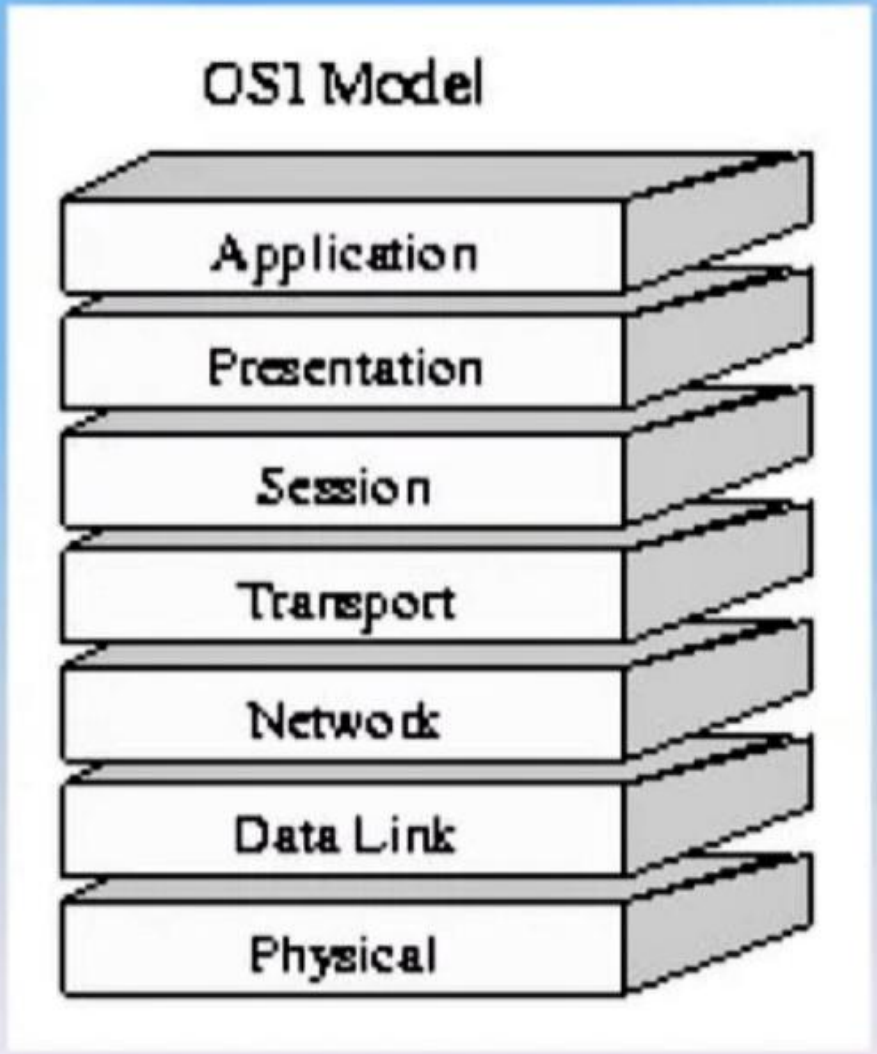

IP SPOOFING

Overview

- ISO-OSI Model
- Network Layer
- History of IP
- IP spoofing
- How IP Spoofing works?
- Types of IP spoofing attack
    - Blind spoofing
    - Non blind spoofing
    - Man in the middle
    - Dos attack

- Why spoofing is easy
- Misconception of IP spoofing
- Detection of IP spoofing
- Prevention of IP spoofing
- Is IP Spoofing a real risk?
- Conclusion

ISO-OSI Model



Network Layer

- The network layer is the third level of the Open Systems Interconnection Model (OSI Model) and it is the layer that provides data routing paths for network communication.
- The network layer is considered the backbone of the OSI Model.
- Network layer protocols exist in every host or router. The router examines the header fields of all the IP packets that pass through it.
- Internet Protocol and Netware IPX/SPX are the most common protocols associated with the network layer

Internet Protocol

History of IP

- Its development began in 1974, led by computer scientists Bob Kahn and Vint Cerf
- It is frequently used in conjunction with the Transmission Control Protocol, or TCP.
- The first major version of the Internet Protocol was version 4, or IPv4.
- The successor to IPv4 is IPv6, which was formalized by the IETF in 1998. It was designed to eventually replace IPv4.

