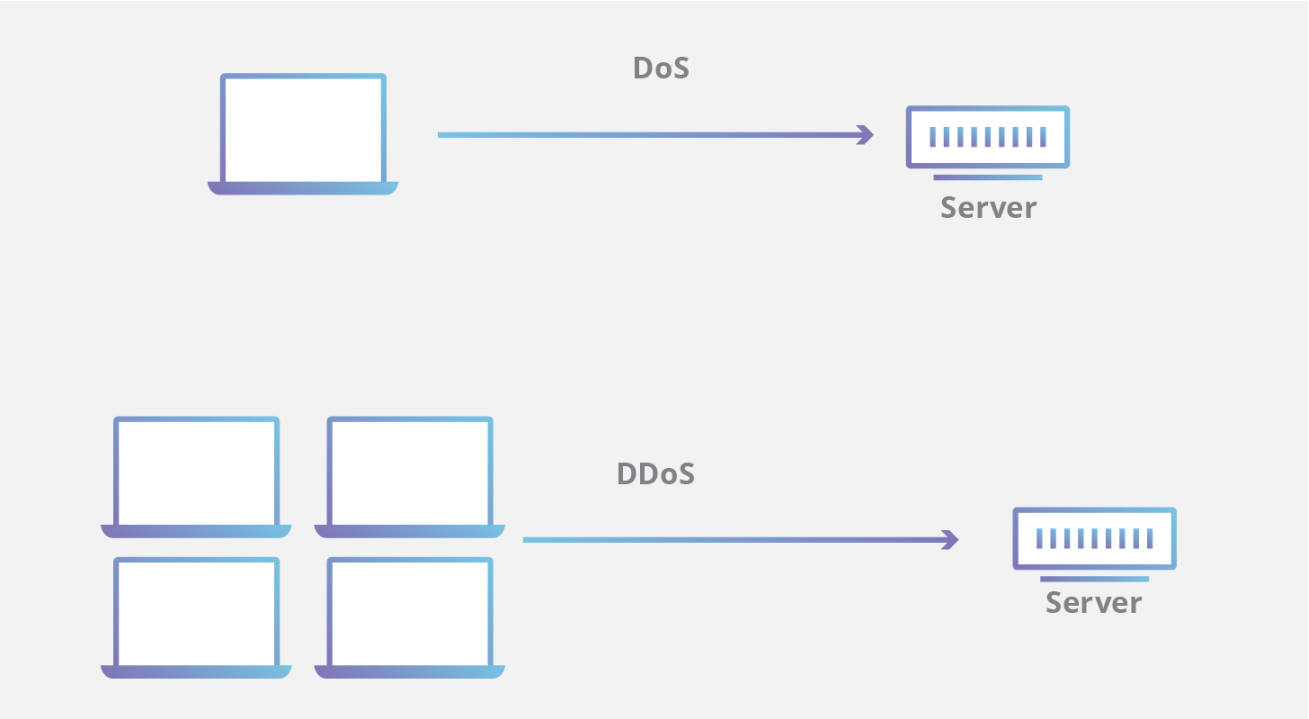
- Atypically slow network performance such as long load times for files or websites

- The inability to load a particular website such as your web property

- A sudden loss of connectivity across devices on the same network

# What is the difference between a DDoS attack and a DOS attack?

The distinguishing difference between DDoS and DoS is the number of connections utilized in the attack. Some DoS attacks, such as “low and slow” attacks like Slowloris, derive their power in the simplicity and minimal requirements needed to them be effective.




DoS utilizes a single connection, while a DDoS attack utilizes many sources of attack traffic, often in the form of a botnet. Generally speaking, many of the attacks are fundamentally similar and can be attempted using one more many sources of malicious traffic. Learn how Cloudflare's DDoS protection stops denial-of-service attacks.

# Ethical Hacking - Sniffing

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of "tapping phone wires" and get to know about the conversation. It is also called **wiretapping** applied to the computer networks.

