
# 02- Common TCP-IP Attacks

**Ahmed Sultan**
Senior Technical Instructor
ahmedsultan.me

# IP Vulnerabilities

- The **IP** is a connectionless protocol that is mainly used to route information across the Internet.
- The role of IP is to provide best-effort services for the delivery of information to its destination.
- Layers above IP use the source address in an incoming packet to identify the sender.
- To communicate with the sender, the receiving station sends a reply by using the source address in the datagram.
- Because IP makes no effort to validate whether the source address in the packet that is generated by a node is actually the source address of the node, you can spoof the source address and the receiver will think the packet is coming from that spoofed address.

# IP Vulnerabilities (cont.)

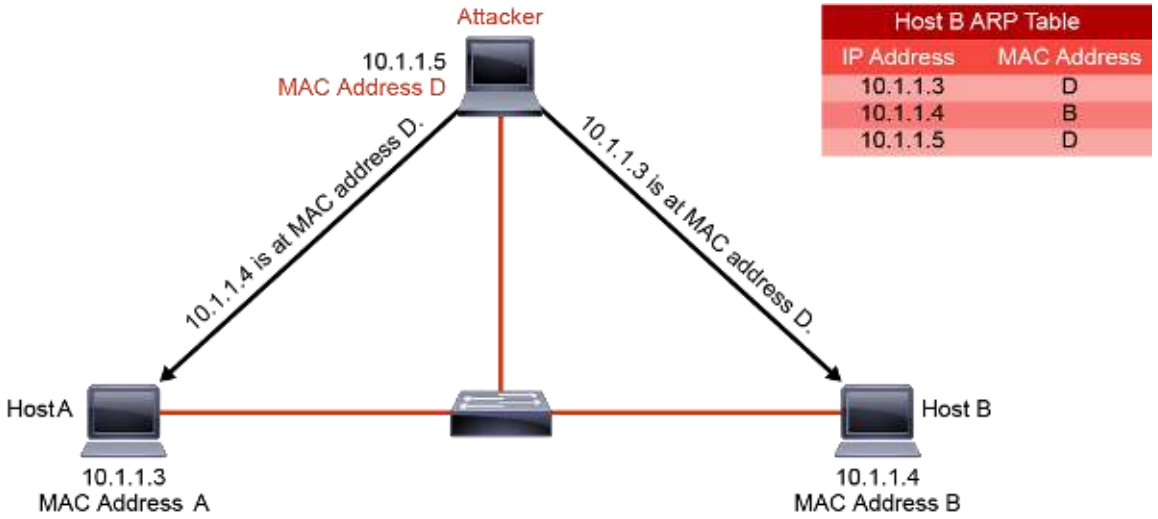
## IP address-based vulnerabilities that threaten network infrastructures

- **Man-in-the-middle attack (MITM):**
  - An MITM attack intercepts a communication between two systems.
  - The attacker inserts a device into a network that grabs packets that are streaming past.
  - Those packets are then modified and placed back on the network for forwarding to their original destination.
  - An MITM attack does not directly threaten your network's stability, but it is an exploit that can target a specific destination IP address.
  - A form of MITM is called "eavesdropping." Eavesdropping differs only in that the perpetrator just copies IP packets off the network without modifying them in any way.

