A cyber attack is a set of actions performed by threat actors, who try to gain unauthorized access, steal data or cause damage to computers, computer networks, or other computing systems. A cyber attack can be launched from any location. The attack can be performed by an individual or a group using one or more tactics, techniques and procedures (TTPs).

The individuals who launch cyber attacks are usually referred to as cybercriminals, threat actors, bad actors, or hackers. They can work alone, in collaboration with other attackers, or as part of an organized criminal group. They try to identify vulnerabilities—problems or weaknesses in computer systems—and exploit them to further their goals.

Cybercriminals can have various motivations when launching cyber attacks. Some carry out attacks for personal or financial gain. Others are “hacktivists” acting in the name of social or political causes. Some attacks are part of cyberwarfare operations conducted by nation states against their opponents, or operating as part of known terrorist groups.

What Is a Denial-of-Service (DoS) Attack?

A denial-of-service (DoS) attack is a cyberattack on devices, information , or other network resources that prevents legitimate users from accessing expected services and resources.

This is usually accomplished by flooding the targeted host or network with traffic until the target can't respond or crashes. DoS attacks can last from a few hours to many months, costing companies and consumers time and money while their resources and services are unavailable.

- A denial-of-service (DoS) is a form of cyberattack that prevents legitimate users from accessing a computer or network.
- In a DoS attack, rapid and continuous online requests are sent to a target server to overload the server’s bandwidth.
- Distributed denial-of-service (DDoS) attacks leverage a wide web of computers or devices infected with malware to launch a coordinated barrage of meaningless online requests, blocking legitimate access.

How Denial-of-Service Attacks Work

DoS attacks are on the rise as businesses and consumers use more digital platforms to and transact with each other.

Cyberattacks are often launched to steal personally identifiable information (PII), causing considerable damage to companies' financial pockets and reputations. Data breaches can target a specific company or a host of companies at the same time. For example, a company with high-security protocols in place may be attacked through a member of its supply chain that has inadequate security measures. When multiple companies have been selected for an attack, the perpetrators can use a DoS approach.

In a DoS attack, the cyber attackers typically use one internet connection and one device to send rapid and continuous requests to a target server to overload the server's bandwidth. DoS attackers exploit a software vulnerability in the system and proceed to exhaust the RAM or CPU of the server.

DoS attacks are attempts to interrupt a website or network's operations by overwhelming it with traffic. The attacker achieves this by sending an enormous amount of requests to the target server, which causes it to slow down or even crash, making it inaccessible to legitimate users. Denial of service (DOS) is a network security attack, in which, the hacker makes the system or data unavailable to someone who needs it.

- Denial of service is of various types :
  1. **Browser Redirection** – This happens when you are trying to reach a webpage, however, another page with a different URL opens. You can view only the directed page and are unable to view the contents of the original page. This is because the hacker has redirected the original page to a different page.
  2. **Closing Connections** – After   the connection, there can be no communication between the sender(server) and the receiver(client). The hacker closes the open connection and prevents the user from accessing resources.
  3. **Data Destruction** – This is when the hacker destroys the resource so that it becomes unavailable. He might delete the resources, erase, wipe, overwrite or drop tables for data destruction.
  4. **Resource Exhaustion** – This is when the hacker repeatedly requests access for a resource and eventually overloads the web

application. The application slows down and finally crashes. In this case the user is unable to get access to the webpage.

How Do DoS Attacks Impact Businesses and Users?

DoS attacks can have severe consequences for businesses and users alike. Here are some impacts of DoS attacks:

- Loss of Revenue: DoS attacks can cause businesses to lose significant amounts of revenue as customers are unable to access their website or service.
- Damage to Reputation: DoS attacks can damage a company's reputation and erode the trust of its customers.
- Financial Losses: The cost of mitigating a DoS attack can be significant, and businesses may also have to pay for lost revenue, legal fees and damages.
- Disruption of Critical Services: DoS attacks can disrupt critical services, such as healthcare and emergency services, which can have life-threatening consequences.
- Loss of Data: Data destruction attacks can cause businesses to lose critical data, leading to financial losses and damage to the company's reputation.

Preventing DoS Attacks: There are several measures businesses can take to prevent DoS attacks, including:

- Implementing DDoS protection solutions that can detect and mitigate DoS attacks in real time.
- Ensuring their website and network infrastructure is up-to-date with the latest security patches.
- Using strong authentication mechanisms, such as multi-factor authentication, to prevent unauthorized access to the network.
- Monitoring network traffic to detect unusual patterns and take immediate action to prevent potential attacks.

Conclusion: *DoS attacks are a serious threat to businesses and users alike. They can cause significant financial losses, damage to reputation, and even life-threatening consequences. Understanding the different types of DoS attacks and implementing appropriate security measures can help businesses mitigate the risks of DoS attacks and protect their assets and customers.*

1. DOS Attack is a denial of service attack, in this attack a computer sends a massive amount of traffic to a victim's computer and shuts it down. Dos attack is an online attack that is used to make the website unavailable for its users when done on a website. This attack makes the server of a website that is connected to the internet by sending a large number of traffic to it.

2. DDOS Attack means distributed denial of service in this attack dos attacks are done from many different locations using many systems.

Difference between DOS and DDOS attacks:

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 attacks the victims system..
Victim 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 location.
Dos attack is slower as compared to DDoS.	DDoS attack is faster than Dos Attack.
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 single device is used with DOS Attack tools.	In DDoS attack,The volumeBots are used to attack at the same time.
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace.
Volume of traffic in the Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.
Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack 4. Flooding Attack	Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks 4. Protocol Attack.

What is DDoS Attack?

A Distributed Denial of Service (DDoS) attack attempts to make an online service or a website unavailable by overloading it with vast floods of internet traffic generated from multiple sources. Exploited machines can include computers and other networked resources such as IoT devices.