IP spoofing

- **IP Spoofing is a technique used to gain unauthorized access to machines.**

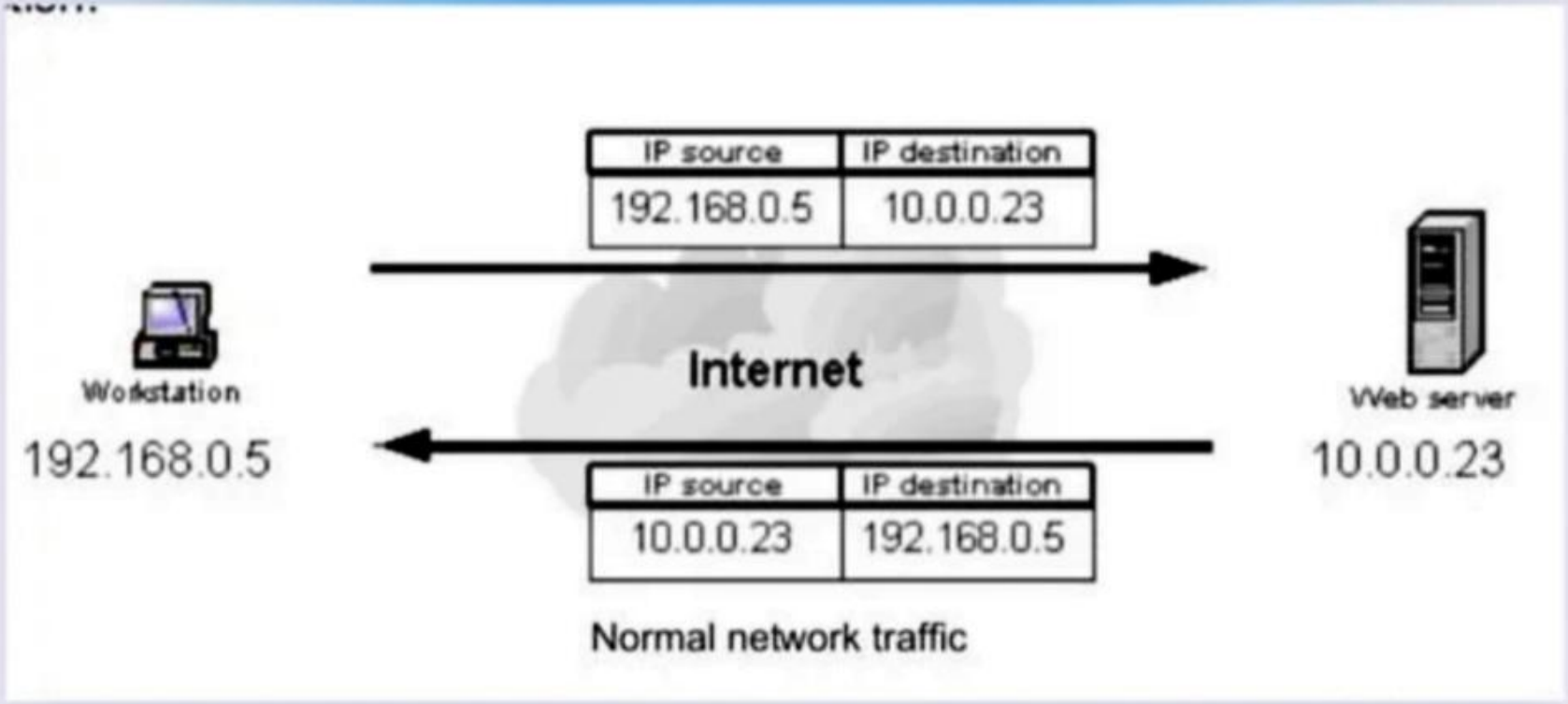
It involves the creation of Internet Protocol (IP) packets which have a modified source address