There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

## What can be sniffed?

One can sniff the following sensitive information from a network –

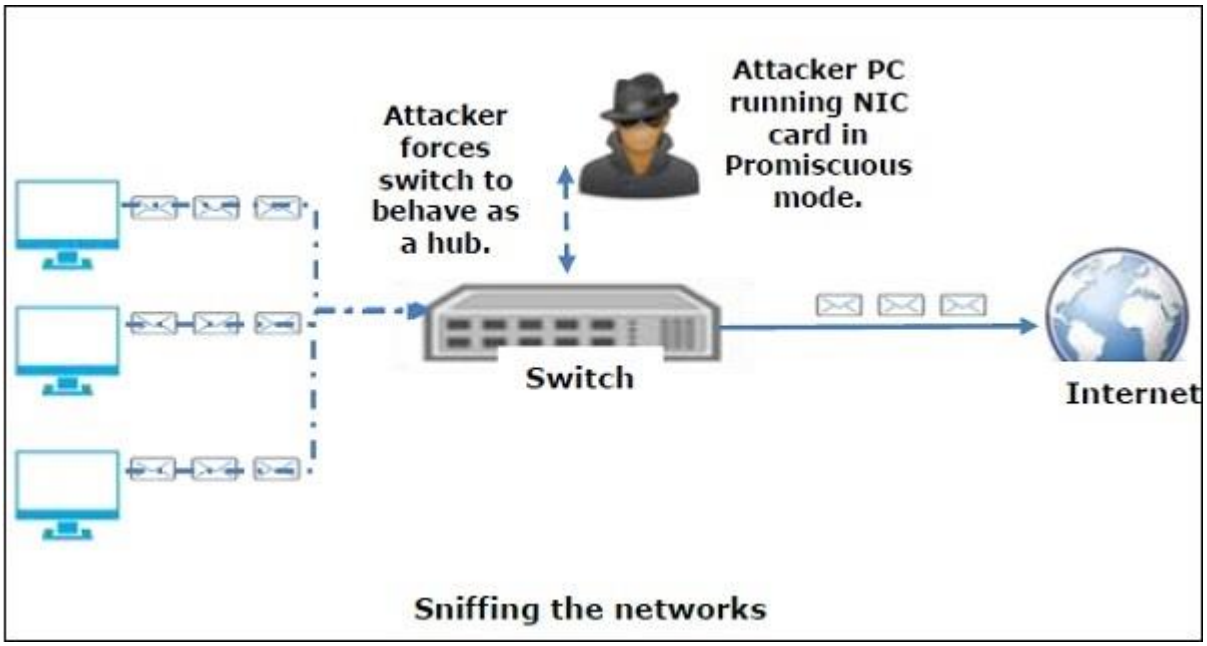
- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

## How it works

A sniffer normally turns the NIC of the system to the **promiscuous mode** so that it listens to all the data transmitted on its segment.

Promiscuous mode refers to the unique way of Ethernet hardware, in particular, network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a.

MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.




A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

## Types of Sniffing

Sniffing can be either Active or Passive in nature.

### Passive Sniffing

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

## Active Sniffing

In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting **address resolution packets** (ARP) into a target network to flood on the switch **content addressable memory** (CAM) table. CAM keeps track of which host is connected to which port.

Following are the Active Sniffing Techniques –

- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Spoofing Attacks
- ARP Poisoning

## Protocols which are affected

Protocols such as the tried and true TCP/IP were never designed with security in mind and therefore do not offer much resistance to potential intruders. Several rules lend themselves to easy sniffing –

- **HTTP** – It is used to send information in the clear text without any encryption and thus a real target.
- **SMTP** (Simple Mail Transfer Protocol) – SMTP is basically utilized in the transfer of emails. This protocol is efficient, but it does not include any protection against sniffing.
- **NNTP** (Network News Transfer Protocol)– It is used for all types of communications, but its main drawback is that data and even passwords are sent over the network as clear text.
- **POP** (Post Office Protocol) – POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.
- **FTP** (File Transfer Protocol) – FTP is used to send and receive files, but it does not offer any security features. All the data is sent as clear text that can be easily sniffed.
- **IMAP** (Internet Message Access Protocol) – IMAP is same as SMTP in its functions, but it is highly vulnerable to sniffing.
- **Telnet** – Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and hence, it can be easily sniffed.

Sniffers are not the dumb utilities that allow you to view only live traffic. If you really want to analyze each packet, save the capture and review it whenever time allows.

# Password Cracking

Password cracking is the most enjoyable hacks for bad guys. It increases the sense of exploration and useful in figuring out the password. The password cracking may not have a burning desire to hack the password of everyone. The actual password of the user is not stored in the well-designed password-based authentication system. Due to this, the hacker can easily access to user's account on the system. Instead of a password, a password hash is stored by the authentication system. The hash function is a one-way design. It means it is difficult for a hacker to find the input that produces a given output. The comparison of the real password and the comparison of two password hash are almost good. The hash function compares the stored password and the hash password provided by the user. In the password cracking process, we extract the password from an associated passwords hash. Using the following ways, we can accomplish it:

**Dictionary attack:** Most of the users use common and weak passwords. A hacker can quickly learn about a lot of passwords if we add a few punctuations like substitute $ for S and take a list of words.