A Denial of Service (DoS) attack, in which one computer and one Internet connection are used to flood a targeted resource with packets, but a DDoS attack uses many computers and many Internet connections, often distributed globally in what is referred to as a **botnet**.

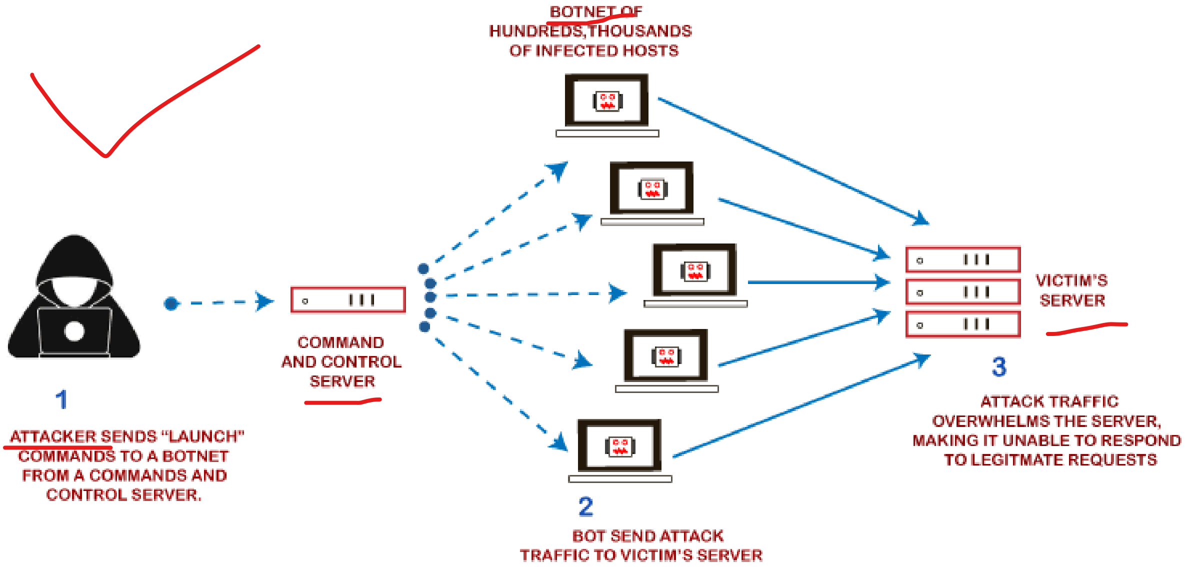
A large-scale volumetric DDoS attack can generate traffic measured in tens of Gigabits (and even hundreds of Gigabits) per second. A regular network will not be able to handle such traffic.

Attackers build a network of hacked machines known as **botnets** by spreading malicious code through emails, websites, and social media. Once these computers are infected, they can be controlled remotely, without their owners' knowledge, and used as an army to launch an attack against any target.

Backward Skip 10sPlay VideoForward Skip 10s

How DDoS attack works?

DDoS attacks are carried out with networks of Internet-connected machines. A DDoS attack can be generated in the following step by step way, such as:



1. These networks consist of computers and other devices such as IoT devices that have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots or zombies, and a group of bots is called a **botnet**.
2. Once a botnet has been established, the attacker can direct an attack by sending remote instructions to each bot. It can use for sending more connection requests than a server can handle at a time.
3. Attackers can have computers send a victim resource huge amounts of random data to use up the target's bandwidth.
4. When the botnet targets a victim's server or network, each bot sends requests to the target's IP address, potentially causing the server or network to become overload, resulting in a denial-of-service to regular traffic.

Due to the distributed nature of these machines, they can use to generate distributed high traffic, which may be difficult to handle. It finally results in a complete blockage of a service.

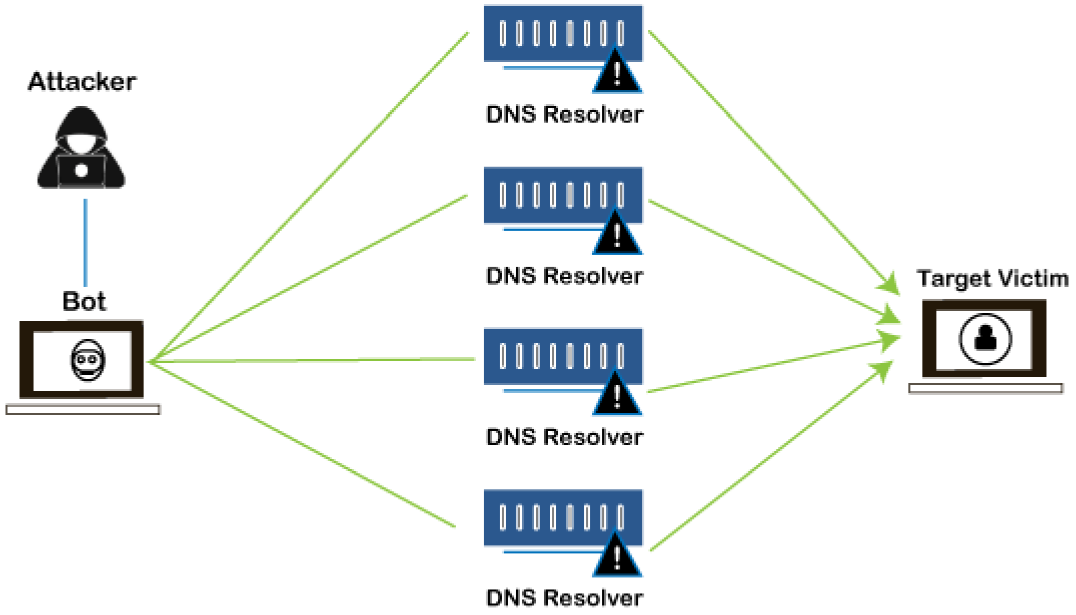
Types of DDoS Attacks

Distributed Denial of Service attacks can be broadly categorized into these three categories:

1. Volume-Based Attacks

Volume-based attacks use massive amounts of fake traffic to overwhelm a resource such as a website or a server.