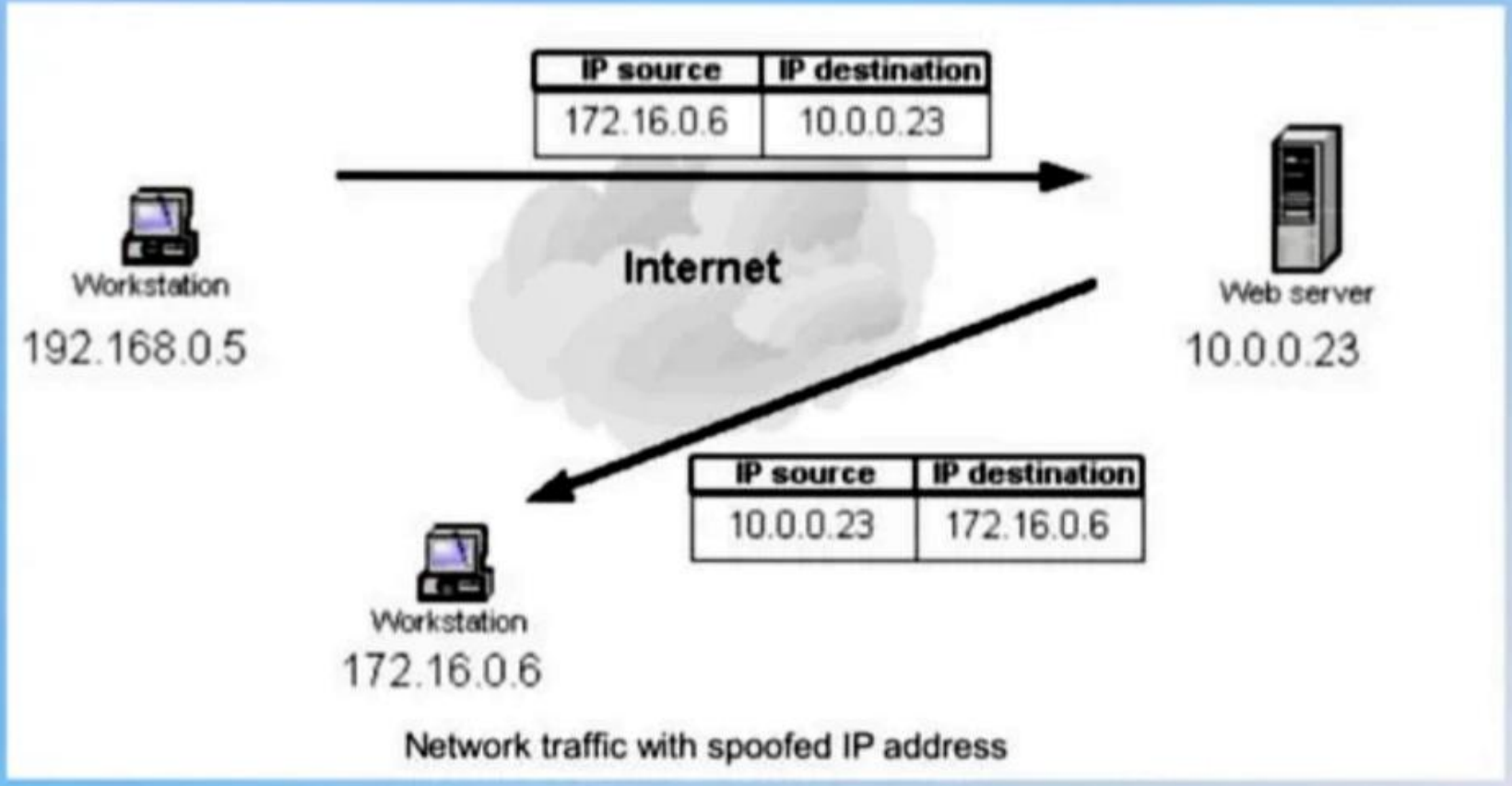
IP spoofing is also called IP address forgery or host file hijack.

- At first, the hacker needs to find the IP address of a trusted host and then modify the headers of the packets which are being sent, so that it appears to the computer that the packets are coming from that trusted host.

- It involves modifying the packet header with a forged (spoofed) source IP address, a checksum, and the order value.

How does IP spoofing works?