**Brute-force guessing attack:** A given length has so many potential passwords. If you use a brute-force attack, it will guarantee that a hacker will eventually crack the password.

**Hybrid Attack:** It is a combination of Dictionary attack and Brute force attack techniques. This attack firstly tries to crack the password using the dictionary attack. If it is unsuccessful in cracking the password, it will use the brute-force attack.



## How to create a strong password

There are 12 tools for password cracking. These tools use different password cracking algorithm to crack the password. Mostly tools of password cracking are free. So you should maintain a strong password. The following tips are important while creating the password:

- The most important factor is **password length**. The Length of password increases the complexity of password guessing brute force attack. The password can be cracked in a minute if it is made by random 7 characters. If the password is 10 characters, it takes more time as compared to 7 characters.
- The **brute force password guessing** will become more difficult if the user uses a variety of characters. Due to this, the hackers have to try various options for each password's character. Special characters and incorporate numbers also increase the difficulty for the hacker.
- In the **credential stuffing attack**, the hacker uses the stolen password from one online account to the other accounts. So it would be best to use a unique, random and long password for all your online accounts.

## What to avoid for a strong password

Cybercriminal or hacker knows all the clever tricks that users use while creating their passwords. Some common avoidable password mistakes are as follows:

**Dictionary word:** Using the dictionary attacks, every word in the dictionary is tested in seconds.

**Personal information:** The dictionary words are birthplace, relative's name, birthdate, favorite name, pet's name, your name and so on. If they are not, there are various tools in the market that grab the information of the users from social media and build a wordlist for the hackers.

**Patterns:** Most commonly used passwords are asdfgh, qwerty, 123457678, 1111111, and so on. Every password cracker has these passwords on their list.

# Session Hijacking?

Session Hijacking is a Hacking Technique. In this, the hackers (the one who perform hacking) gain the access of a target's computer or online account and exploit the whole web session control mechanism. This is done by taking over an active TCP/IP communication session by performing illegal actions on a protected network. Normally, the web sessions are managed by the session token. The Session Hijacker has access over everything which the actual user has. **For Example,** shopping in an online store or paying your electricity bills, the session hijackers attack over web browsers or web application sessions.

## Types of Session Hijacking:

Session Hijacking is of Three types:

1. **Active Session Hijacking** : An Active Session Hijacking occurs when the attacker takes control over the active session. The actual user of the network becomes in offline mode, and the attacker acts as the authorized user. They can also take control over the communication between the client and the server. To cause an interrupt in the communication between client and server, the attackers send massive traffic to attack a valid session and cause a denial of service attack(DoS).
2. **Passive Session Hijacking** : In Passive Session Hijacking, instead of controlling the overall session of a network of targeted user, the attacker monitors the communication between a user and a server. The main motive of the hacker is to listen to all the data and record it for the future use. Basically, it steals the exchanged information and use for irrelevant activity. This is also a kind of man-in-middle attack (as the attacker is in between the client and the server exchanging information.
3. **Hybrid Hijacking** : The combination of Active Session Hijacking and Passive Session Hijacking is referred to as Hybrid Hijacking. In this the attackers monitors the communication channel (the network traffic), whenever they find the issue, they take over the control on the web session and fulfill their malicious tasks.

To perform these all kinds of Session Hijacking attacks, the attackers use various methods. They have the choice to use a single method or more than one method simultaneously to perform Session Hijacking. Those methods are:

1. Brute-forcing the Session ID
2. Cross-Site Scripting (XSS) or Misdirected Trust
3. Man-in-the-browser
4. Malware infections
5. Session Fixation
6. Session side-jacking
7. **Brute-forcing the Session ID** : As the name suggests, the attack user uses guessing and trial method to find Session ID depending on its length. This is due to lack of security and shorter length. The

introduction of a strong and long session key made this method increase in a slow rate.