It includes TCP floods, UDP floods, ICMP floods, and other spoofed-packet floods. These are also called Layer 3 & 4 Attacks. Here, an attacker tries to saturate the bandwidth of the target site. The attack magnitude is measured in **Bits per Second** (bps).

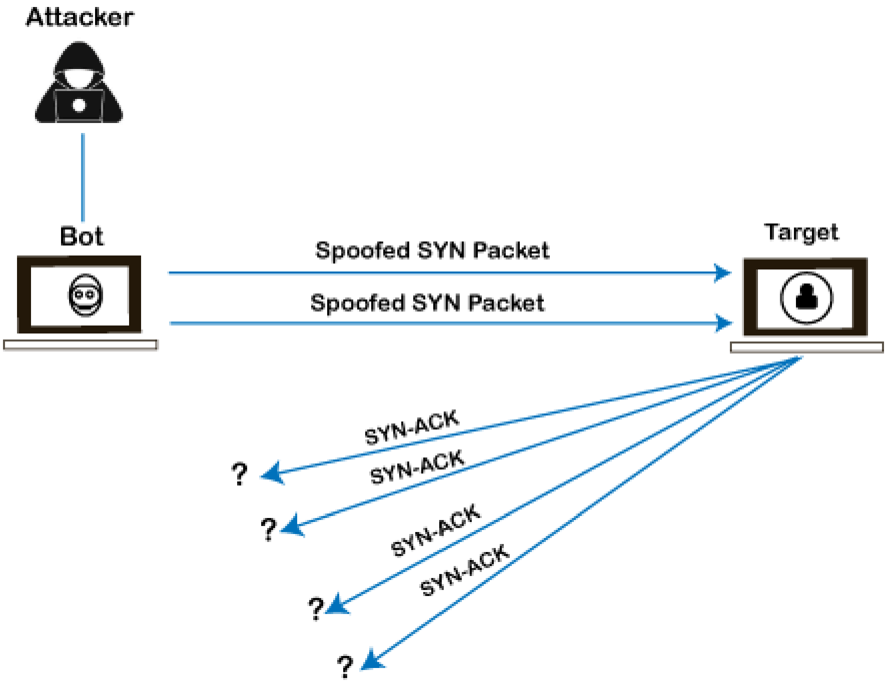


- **Amplification Attack:** The attacker makes a request that generates a significant response which includes DNS requests for large TXT records and HTTP GET requests for large files like images, PDFs, or any other data files.
- **UDP Flood:** A UDP flood is used to flood random ports on a remote host with numerous UDP packets, more specifically port number 53. Specialized firewalls are used to filter out or block malicious UDP packets.
- **ICMP Flood:** This is similar to UDP flood and flooded a remote host with numerous ICMP Echo Requests. This type of attack can consume both outgoing and incoming bandwidth, and a high volume of ping requests will result in overall system slowdown.
- **HTTP Flood:** The attacker sends HTTP GET and POST requests to a targeted web server in a large volume that the server cannot handle and leads to denial of additional connections from legitimate clients.

2. Protocol Attacks

Protocol or network-layer DDoS attacks send large numbers of packets to targeted network infrastructures and infrastructure management tools.

It includes SYN floods, Ping of Death, fragmented packet attacks, Smurf DDoS, etc. This type of attack consumes existing server resources and other resources, such as firewalls and load balancers. The attack magnitude is measured in **Packets per Second** (PPS).

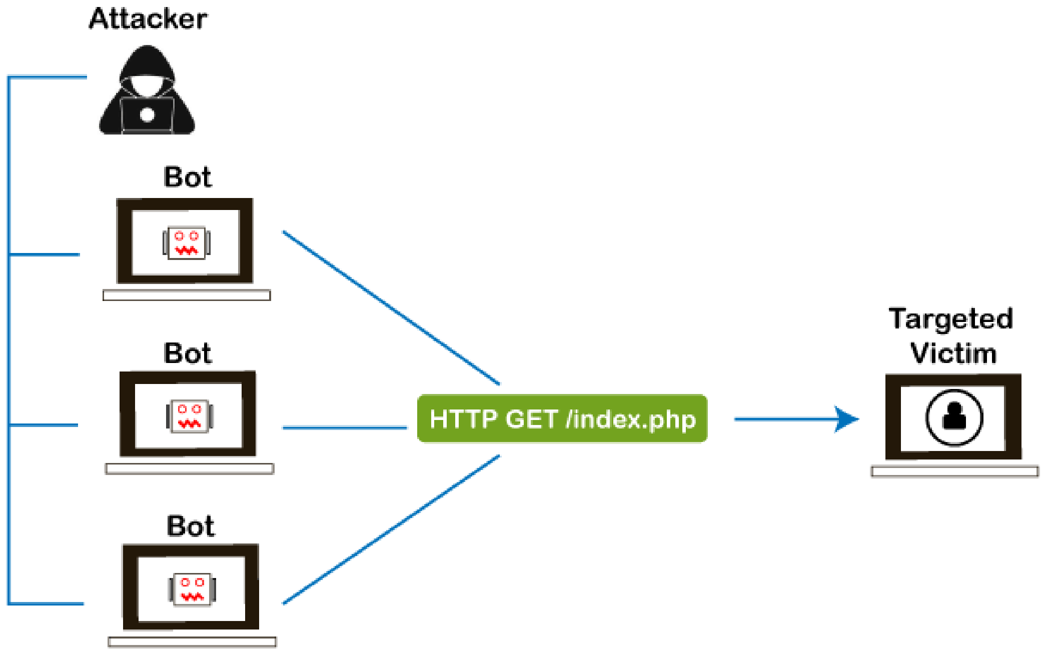


- **SYN Flood:** The attacker sends TCP connection requests faster than the targeted machine can process them, causing network saturation. Administrators can tweak TCP stacks to mitigate the effect of SYN floods. To reduce the effect of SYN floods, you can reduce the timeout until a stack frees memory allocated to a connection or selectively dropping incoming connections using a **firewall** or **iptables**.
- **DNS Flood:** DNS floods are used for attacking both the infrastructure and a DNS application to overload a target system and consume all its available network bandwidth.
- **Ping of Death:** The attacker sends malformed or oversized packets using a simple ping command. IP allows sending 65,535 bytes packets but sending a ping packet larger than 65,535 bytes violates the Internet Protocol and could cause memory overflow on the target system and finally crash the system. Many sites block ICMP ping messages altogether at their firewalls to avoid Ping of Death attacks and their variants.

