Network-Based Cyber Attacks

Network-based attacks are attacks designed to compromise network security by either eavesdropping on or intercepting and manipulating network traffic. These may be active attacks, wherein the hacker manipulates network activity in real-time; or passive attacks, wherein the attacker sees network activity but does not attempt to modify it.

There are different types of Network- Based attacks:

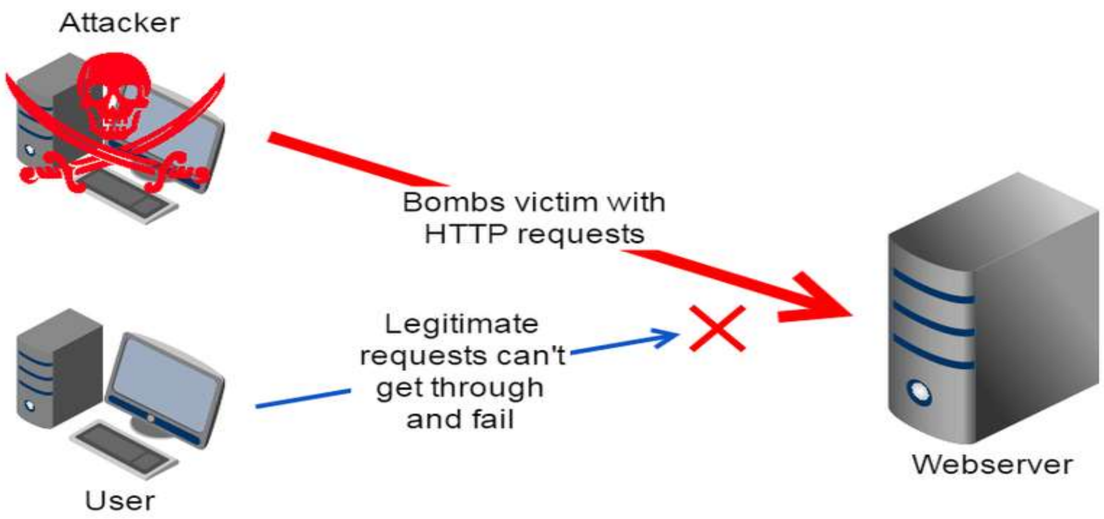
1. DOS
2. DDOS
3. ICMP Flood Attack
4. SYN Flood Attack
5. Smurf Attack
6. Man in the Middle attack
7. Spoofing
8. ARP Spoofing
9. DNS Spoofing
10. Sniffing

DOS Attack

A Denial-of-Service (DOS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DOS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

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.


Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
Webserver
User

DDOS Attack

Distributed Denial-of-Service {DDOS) is a type of attack where multiple systems are used to launch DOS attack on one targeted system. Usually DDOS are result of multiple compromised systems (called Botnet's)

How DDOS IS Carried?

1. DDOS attacks are carried out with networks of Internet-connected machines.
2. These networks consist of computers and other devices (such as IOT devices)which 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.
3. Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.
4. When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic. Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