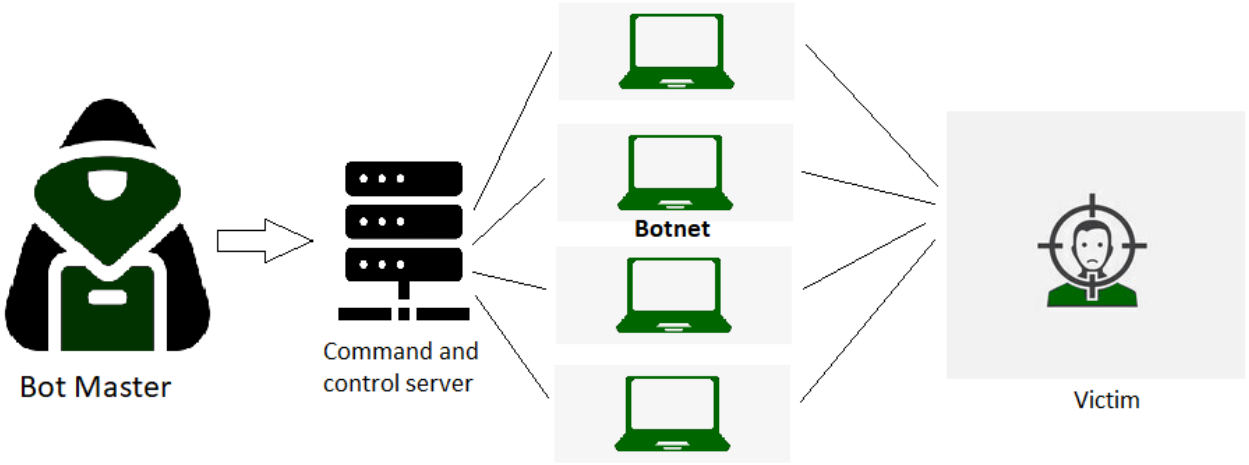
8. **Cross-Site Scripting (XSS) or Misdirected Trust** : In Cross-Site-Scripting, the attacker tries to find out the flaws and the weak point in the web server and injects its code into that. This activity of the attacker will help the attacker to find out the Session ID.
9. **Man-in-the-browser** : Man-in-the-browser uses a Trojan Horse (program that uses malicious code) to perform its required action. The attacker puts themselves in the communication channel of a server and a client. The main purpose of performing this attacks by the attacker is to cause financial fraud.
10. **Malware infections** : In Malware Infections, attacker can deceive the user to open a link that is a malware or Trojans program which will install the malicious software in the device. These are programmed to steal the browser cookies without the user's knowledge.
11. **Session Fixation** : Attackers create a duplicate or another disguised session in Session Fixation. It simply motivates or trick the user into authenticating the vulnerable server. This can be done by sending an email to the user, which on clicking directs to the attacker session.
12. **Session side-jacking** : In Session side-jacking, the attackers tries to get access over a session using the network traffic. This becomes easy when the user is using an insecure Wi-Fi. The reading of network traffic and stealing of session cookie is done by packet sniffing. Packet Sniffing is a technique by which the data flowing across a network is observed.

# What is DDoS(Distributed Denial of Service)?

Distributed Denial of Service (DDoS) is a type of DOS attack where multiple systems, which are trojan infected, target a particular system which causes a DoS attack.

A DDoS attack uses multiple servers and Internet connections to flood the targeted resource. A DDoS attack is one of the most powerful weapons on the cyber platform. When you come to know about a website being brought down, it generally means it has become a victim of a DDoS attack. This means that the hackers have attacked your website or PC by imposing heavy traffic. Thus, crashing the website or computer due to overloading.

**Example:** In 2000, Michael Calce, a 15-year-old boy who used the online name "Mafiaboy", was behind one of the first DDoS attacks. He hacked into the computer networks of various different universities. He used their servers to operate a DDoS attack that brought down several websites such as eBay and Yahoo. In 2016, Dyn was hit with a massive DDoS attack that took down major websites and services such as Netflix, PayPal, Amazon, and GitHub.




## DoS

DoS stands for Denial of Service. It is a type of attack on a service that disrupts its normal function and prevents other users from accessing it. The most common target for a DoS attack is an online service such as a website, though attacks can also be launched against networks, machines, or even a single program.