3. Application Layer Attacks

Flooding applications with maliciously crafted requests conduct Application-layer attacks. The size of application-layer attacks is measured in requests per second (rps).

It includes Slowloris, Zero-day DDoS attacks, DDoS attacks that target Apache, Windows, or OpenBSD vulnerabilities, and more. Here the goal is to crash the webserver.



- **Application Attack:** This is also called Layer 7 Attack, where the attacker makes excessive log-in, database-lookup, or search requests to overload the application. It is tough to detect Layer 7 attacks because they resemble legitimate website traffic.
- **Slowloris:** The attacker sends many HTTP headers to a targeted web server but never completes a request. The targeted server keeps each of these false connections open and eventually overflows the maximum concurrent connection pool, leading to a denial of additional connections from legitimate clients.
- **NTP Amplification:** The attacker exploits publically accessible Network Time Protocol (NTP) servers to overwhelm the targeted server with User Datagram Protocol (UDP) traffic.
- **Zero-day DDoS Attacks:** Zero-day vulnerability is a system or application flaw previously unknown to the vendor and has not been fixed or patched. These are new types of attacks coming into existence day by day, such as exploiting vulnerabilities for which no patch has yet been released.

How to Fix a DDoS Attack

You must be careful while approaching and selecting a DDoS protection service provider. Many service providers want to take advantage of your situation. If you inform them that you are under a DDoS attack, they will start offering you various services at unreasonably high costs.

If you see a low magnitude of the DDoS, you can find many firewall-based solutions that can help you filter out DDoS-based traffic. If you have a high volume of DDoS attacks like in gigabits or even more, you should take the help of a DDoS protection service provider that offers a more holistic, proactive, and genuine approach.

There are quite a few DDoS protection options that you can apply depending on the type of DDoS attack.

1. Blocking vulnerable ports

Your DDoS protection starts from identifying and closing all the possible OS and application-level vulnerabilities in your system, closing all the possible ports, removing unnecessary access from the system, and hiding your server behind a proxy or CDN system.

2. Configure firewalls and routers

Firewalls and routers should be configured to reject bogus traffic, and you should keep your routers and firewalls updated with the latest security patches. These remain your initial line of defense.

Application front-end hardware integrated into the network before traffic reaches a server analyzes and screens data packets classifying the data as a priority, regular, or dangerous as they enter a system and can be used to block threatening data.

3. Consider artificial intelligence

While present defenses of advanced firewalls and intrusion detection systems are common, AI is being used to develop new systems.

The systems that can quickly route Internet traffic to the cloud, where it's analyzed, and malicious web traffic blocked before it reaches a company's computers. Such AI programs could identify and defend against known DDoS indicative patterns. Plus, the self-learning capabilities of AI would help predict and identify future DDoS patterns.

Researchers are exploring the use of blockchain, the same technology behind Bitcoin and other cryptocurrencies, to permit people to share their unused bandwidth to absorb the malicious traffic created in a DDoS attack and render it ineffective.

4. Secure IoT devices

If you have IoT devices, you should make sure your devices are formatted for maximum protection. Secure passwords should be used for all devices. IoT devices have been vulnerable to weak passwords, with many devices operating with easily discovered default passwords.

A strong firewall is also important. Protecting your devices is an essential part of Cyber Safety.

5. Application front end hardware

Application front-end hardware is intelligent hardware placed on the network before traffic reaches the servers. It can be used on networks in conjunction with routers and switches. Application front-end hardware analyzes data packets as they enter the system and then identifies them as a priority, regular, or dangerous. There are more than 25 bandwidth management vendors.

6. Blackhole and sinkhole

With **blackhole** routing, all the traffic to the attacked DNS or IP address is sent to a "black hole" (null interface or a non-existent server). It is managed by the ISP to be more efficient and avoid affecting network connectivity.

A DNS **sinkhole** routes traffic to a valid IP address which analyzes traffic and rejects bad packets. Sinkholing is not efficient for most severe attacks.

7. IPS based prevention

Intrusion prevention systems (IPS) are effective if the attacks have signatures associated with them. However, the trend among the attacks is to have legitimate content but bad intent. Intrusion-prevention systems which work on content recognition cannot block behavior-based DoS attacks.

An ASIC-based IPS may detect and block denial-of-service attacks because they have the processing power and the granularity to analyze the attacks and act like a circuit breaker in an automated way.

A rate-based IPS (RBIPS) must analyze traffic granularly and continuously monitor the traffic pattern and determine if there is a traffic anomaly. It must let the legitimate traffic flow while blocking the DoS attack traffic.

8. DDS based defense

More focused on the problem than IPS, a DoS defense system (DDS) can block connection-based DoS attacks and those with legitimate content but bad intent. A DDS can also address both protocol attacks (such as teardrop and ping of death) and rate-based attacks (such as ICMP floods and SYN floods). DDS has a purpose-built system that can quickly identify and obstruct denial of service attacks at a more incredible speed than software that is based system.