How Botnet are used in DDOS

1. Attackers can use flaws or malware to install C2 software on user's systems to create a botnet

2. Once the botnet is ready, the attackers send the start command to all their botnet nodes.

3. The botnet will then send its programmed requests to the target server

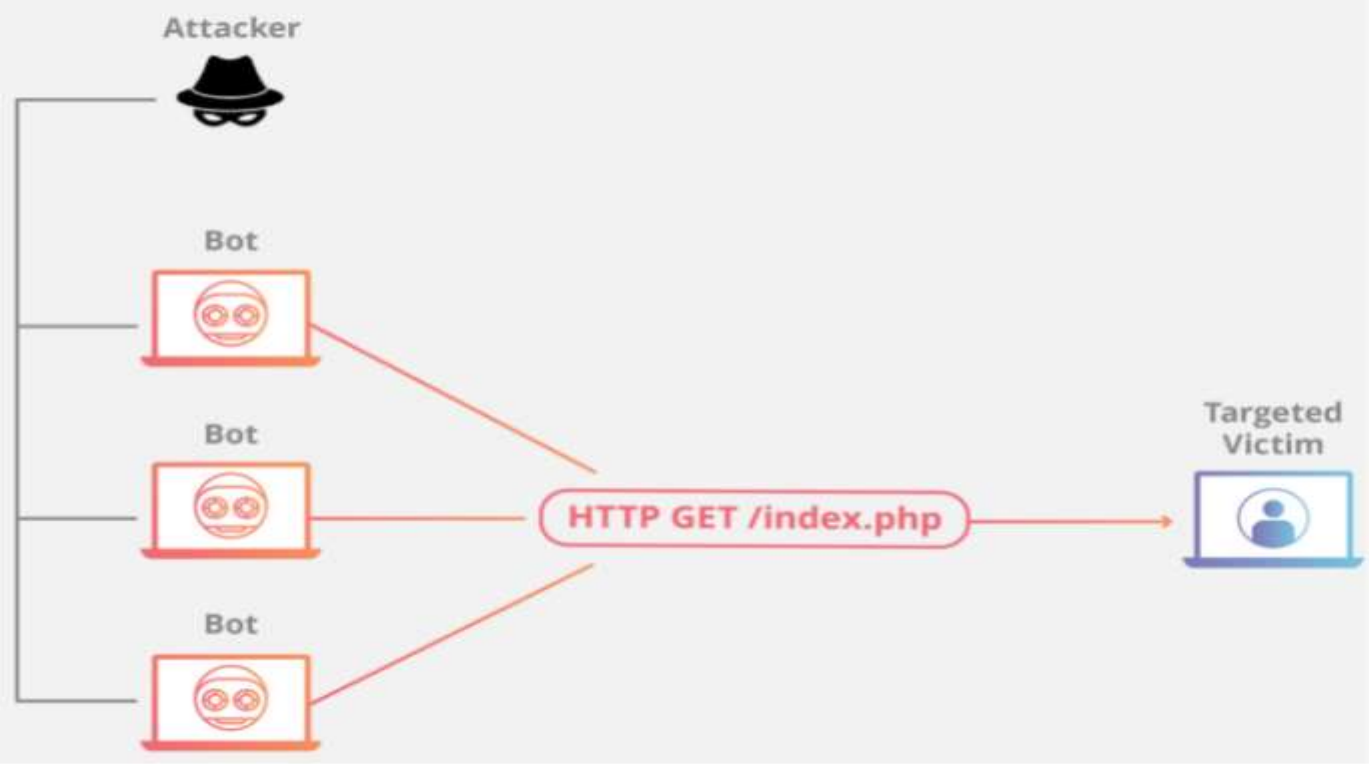
4. If the attack makes it past the outer defenses, it quickly overwhelms most systems.