## Difference between DoS and DDoS

Some of the common differences between DoS and DDoS are mentioned below.

| DoS | DDoS |
|---|---|
| DoS Stands for Denial of service attack. | DDoS Stands for Distributed Denial of service attack. |
| In Dos attack single system targets the victim system. | In DDoS multiple systems attack the victim's system. |
| Victim's PC is loaded from the packet of data sent from a single location. | Victim PC is loaded from the packet of data sent from Multiple locations. |
| Dos attack is slower as compared to DDoS. | A DDoS attack is faster than Dos Attack. |

| DoS | DDoS |
| --- | --- |
| Can be blocked easily as only one system is used. | It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations. |
| In DOS Attack only a single device is used with DOS Attack tools. | In a DDoS attack, The volumeBots are used to attack at the same time. |
| DOS Attacks are Easy to trace. | DDOS Attacks are Difficult to trace. |
| Types of DOS Attacks are:<br>1. Buffer overflow attacks<br>2. Ping of Death or ICMP flood<br>3. Teardrop Attack<br>4. Flooding Attack | Types of DDOS Attacks are:<br>1. Volumetric Attacks<br>2. Fragmentation Attacks<br>3. Application Layer Attacks<br>4. Protocol Attack. |

## Types of DDoS Attacks

There are various types of DDoS attacks mentioned below:

1. **Volumetric Attacks:** Volumetric Attacks are the most prevalent form of DDoS attacks. They use a botnet to overload the network or server with heavy traffic but exceed the network's capabilities of processing the traffic. This attack overloads the target with huge amounts of junk data. This leads to the loss of network bandwidth and can lead to a complete denial of service.
2. **Protocol Attacks:** TCP Connection Attacks exploit a vulnerability in the TCP connection sequence which is commonly referred to as the three-way handshake connection between the host and the server. The work is explained as follows. The targeted server receives a request to start with the handshake. In this attack, the handshake is never accomplished. This leaves the connected port as busy and unavailable to process any further requests. Meanwhile, the cybercriminal continues to send multiple requests overwhelming all the working ports and shutting down the server.
3. **Application Attacks:** Application layer attacks (Layer 7 attacks) target the applications of the victim in a slower fashion. Thus, they may initially appear as legitimate requests from users and the victim becomes unable to respond. These attacks target the layer where a server generates web pages and responds to HTTP requests. Application-level attacks are

combined with other kinds of DDoS attacks targeting applications, along with the network and bandwidth. These attacks are threatening as it is more difficult for companies to detect.

4. **Fragmentation Attacks:** The cybercriminal exploits frangibility in the datagram fragmentation process, in which IP datagrams are divided into smaller packets, transferred across a network, and then reassembled. In such attacks, fake data packets are unable to be reassembled.

## How do DDoS Attacks Work?

The logic of a DDoS attack is very simple, although attacks can be highly different from each other. Network connections consist of various layers of the OSI model. Various types of DDoS attacks focus on particular layers. Examples are illustrated below:

- **Layer-3:** Network layer **–** Attacks are known as Smurf Attacks, ICMP Floods, and IP/ICMP Fragmentation.
- **Layer-4:** Transport layer **–** Attacks include SYN Floods, UDP Floods, and TCP Connection Exhaustion.
- **Layer-7:** Application layer **–** HTTP-encrypted attacks.

# Hack a Web Server

Customers usually turn to the internet to get information and buy products and services. Towards that end, most organizations have websites.**Most websites store valuable information such as credit card numbers, email address and passwords, etc**. This has made them targets to attackers. Defaced websites can also be used to communicate religious or political ideologies etc.

## Web server vulnerabilities

**A web server is a program that stores files (usually web pages) and makes them accessible via the network or the internet**. A web server requires both hardware and software. Attackers usually target the exploits in the software to gain authorized entry to the server. Let’s look at some of the common vulnerabilities that attackers take advantage of.

- **Default settings**– These settings such as default user id and passwords can be easily guessed by the attackers. Default settings might also allow performing certain tasks such as running commands on the server which can be exploited.
- **Misconfiguration**of operating systems and networks – certain configuration such as allowing users to execute commands on the server can be dangerous if the user does not have a good password.

- **Bugs in the operating system and web servers**– discovered bugs in the operating system or web server software can also be exploited to gain unauthorized access to the system.

In additional to the above-mentioned web server vulnerabilities, the following can also led to unauthorized access

- **Lack of security policy and procedures**– lack of a security policy and procedures such as updating antivirus software, patching the operating system and web server software can create security loop holes for attackers.