9. Switches

Most switches have some rate-limiting and ACL capability. Some switches provide automatic or system-wide rate limiting, traffic shaping, delayed binding (TCP splicing), deep packet inspection, and Bogon filtering (bogus IP filtering) to detect and remediate DoS attacks through automatic rate filtering and WAN Link failover and balancing.

These schemes will work as long as the DoS attacks can be prevented by using them. For example, SYN flood can be prevented using delayed binding or TCP splicing. Similarly, content-based DoS may be prevented using deep packet inspection. Attacks originating from dark addresses or going to dark addresses can be prevented using bogon filtering. Automatic rate filtering can work as long as set rate thresholds have been set correctly. Wan-link failover will work as long as both links have DoS/DDoS prevention mechanism.

Man-in-the-middle (MITM) Attacks

What is MITM Attack

A MITM attack is a form of cyber-attack where a user is introduced with some kind of meeting between the two parties by a malicious individual, manipulates both parties and achieves access to the data that the two people were trying to deliver to each other. A man-in-the-middle attack also helps a malicious attacker, without any kind of participant recognizing till it's too late, to hack the transmission of data intended for someone else and not supposed to be sent at all. In certain aspects, like MITM, MitM, MiM or MIM, MITM attacks can be referred.

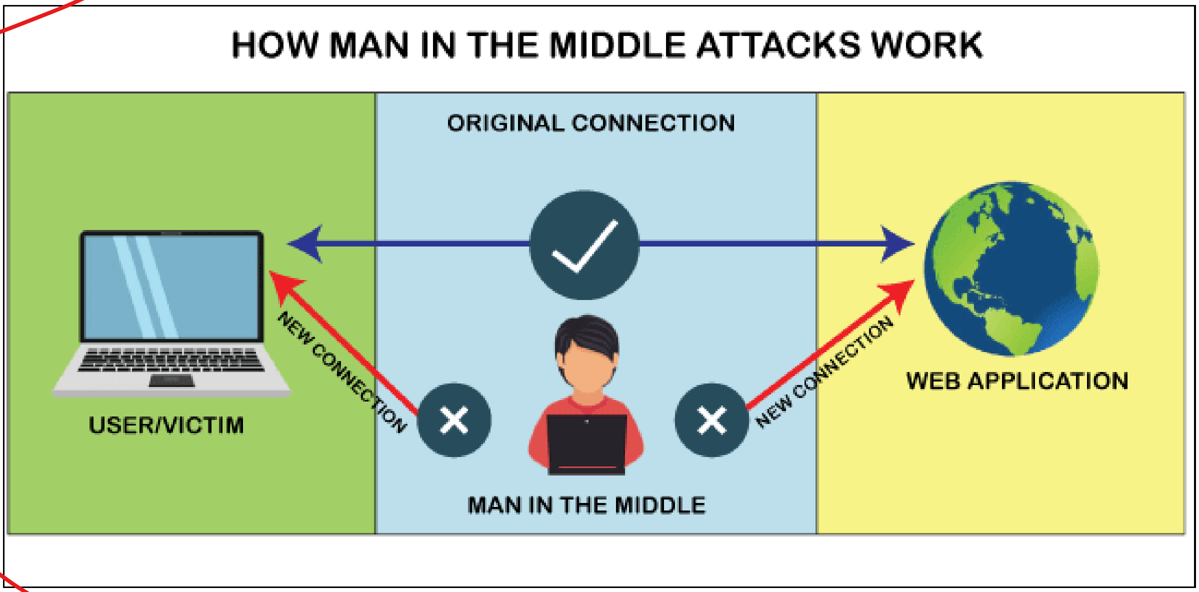
If an attacker puts himself between a client and a webpage, a Man-in-the-Middle (MITM) attack occurs. This form of assault comes in many different ways.

For example, In order to intercept financial login credentials, a fraudulent banking website can be used. Between the user and the real bank webpage, the fake site lies "in the middle."

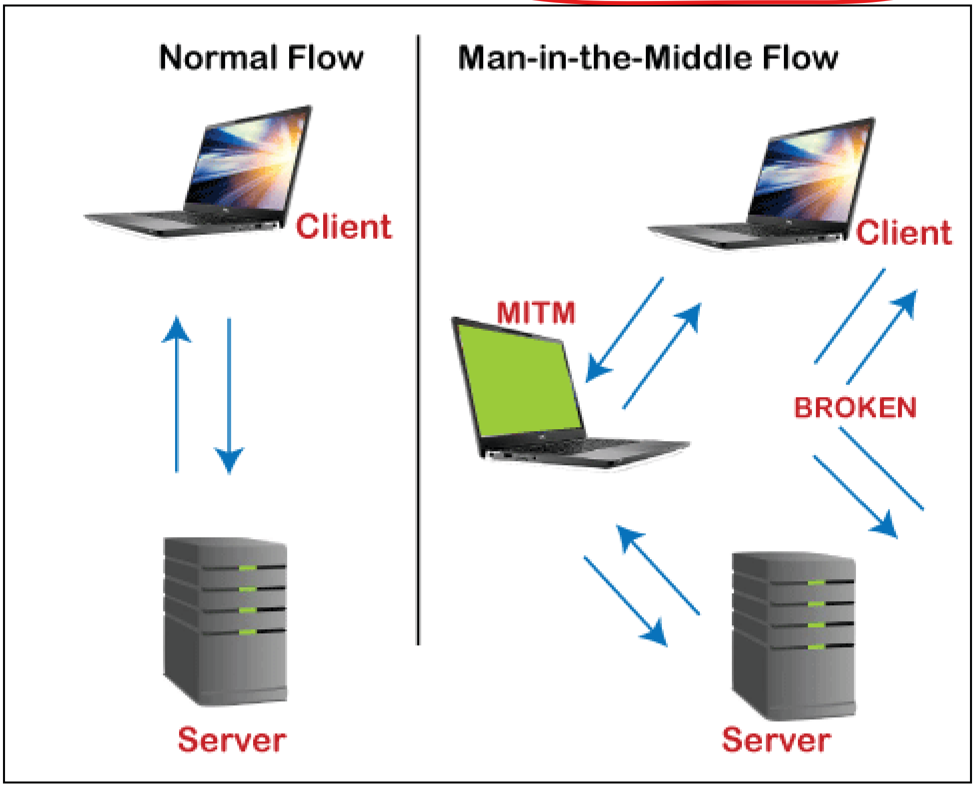
How does MITM work

There are several reasons and strategies for hackers to use a MITM attack. Usually, like credit card numbers or user login details, they try to access anything. They also spy on private meetings, which may include corporate secrets or other useful information.