5. It usually causes service outages, and in some cases, crashes the server.

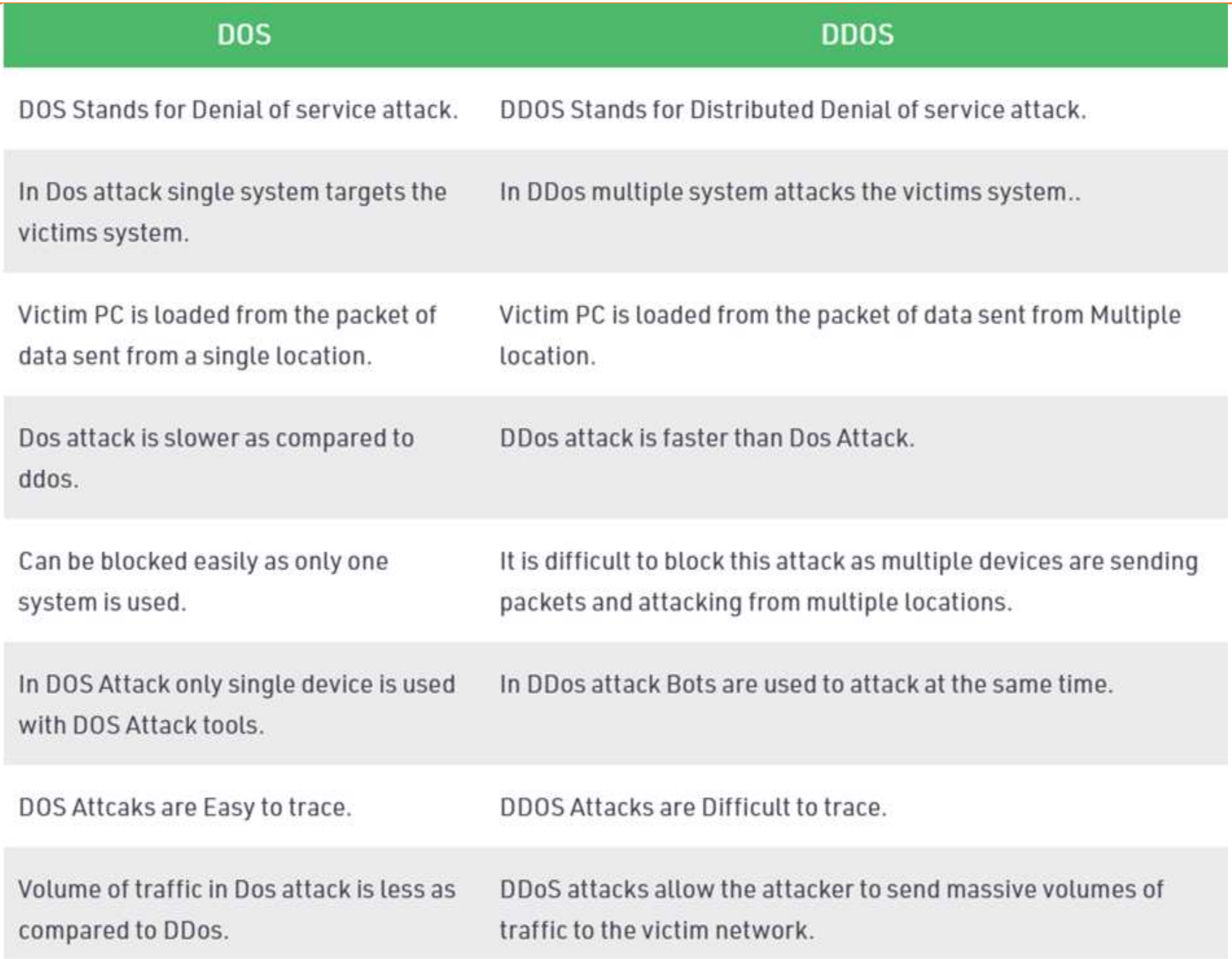
6. This causes a loss in productivity or service interruption.

Mitigation for DOS and DDOS:

1. Use Anti-DDOS technology (like Arbor)
2. Rate limit (limit the number of connections from an IP or User)
3. Reduce connection wait time.
4. Deploy load balancers



Difference between DOS & DDOS



DOS	DDOS
DOS Stands for Denial of service attack.	DDOS Stands for Distributed Denial of service attack.
In Dos attack single system targets the victims system.	In DDos multiple system 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 Bots are used to attack at the same time.
DOS Attcaks are Easy to trace.	DDOS Attacks are Difficult to trace.
Volume of traffic in Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.