# IP Vulnerabilities (cont.)

## IP address-based vulnerabilities that threaten network infrastructures (cont.)

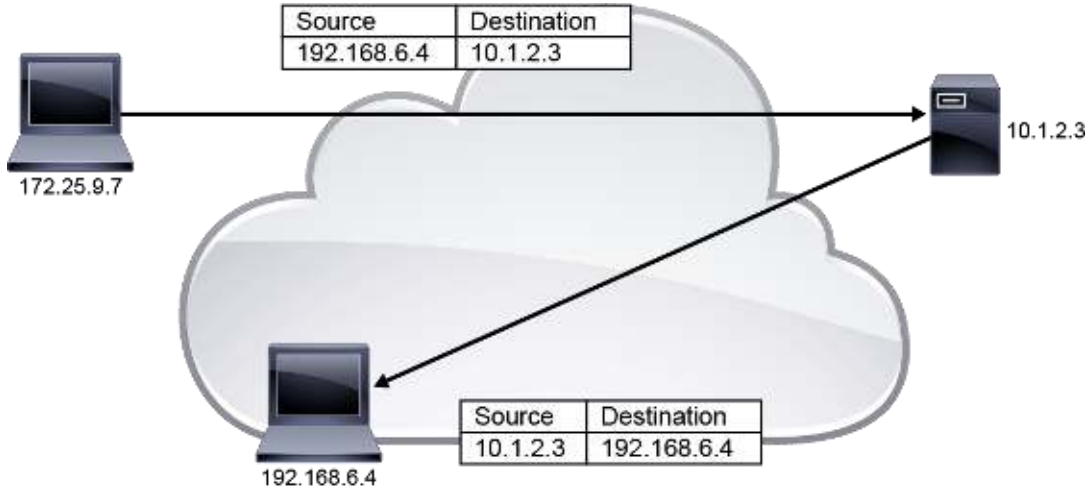
- **Man-in-the-middle attack (MITM) :**



# IP Vulnerabilities (cont.)

## IP address-based vulnerabilities that threaten network infrastructures (cont.)

- **IP address spoofing:**
  - Attackers spoof the source IP address in an IP packet.



# IP Vulnerabilities (cont.)

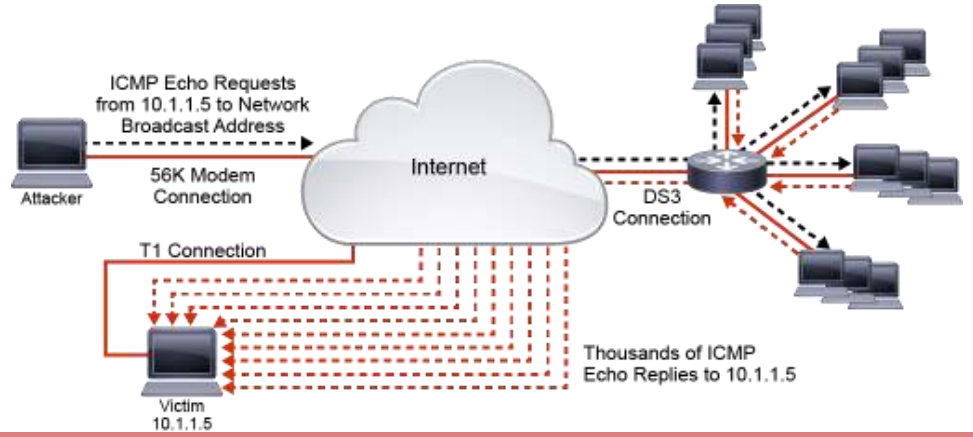
## IP address-based vulnerabilities that threaten network infrastructures (cont.)

- **DoS attack:**
  - In a DoS attack, an attacker attempts to prevent legitimate users from accessing information or services.
  - Since the second half of 2010, DoS has been one of the most common attacks in the United States. By targeting your computer and its network connection, or the computers and network of the sites that you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts, or other services that rely on the affected computers.

# IP Vulnerabilities (cont.)

## IP address-based vulnerabilities that threaten network infrastructures (cont.)

- **DDoS attack:**
  - A DDoS attack is a DoS attack that features a simultaneous, coordinated attack from multiple source machines. The best-known example of a DDoS attack is the "smurf" attack.



# ICMP Vulnerabilities

- **ICMP** is a connectionless protocol that does not use any port number and works on the network layer.
- ICMP was not designed to transfer data in the same way as TCP and UDP. Rather, ICMP was intended to carry diagnostic messages to ensure that links were active and to report error conditions when routes, hosts, and ports are inaccessible.
- ICMP datagrams are often associated with commands that are used by network administrators, such as ***ping*** (ICMP echo request) and ***traceroute*** (ICMP Time to Live [TTL] expired in transit).
- Most ICMP traffic is generated by routers, firewalls, and endpoints to detect and diagnose network connection issues.