The feature that almost every attack has, in general, is that the attacker pretends to be somebody you trust (or a webpage).

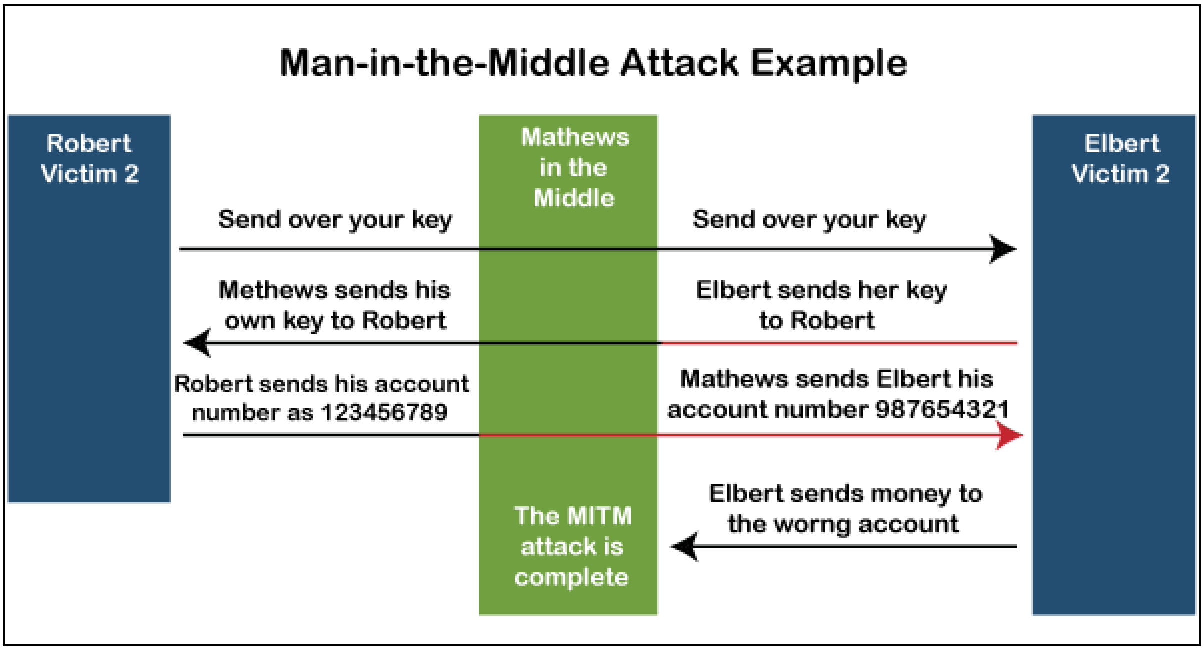


Real life Instances of MITM attack



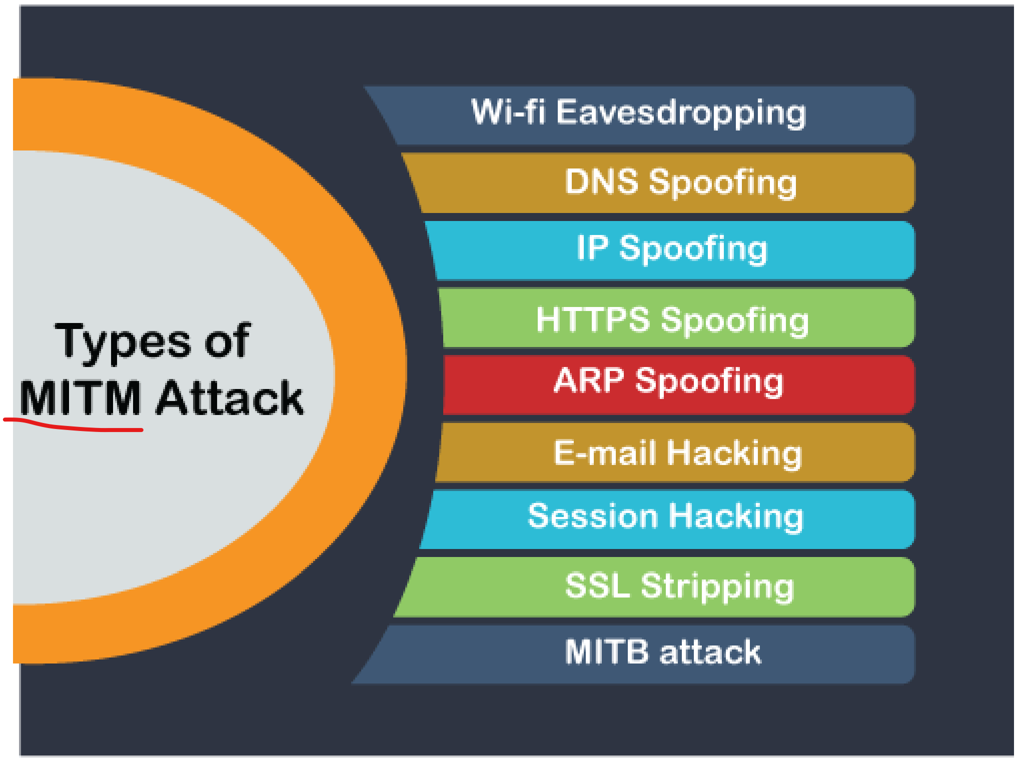
In the above diagram, you can see that the intruder positioned himself in between the client and server to intercept the confidential data or manipulate the incorrect information of them.