ICMP flood

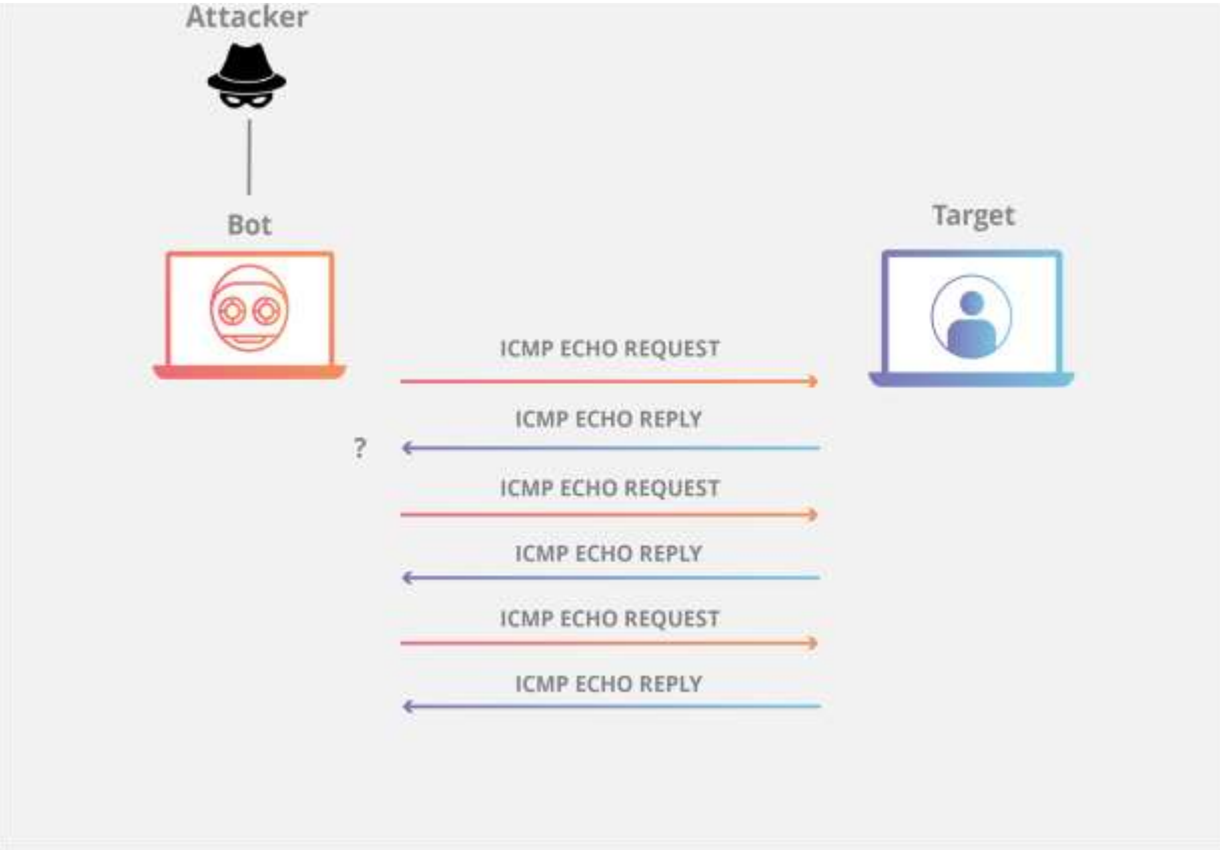
Ping flood, also known as ICMP flood, is a common Denial of Service (DoS) attack in which an attacker takes down a victim's computer by overwhelming it with ICMP echo requests, also known as pings.

The attack involves flooding the victim's network with request packets, knowing that the network will respond with an equal number of reply packets.

Additional methods for bringing down a target with ICMP requests include the use of custom tools or code, such as hping and scapy.

Mitigations:

1. Use Anti-DDO S technology (like Arbor)
2. Rate limit (limit the number of connections from an IPorUser)
3. Reduce connection wait time
4. Deploy load balancers