# ICMP Vulnerabilities (cont.)

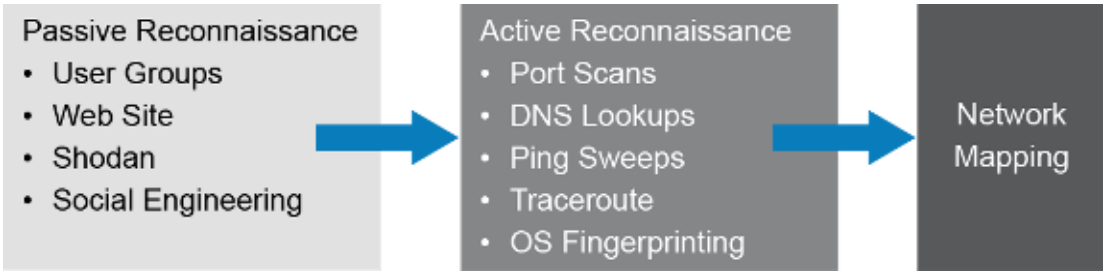
- ICMP is used to inform the sender that a problem has occurred while delivering the data.
- Every network device must implement ICMP, but some administrators block ICMP to prevent attackers from gathering information about their internal network.

- For example:
  - If a host is unable to reach another host on the local network, the sender might receive an *ICMP Destination Host Unreachable message*.
  - If a network link is down, a router may respond to the sender with an *ICMP Destination Network Unreachable message*.

# ICMP Vulnerabilities (cont.)

**Security issues of ICMP messages that you need to understand**

- **Reconnaissance and scanning:**
  - ICMP can be used to launch information gathering attacks. Attackers can use different methods within the ICMP to find out live host, network topology, and OS fingerprinting, and determine the state of a firewall.



# ICMP Vulnerabilities (cont.)

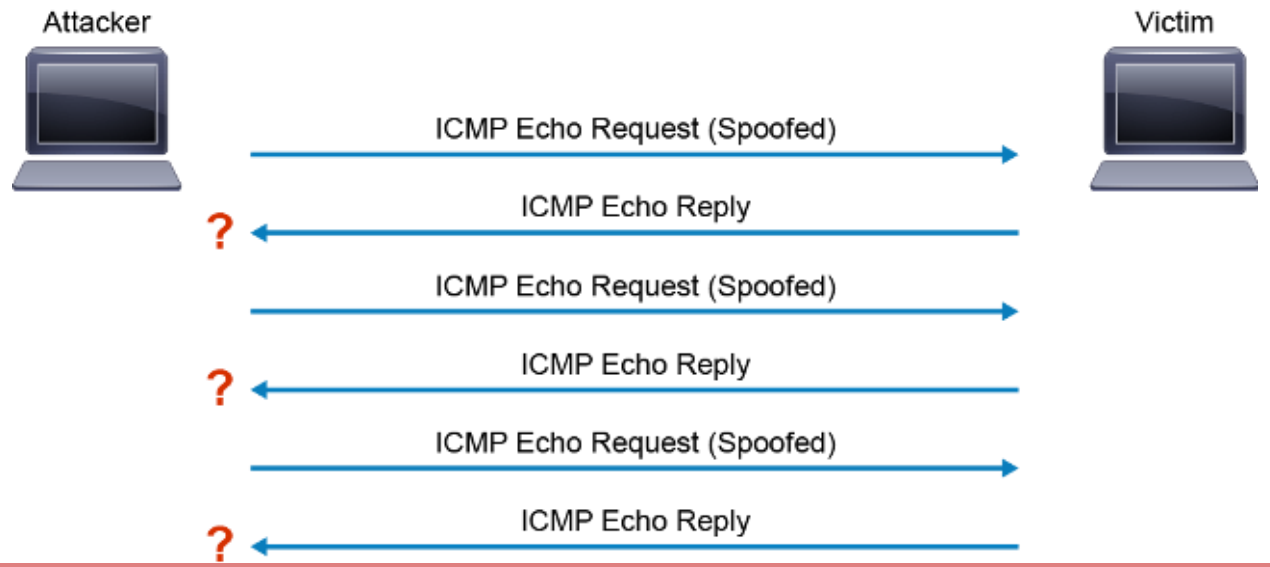
## Security issues of ICMP messages that you need to understand (cont.)