Another Instance of MITM attack


Man-in-the-Middle Attack Example
Robert Victim 2
Mathews in the Middle
Elbert Victim 2
Send over your key
Send over your key
Methews sends his own key to Robert
Elbert sends her key to Robert
Robert sends his account number as 123456789
Mathews sends Elbert his account number 987654321
The MITM attack is complete
Elbert sends money to the worng account

As shown in the above picture, to obtain access to banking, the attacker is trying to imitate both sides of the discussion. This instance is accurate for the client and the server discussions and also person-to-person discussions. Shown in this instance, the attacker retrieves a public key and can modulate his own passwords to manipulate the audience to accept that they are safely communicating with each other at either end.

Types of MITM Attack



- **Wi-fi Eavesdropping**
- **DNS Spoofing**
- **IP Spoofing**
- **HTTPS Spoofing**
- **ARP Spoofing**
- **E-mail Hacking**
- **Session Hacking**
- **SSL Stripping**
- **MITB attack**

Here, we have explained the above concepts, one by one in detail.

Wi-fi Eavesdropping

You may have seen a notification that suggests, "This connection is not safe," if you've used a device in a cafe. Public wi-fi is typically offer "as-is," without any promises of service quality.

The unencrypted wi-fi networks are easy to watch. Although, it's just like having a debate in a public place-anybody can join in. You can limit your access by setting your computer to "public," which disables Network Discovery. This avoids other users on the network from exploiting the system.

Some other Wi-Fi snooping attack occurs when an attacker establishes his own "Evil Twin" wi-fi hotspot. Attacker make the link, through the network Address and passwords, appear identical to the real ones. Users will link to the "evil twin" unintentionally or automatically, enabling the attacker to intrude about their actions.

DNS Spoofing

The Site operates with numeric IP addresses like 192.156.65.118 is one of Google's addresses.

For example, a server is used by several sites to interpret the address to a recognizable title: google.com. A DNS server, or DNS, is the server that transforms 192.156.65.118 to google.com.

A fraudulent Web server can be developed by an attacker. The fraudulent server transports a specific web address to a unique IP address, which is termed as "spoofing."

IP Spoofing

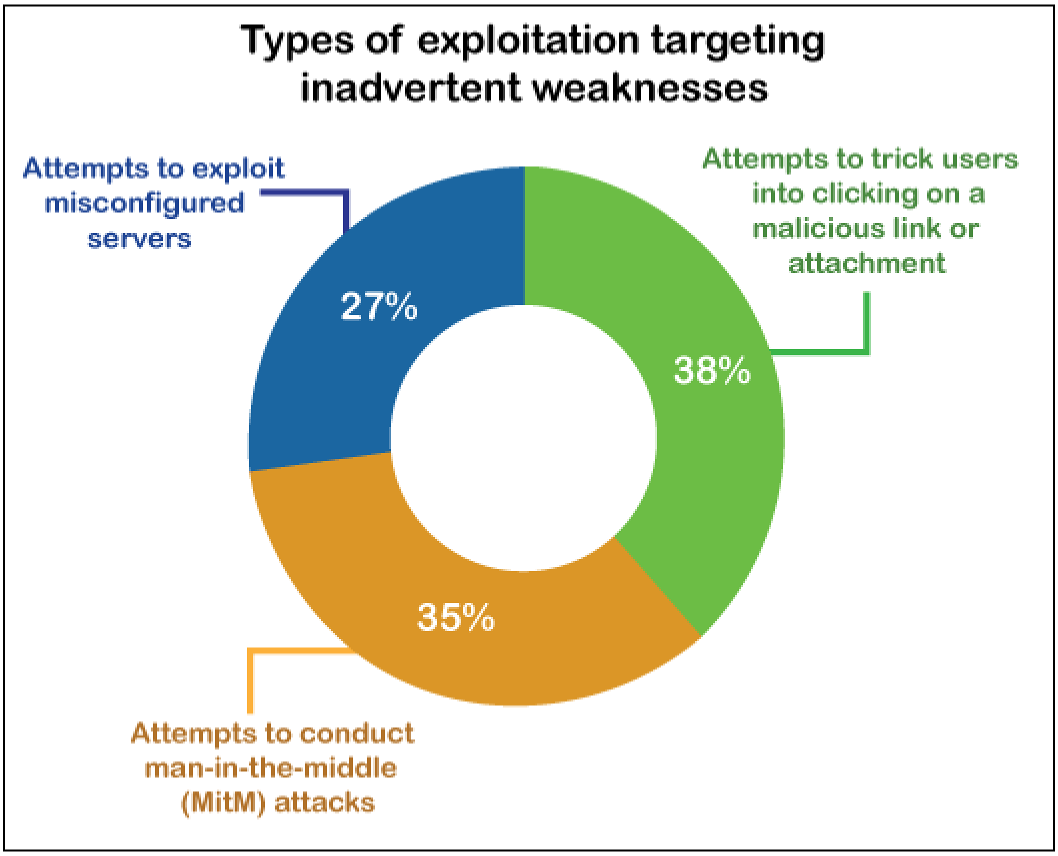
Many devices connected to the same network contains an IP address, as we all know. Each device is equipped with its IP address in several enterprise internal web networks. In IP spoofing, the attackers imitate an approved console's IP address. For a network, it appears just as the system is authorized.

It might be causing a network to be exploited by unauthorized access. They must stay quiet and track the actions, or a Denial of Service (DoS) attack may also be released. In a Middle-in-the-man attack, IP spoofing may also be used by placing between two devices.