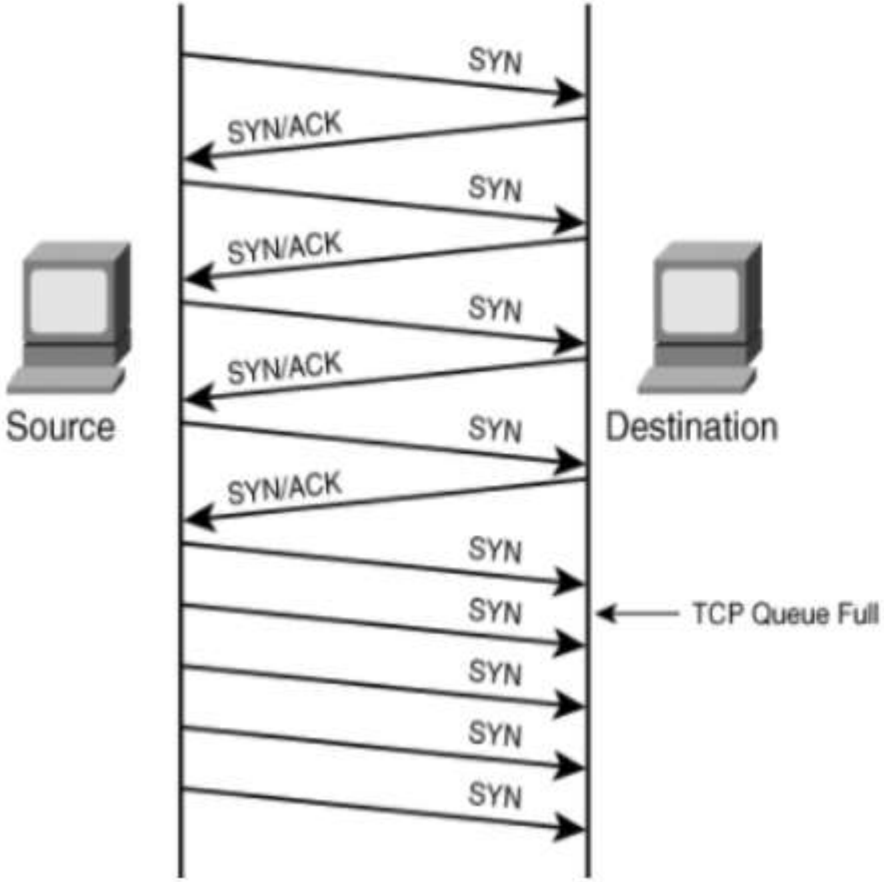
SYN flood

SYN Flood attack is a type of DOS attack where it exploits the normal TCP three-way handshake.

The attacker send huge connection requests (SYN) but never sends an acknowledge back to the sever. This will make the server wait for certain time and hold the connection. This will consume all the concurrent connections on the target server making it inaccessible for legit users.

Mitigations:

1. Use Anti-DDO S technology (like Arbor)
2. Rate limit (limit the number of connections from an IP or User)
3. Reduce connection wait time
4. Deploy load balancers



Smurf attack

A Smurf attack is a distributed denial-of-service (DDoS) attack in which an attacker attempts to flood a targeted server with Internet Control Message Protocol (ICMP) packets. By making requests with the spoofed IP address of the targeted device to one or more computer networks, the computer networks then respond to the targeted server, amplifying the initial attack traffic and potentially overwhelming the target, rendering it inaccessible.

Mitigations:

1. Use Anti-DDOS technology (like Arbor)

2. Rate limit (limit the number of connections from an IP or User)

3. Reduce connection wait time

4. Deploy load balancers

Man-in-the-Middle Attack

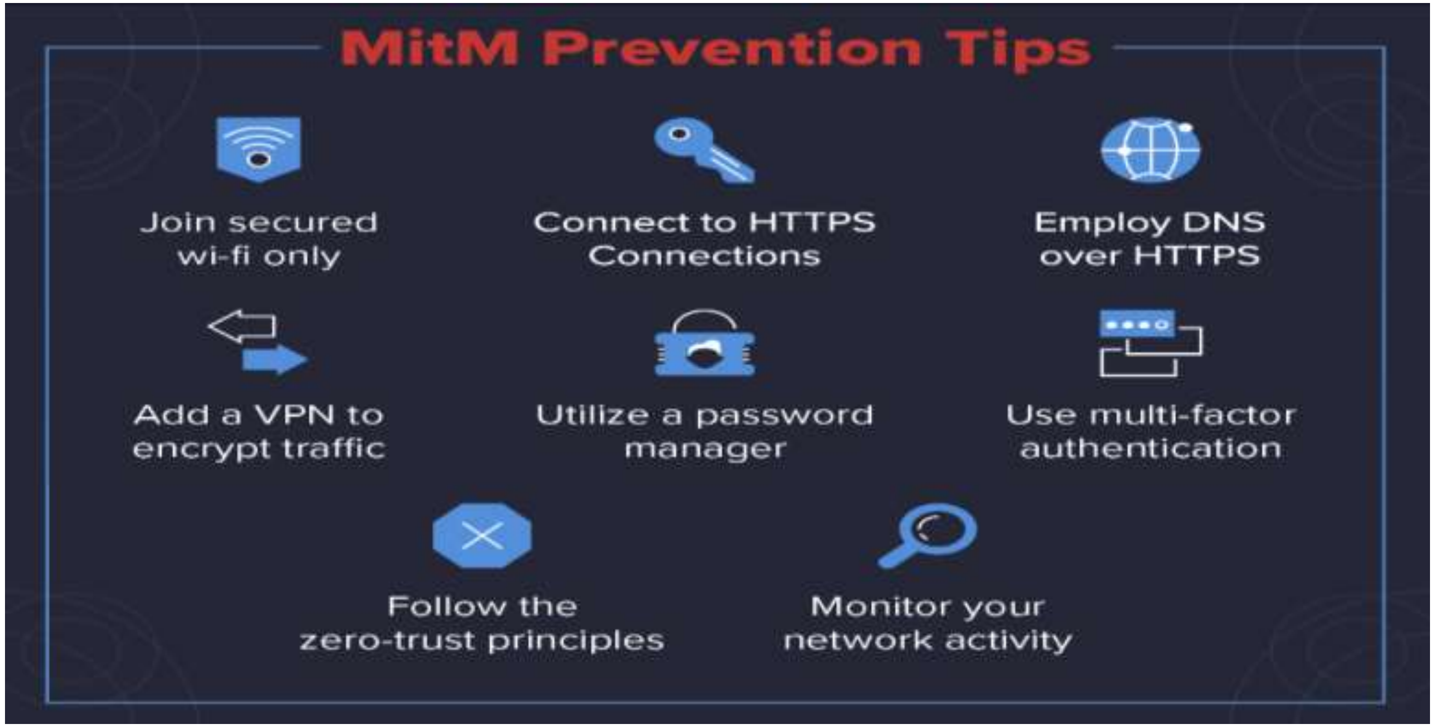
- Man-in-the-Middle is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.
- A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.
- The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.
- Information obtained during an attack could be used for many purposes, including identity theft, unapproved fund transfers or an illicit password change.

Mitigations:

1. Use Static ARP (to prevent ARP poisoning)

2. Use Encryption (prevent the attacker from leveraging the data)

3. IPS system (can detect sudden change in the network performance)



MitM Prevention Tips

Join secured wi-fi only

Connect to HTTPS Connections

Employ DNS over HTTPS

Add a VPN to encrypt traffic

Utilize a password manager

Use multi-factor authentication

Follow the zero-trust principles

Monitor your network activity

Spoofing

- Spoofing is a cyber attack that occurs when a scammer is disguised as a trusted source to gain access to important data or information. Spoofing can happen through websites, emails, phone calls, texts, IP addresses and servers.
- These attacks are carried out when someone(or something) try to introduce himself as another person (or another object), this called spoofing. (Changing person’s identity)
- Usually, the main goal of spoofing is to access personal information, steal money, bypass network access controls or spread malware through infected attachments or links. With every form of communication online, scammers will try to use spoofing to try to steal your identity and assets.

Mitigations:

1. Use authentication based on key exchange
2. Enable encryption sessions

3 . Implement filtering of both inbound and outbound traffic.