- **ICMP-based Operating System fingerprinting:**
  - Operating system fingerprinting is the process of learning which operating system is running on a device. ICMP can be used to perform an active operating system fingerprint scan.
  - For example,
    - if the ICMP reply contains a TTL value of 128, it is probably a Windows machine,
    - if the ICMP reply contains a TTL value of 64, it is probably a Linux-based machine.

# ICMP Vulnerabilities (cont.)

## Security issues of ICMP messages that you need to understand (cont.)

- **Denial of service attacks:**
  - **ICMP flood attack**



# TCP Vulnerabilities

- TCP stateful communication between two parties happens by way of TCP three-way handshake.
- Before data can be transferred using TCP, a *three-way handshake* opens the TCP connection.
- If both sides agree to the TCP connection, data can be sent and received by both parties using TCP.
- At the conclusion of the TCP session, a *four-way handshake* generally closes the TCP connection gracefully where a typical tear-down requires a pair of Finished (FIN) and Acknowledgement (ACK) segments from each TCP endpoint.

# TCP Vulnerabilities

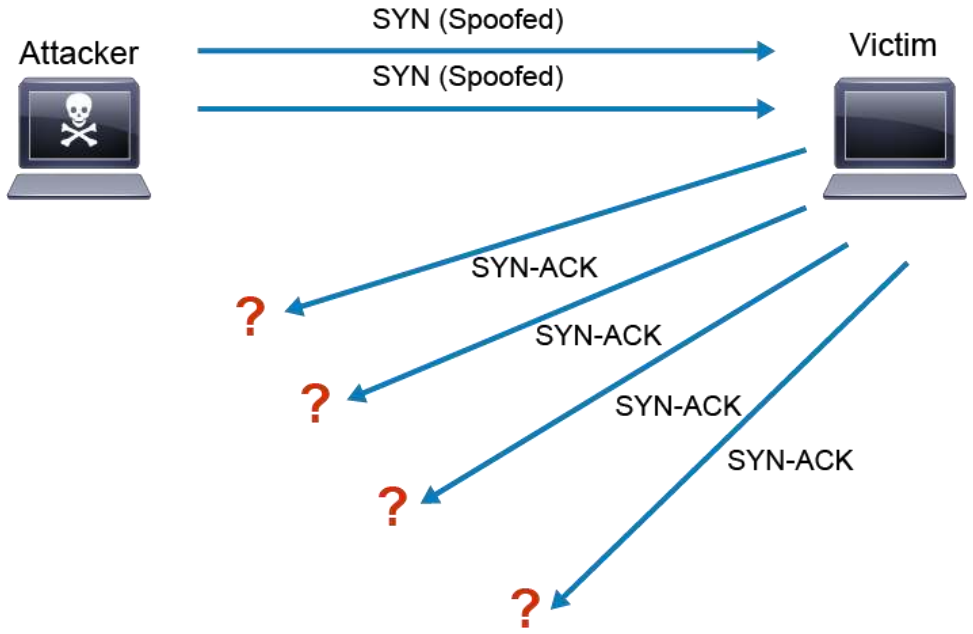
**TCP vulnerabilities are explained in terms of the following attacks**

- **TCP SYN flooding:**
  - TCP Synchronize (TCP) flooding causes a DoS attack.
  - It exploits an implementation characteristic of the TCP that can be used to make server processes incapable of responding to any legitimate client's requests.
  - Any service, such as server applications for email, web, and file storage, that binds to and listens on a TCP socket, is potentially vulnerable to TCP SYN flooding attacks.
  - The basis of the SYN flooding attack lies in the design of the three-way handshake that begins a TCP connection.