For Example, Device A and device B assume that they communicate with each other, but both are intercepted and communicated to the attacker.

Device A= = = = Attacker= = = = Device B

35 percent of the intrusion operations include hackers conducting MITM exploits, as per the IBM X-Force 's Threat Intelligence 2018 Reports. It is represented in below Pie chart.



HTTPS Spoofing

Duplicating an HTTPS webpage is not currently possible.

A theoretical approach for circumventing HTTPS, however, has been illustrated by cybersecurity experts. The attacker creates an authoritative address.

It uses letters of international alphabets rather than standard scripts. This acts as phishing emails with unusual characters that you might have used. Rolex may be written Rólex, for example.

ARP Spoofing

ARP refers to the Protocol on Address Resolution.

An ARP request is sent out by a client, and an attacker produces a fraudulent response. The attacker is like a computer modem in this situation, which enables the attacker to access the traffic flow. Usually, this is restricted to local area networks (LAN) that use the ARP protocol.

E-mail Hacking

An attacker exploits the email system of a user in a such a kind of cybersecurity intrusion. The intruder also watches quietly, collecting data and eavesdropping on the discussion via email. The Attackers may have a scan pattern that searches for targeted keywords, such as "financial" or "hidden Democratic policies."

Through Social Engineering, email hacking operates perfectly. To imitate an online friend, the attackers might use relevant data from some kind of hijacked email address. Spear-phishing can also be used to trick a user into downloading malicious apps.

Session Hacking

Usually, this form of MITM attack is often used to hack social media platforms. The webpage contains a "session browser cookie" on the victim's machine for most social media platforms. If the person steps off, this cookie is disproved. But when the session is running, the cookie offers identity, exposure, and monitoring data.

A Session Hijack happens when a configuration cookie is stolen by an intruder. Unless the victim's account is hacked with malware or application attackers, it can arise. It can occur if a user exploits an XSS cross-scripting intrusion, in which the hacker injects malicious script into a site that is commonly visited.

SSL Stripping

SSL refers to Secure Socket Layer. SSL is the security standard used if you see https:/ next to a website address, not http:/. The attacker accesses and routes data packets from a user using SSL Stripping:

User = = = = Encrypted website User = = = = Authenticated website

The user tries to link to a website that is secured. In the account of the client, the attacker encrypts and links to the secured website. Usually, a fake design is developed by the attacker to present it to the customer. The victim thinks that they have signed on to the normal website, but actually they signed in to a hacker's website. The attacker does have the SSL certificate "stripped" from the data connection of the victim.

MITB attack

This is a form of attack that leverages internet browser security flaws.

The malicious attacks will be trojans, desktop worms, Java vulnerabilities, SQL injection attacks, and web browsing add-ons. These are commonly used to collect financial information.

Malware steals their passwords as the user signs in to their bank account. In certain instances, malware scripts may move money and then alter the receipt of the transaction to conceal the transaction.

Detection of Man-in-the-middle attack

It is harder to identify a MITM attack without taking the appropriate measures. A Man-in-the-middle assault will theoretically proceed unchecked till it's too late when you do not consciously need to evaluate if your interactions have been monitored. Usually, the main technique for identifying a potential-attacks are always searching for adequate page authorization and introducing some kind of temper authentication; however, these approaches may need further forensic investigation after-the-fact.

Instead of trying to identify attacks when they are operational, it is necessary to manage precautionary measures to avoid MITM attacks whenever they occur. To sustain a safe environment, being mindful of your surfing habits and identifying possibly hazardous environments can be important.

Preventions of Man-in-the-middle attack

Here, we have discussed some prevention techniques to avoid the interactions being compromised by MITM attacks.

1. Wireless access point (WAP) Encryption

Creating a strong protection feature on access points eliminates legitimate access just from being closer from accessing the system. A vulnerable system of protection will enable an intruder to brute-force his way into the system and start attacking the MITM.

2. Use a VPN

- **Use a Virtual Private Network (VPN)**
  To encrypt your web traffic, an encrypted VPN severely limits a hacker's ability to read or modify web traffic.
  Be prepared to prevent data loss; have a cybersecurity incident response plan.
- **Network Security**
  Secure your network with an intrusion detection system. Network administrators should be using good network hygiene to mitigate a man-in-the-middle attack. Analyze traffic patterns to identify unusual behavior.

3. Public Key Pair Authentication

MITM attacks normally include something or another being spoofed. In different layers of the protocol stack, public key pair authentication such as RSA is used to ensure that the objects you communicate with that are essentially the objects you want to communicate with.

4. Strong Network User Credentials

Ensuring that the primary email login is modified is extremely important. Not only the login credentials for Wi-Fi but the password hashes for your router. When a hacker detects the wireless router login details, they can switch the fraudulent servers to the DNS servers. Or, at worst, hack the modem with harmful malware.

5. Communication security

Communication security help the users to protect from unauthorized messages and provides secure data encryption.

Enabling two-factor authentication is the most powerful way to avoid account hacking. It implies that you'll have to give another protection factor, in contrast with your login credentials. One instance is the conjunction of a login credential and a text to your device from Gmail.

6. Using proper hygiene for network protection on all platforms, such as smartphone apps.

- Since phishing emails are the most popular attack vector when lookout a spam email. Analyze the references cautiously before opening.
- Just mount plug-ins for the browser from trusted sources.
- Reduce the chance of exploits to disprove persistent cookies by logging out inactive accounts.
- Avoid what you're doing and execute a security scan if you anticipate a secure link but do not have one.

7. Avoid using public wi-fi

Configure your phone to require a manual link if you're using public wi-fi.

It can be hard to identify MITM attacks as they are occurring. The easiest way to remain secure is to regularly incorporate all of the above prevention for security.

Be conscious that such attacks are a part of social engineering. Take a couple of minutes to dig deeper if anything doesn't seem normal about social media and email.