4. Enable port level security (ARP and MAC Address Spoofing)

5. Educate Users (Spoofing techniques)

6. Deploy IPS (IP Spoofing)

ARP Spoofing (ARP Cache Poisoning)

ARP (Address Resolution Protocol) translates between the physical address of an Internet device (MAC address – media access control) and the IP address assigned to it on the local area network. An attacker who uses ARP spoofing tries to inject false information onto the local area network to redirect connections to their device.

ARP poisoning is when an attacker sends falsified ARP messages over a local area network (LAN) to link an attacker's MAC address with the IP address of a legitimate computer or server on the network

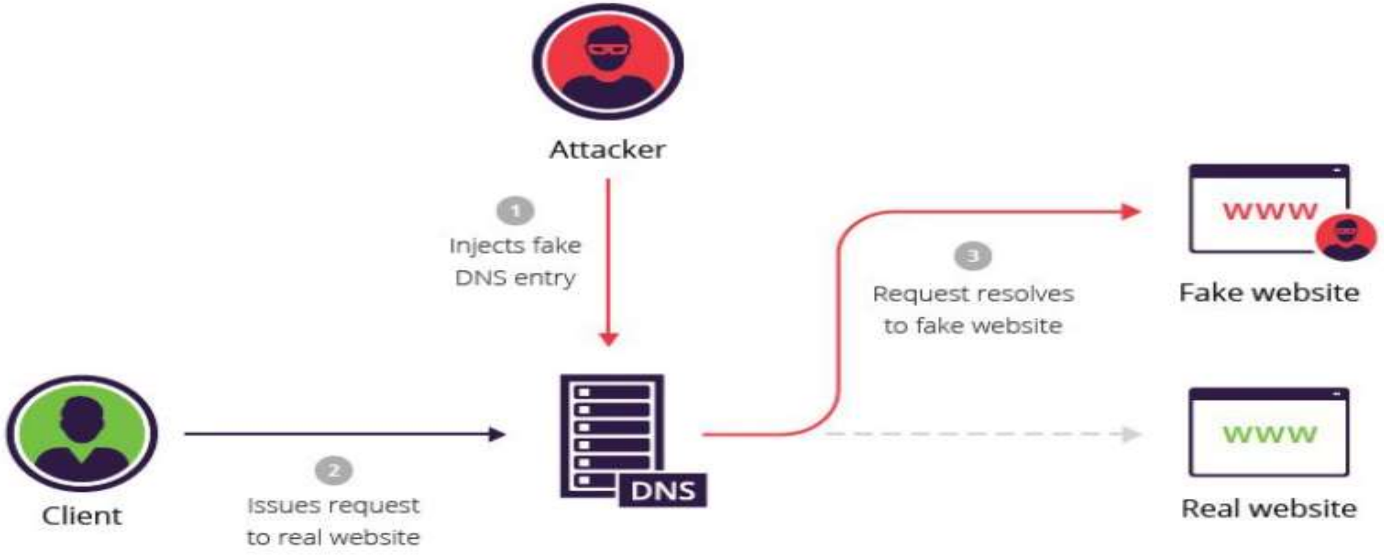
Mitigations:

1. Use Static ARP
2. Detect ARP poisoning using tools like XARP
3. Set up Packet filtering
4. Install AV and keep signatures updated

DNS Spoofing (DNS Cache Poisoning)