Network traffic with spoofed IP address

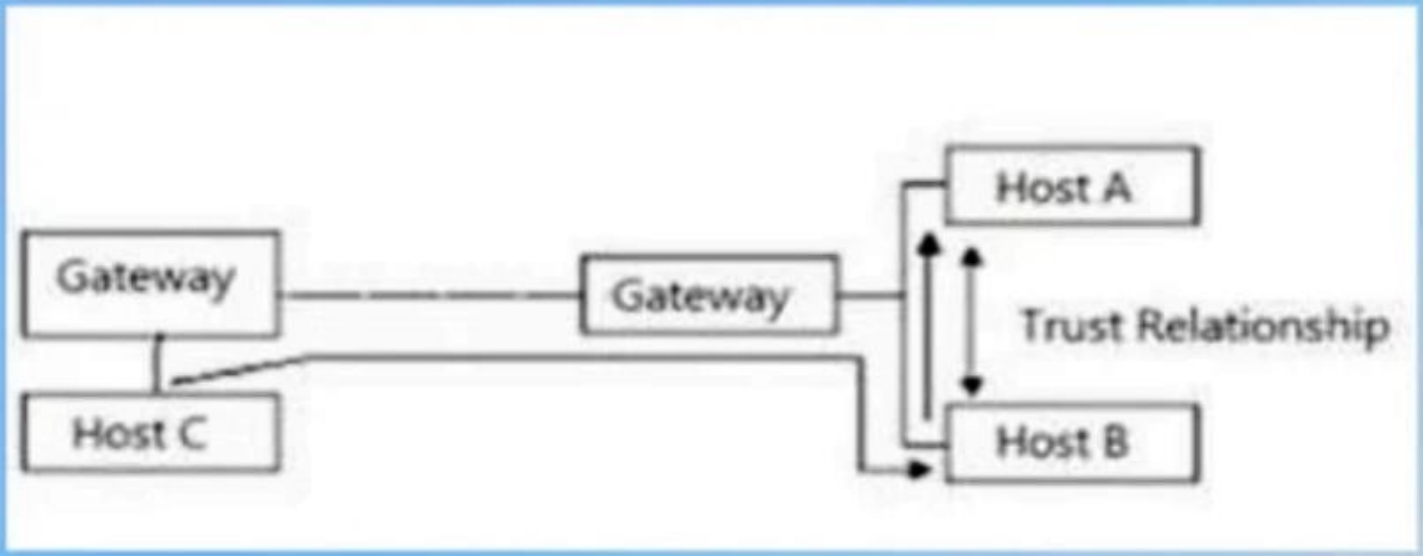
Types of IP spoofing Attacks

- The IP spoofing can further cause various attacks. These attacks can be caused by the IP spoofing.

1) Blind Spoofing
2) Non-Blind Spoofing
3) Denial-of-service attack
4) Man-in-the-middle attack

Blind spoofing

- Blind spoofing occurs when the attacker is not on the same subnet as the destination
- This is a more sophisticated attack, because the sequence and acknowledgement numbers are unreachable.
- the attacker transmits multiple packets to his intended target to receive a series sequence of numbers
- Now the attacker can inject data into the stream of packets without having authenticated himself when the connection was first established.



- **Usually,the attacker does not have access to reply and abuses trust relationship between host.**