## Types of Web Servers

The following is a list of the common web servers

- **Apache**– This is the commonly used web server on the internet. It is cross platform but is it's usually installed on Linux.
  Most PHP websites are hosted on Apache servers.
- **Internet Information Services (IIS)**– It is developed by Microsoft. It runs on Windows and is the second most used web server on the internet. Most asp and aspx websites are hosted on IIS servers.
- **Apache Tomcat** – Most Java server pages (JSP) websites are hosted on this type of web server.
- **Other web servers** – These include Novell's Web Server and IBM's Lotus Domino servers.

## Types of Attacks against Web Servers

**Directory traversal attacks**– This type of attacks exploits bugs in the web server to gain unauthorized access to files and folders that are not in the public domain. Once the attacker has gained access, they can download sensitive information, execute commands on the server or install malicious software.

- **Denial of Service Attacks**– With this type of attack, the web server may crash or become unavailable to the legitimate users.
- **Domain Name System Hijacking –** With this type of attacker, the DNS setting are changed to point to the attacker's web server. All traffic that was supposed to be sent to the web server is redirected to the wrong one.
- **Sniffing**– Unencrypted data sent over the network may be intercepted and used to gain unauthorized access to the web server.

- **Phishing**– With this type of attack, the attack impersonates the websites and directs traffic to the fake website. Unsuspecting users may be tricked into submitting sensitive data such as login details, credit card numbers, etc.
- **Pharming**– With this type of attack, the attacker compromises the Domain Name System (DNS) servers or on the user computer so that traffic is directed to a malicious site.
- **Defacement**– With this type of attack, the attacker replaces the organization's website with a different page that contains the hacker's name, images and may include background music and messages.

**Password cracking** doesn't have to involve fancy tools, but it's a fairly tedious process. If the target doesn't lock you out after a specific number of tries, you can spend an infinite amount of time trying every combination of alphanumeric characters. It's just a question of time and bandwidth before you break into a system.

We have passwords for emails, databases, computer systems, servers, bank accounts, and virtually everything that we want to protect. Passwords are in general the keys to get access into a system or an account.

In general, people tend to set passwords that are easy to remember, such as their date of birth, names of family members, mobile numbers, etc. This is what makes the passwords weak and prone to easy hacking.

One should always take care to have a strong password to defend their accounts from potential hackers. A strong password has the following attributes −

- Contains at least 8 characters.
- A mix of letters, numbers, and special characters.
- A combination of small and capital letters.

The most common passwords found are password, root, administrator, admin, operator, demo, test, webmaster, backup, guest, trial, member, private, beta, [company_name] or [known_username].

There are three basic types of password cracking tests that can be automated with tools:

- Dictionary - A file of words is run against user accounts, and if the password is a simple word, it can be found pretty quickly.
  - In a dictionary attack, the hacker uses a predefined list of words from a dictionary to try and guess the password. If the set password is weak, then a dictionary attack can decode it quite fast.
  - **Hydra** is a popular tool that is widely used for dictionary attacks.

- Hybrid - A common method utilized by users to change passwords is to add a number or symbol to the end. A hybrid attack works like a dictionary attack, but adds simple numbers or symbols to the password attempt.

  - Hybrid dictionary attack uses a set of dictionary words combined with extensions. For example, we have the word “admin” and combine it with number extensions such as “admin123”, “admin147”, etc.
  - **Crunch** is a wordlist generator where you can specify a standard character set or a character set. **Crunch** can generate all possible combinations and permutations. This tool comes bundled with the Kali distribution of Linux.

- Brute force - The most time-consuming, but comprehensive way to crack a password. Every combination of character is tried until the password is broken.
  - In a brute-force attack, the hacker uses all possible combinations of letters, numbers, special characters, and small and capital letters to break the password. This type of attack has a high probability of success, but it requires an enormous amount of time to process all the combinations. A brute-force attack is slow and the hacker might require a system with high processing power to perform all those permutations and combinations faster.
  - **John the Ripper** or **Johnny** is one of the powerful tools to set a brute-force attack and it comes bundled with the Kali distribution of Linux.

Some common Web password cracking tools are:

- Brutus is a password cracking tool that can perform both dictionary attacks and brute force attacks where passwords are randomly generated from a given character. Brutus can crack the multiple authentication types, HTTP (Basic authentication, HTML Form/CGI), POP3, FTP, SMB and Telnet.
- WebCracker is a simple tool that takes text lists of usernames and passwords, and uses them as dictionaries to implement basic authentication password guessing.
- ObiWan is a Web password cracking tool that can work through a proxy. ObiWan uses wordlists and alternations of numeric or alpha-numeric characters as possible passwords.