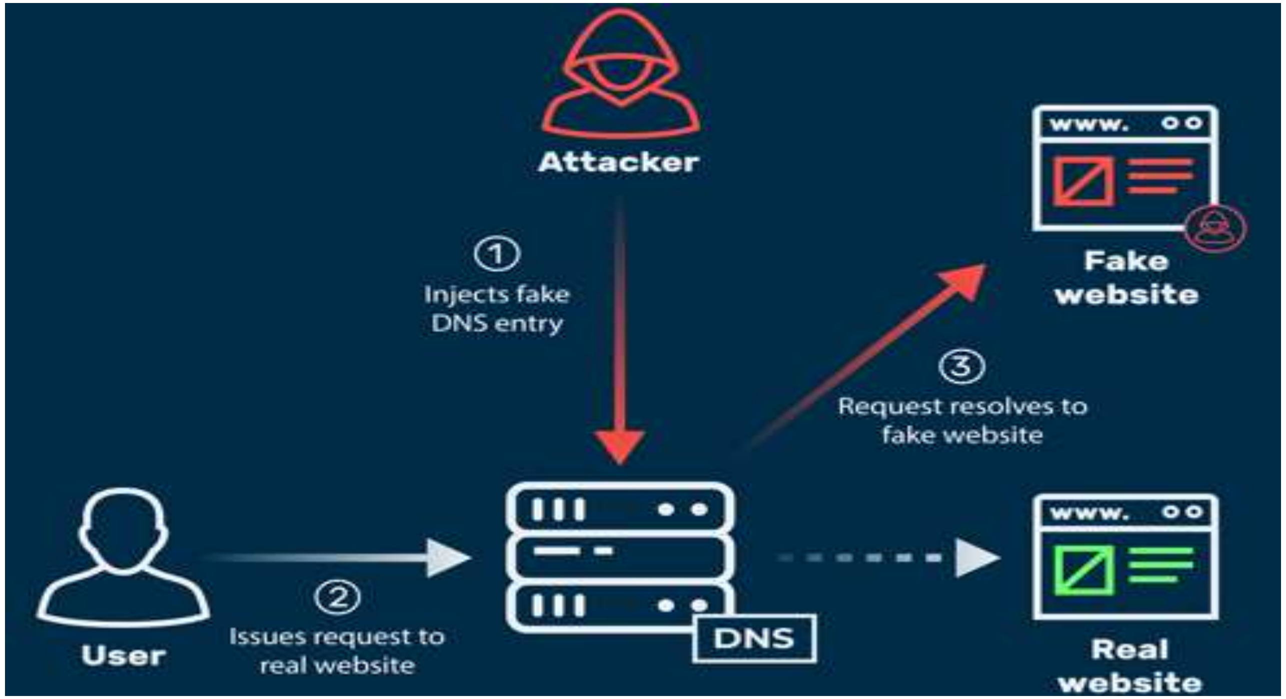
Domain Name System (DNS) spoofing is a technique that tricks a user to a bogus website rather than the real one the user intends to visit. The website will appear to be the real one and you may think you're visiting a safe, trusted website when you're actually interacting with a fraudster. The attacker's goal is to divert traffic from the real site or capture user login credentials and other data.

DNS spoofing is done by replacing the IP addresses stored in the DNS server with the ones under the control of the attacker so, whenever a user tries to access a particular website, they get directed to the malicious website placed by the attacker in the spoofed DNS server.



Mitigations for Spoofing and its Types:

1. Regularly audit DNS Zones
2. Keeping DNS Servers up-to-date.
3. Restrict Zone Transfers
4. Limit recursive queries.
5. Store only data related to the requested domain.



Sniffing

- Sniffing corresponds to theft or interception of data by capturing the network traffic when it flows through a computer network.
- A sniffing attack involves an attacker getting into the network data-stream and reading, monitoring or capturing full packets of data flowing between a client and a server. A hacker intercepting a network packet containing unencrypted information can cause severe damage to the organization or entity that owns the data.
- Data compromised may include sensitive information like account credentials, bank details, and different kinds of Personally Identifiable Information (PII). Sniffing attacks can either be active (involving both data access and manipulation) or passive (where the attacker only sees the information but does not actively interfere in its transmission).
- Examples of tools used for sniffing attacks are Wireshark, tcpdump, dSniff and Debookee.

Mitigations:

- Install a strong antivirus tool
- Encrypt your data with a VPN
- Don’t visit unencrypted websites
- Stay off public Wi-Fi
- Don’t use unencrypted messaging apps

Visit the below link to know more about Password Sniffing using Wireshark

https://www.guru99.com/wireshark-passwords-sniffer.html