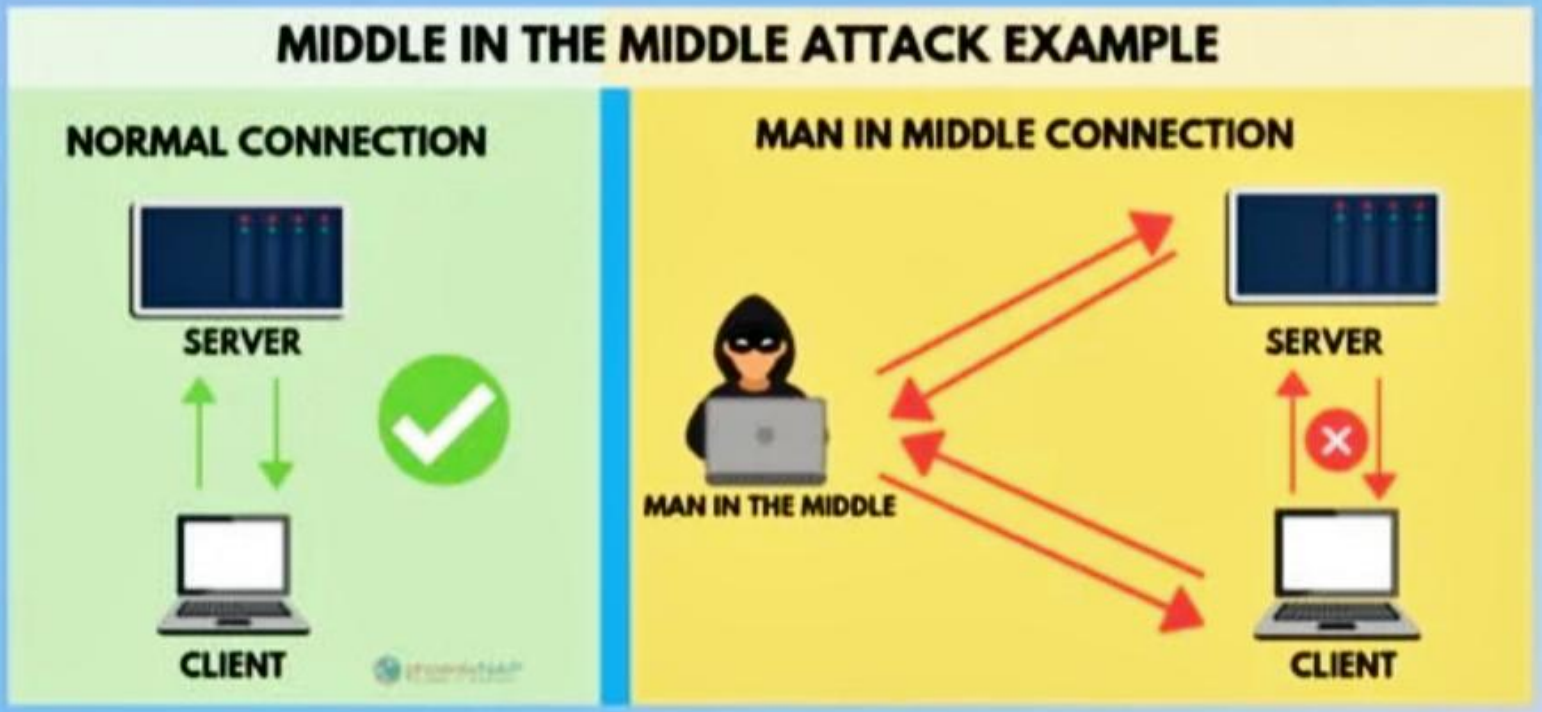
for ex:here Host C sends an IP datagram with the address of some other host(Host A) as the source address to host B.Attacked host(B) replies to legitimate host(A)

Non Blind Spoofing

- This attack takes place when the attacker is on the same subnet as the target that could see sequence and acknowledgement of packets.
- Using the spoofing to interfere with a connection that sends packets along your subnet.

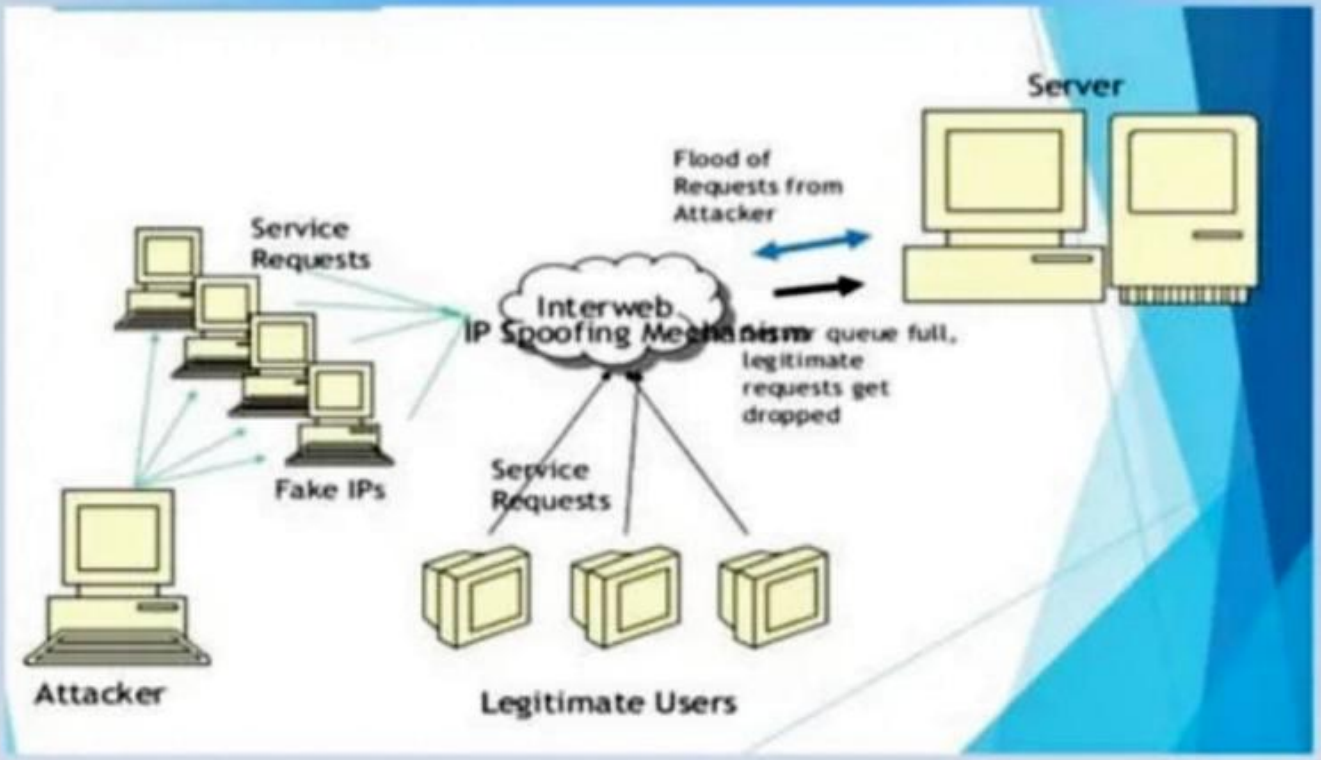
Man in the Middle

- In these attacks, a malicious party intercepts a legitimate communication between two friendly parties.
- The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient.
- In this way, an attacker can fool a victim into disclosing confidential information by "spoofing" the identity of the original sender.



This is also called connection hijacking.

Denial of Service



- **A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.**
- **In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return address.**

Why IP Spoofing is easy?

- Problem with the Routers.
- Routers look at Destination addresses only.
- Authentication based on Destination addresses only.
- To change source address field in IP header field is easy.

Misconception of IP spoofing

- A common misconception is that "IP Spoofing" can be used to hide your IP address while surfing the Internet,chatting on-line,sending email, and so forth.

  This is generally not true. Forging the source IP address causes the responses to be misdirected, meaning you cannot create a normal network connection. However, IP spoofing is an integral part of many networks that do not need to see responses.

Detection of IP spoofing

- **1. If you monitor packets using network-monitoring software such as netlog, look for a packet on your external interface that has both its source and destination IP addresses in your local domain. If you find one, you are currently under attack.**

Source Address Validation :

- Check the source IP address of IP packets
  - filter invalid source address
  - filter close to the packets origin as possible
  - filter precisely as possible

If no networks allow IP spoofing, we can eliminate these kinds of attacks

Prevention of IP Spoofing:

To prevent IP spoofing happen in your network, the following are some common practices:

1- Avoid using the destination address authentication. Implement cryptographic authentication system-wide.

2- Configuring your network to reject packets from the Net that claim to originate from a local address.

3- Implementing ingress and egress filtering on the border routers and implement an ACL (access control list) that blocks private IP addresses on your downstream interface.

If you allow outside connections from trusted hosts, enable encryption sessions at the router.

- **Enable encryption sessions on your router so that trusted hosts that are outside your network can securely communicate with your local hosts.**
- **Firewall Protection**

Is IP Spoofing a Real Risk

- The concept of IP spoofing was initially discussed in academic circles in the 1980's. In the April 1989 article entitled: "Security Problems in the TCP/IP Protocol Suite", author S. M Bellovin of AT & T Bell labs was among the first to identify IP spoofing as a real risk to computer networks.

New Internet Research Shows 30,000 Spoofing Attacks Per Day

One CAIDA study concluded that there were almost 30,000 spoofing attacks each day – and a total of 21 million attacks on about 6.3 million unique internet protocol addresses between March 1, 2015 and Feb. 28, 2017 alone.

CONCLUSION

IP spoofing is an attack that is unavoidable. The attack exploits trust relationships in a world that everything wants to be connected to everything else. If a system is connected to the Internet and provides services, it is vulnerable to the attack. By studying the attack methods, we learn how IP spoofing works and can then identify the weaknesses of a system. By examining the counter-measures, we learn what we need to do for defense, and what we do not need to have, in terms of services and applications.

THANK YOU