# TCP Vulnerabilities

**TCP vulnerabilities are explained in terms of the following attacks**

- **TCP SYN flooding (cont.)**



# TCP Vulnerabilities

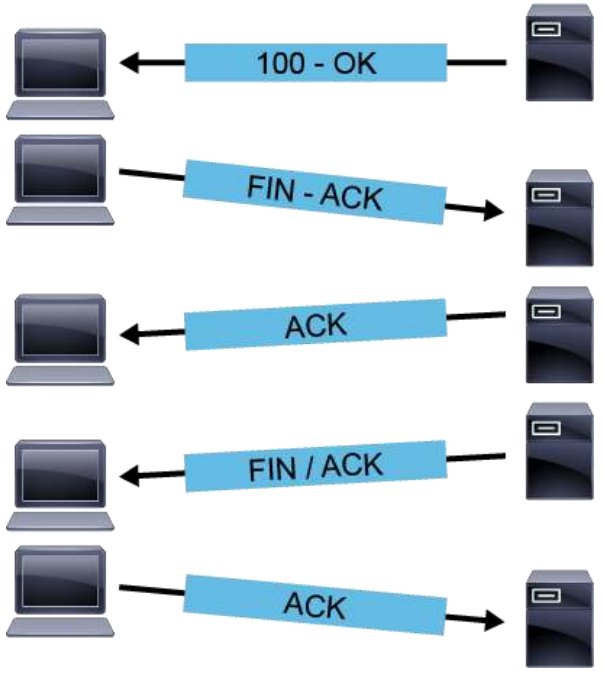
**TCP vulnerabilities are explained in terms of the following attacks**

- **TCP Reset Attack:**
  - The TCP reset attack, also known as "*forged TCP reset*" is a technique of maliciously killing TCP communications between two hosts.
  - A TCP connection is terminated by using the FIN bit in the TCP flags or by using the Reset (RST) bit.
  - The regular way that a TCP connection is torn down is by using the Finish (FIN) bit in the TCP flags.
  - One side of the connection sends a packet with the FIN bit set. The other side of the connection responds with two packets, an ACK, and a FIN of its own.
  - This last FIN is acknowledged by the original station, indicating that the connection has been closed on both sides, as shown in the figure below.

# TCP Vulnerabilities

**TCP vulnerabilities are explained in terms of the following attacks**

- **TCP Reset Attack (cont.)**



# TCP Vulnerabilities

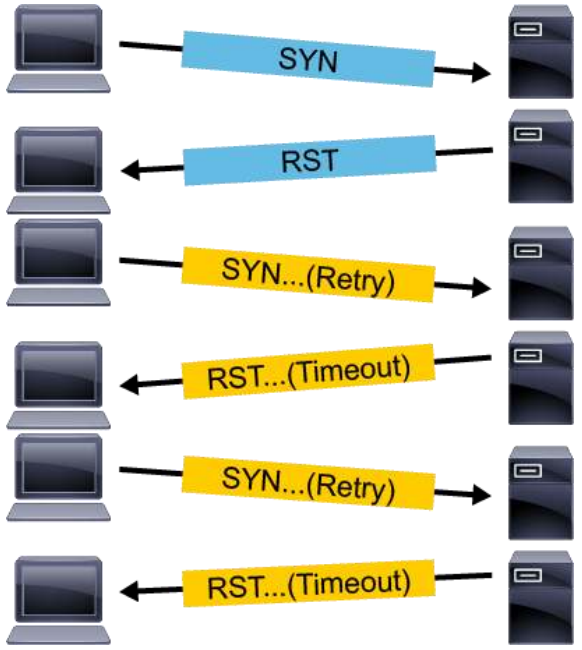
**TCP vulnerabilities are explained in terms of the following attacks**

- **TCP Reset Attack (cont.)**
  - Closing a connection can also be done by using the RST bit in the TCP flags field.
  - In most packets, the RST bit is set to 0 and has no effect. If the RST bit is set to 1, it indicates to the receiving computer that the computer should immediately stop using the TCP connection.
  - A reset indicates that this connection is considered closed, and there is no need to send additional packets.
  - A reset is an abrupt way to tear down the TCP connection. The server should reply with a reset, showing that the connection is closed or unavailable, as shown in the figure below.

# TCP Vulnerabilities

**TCP vulnerabilities are explained in terms of the following attacks**

- **TCP Reset Attack (cont.)**



# DHCP Attacks

- In a TCP/IP-based network, every device must have a unique unicast IP address to access the network and its resources.
- Without **DHCP**, the IP address for each client (a host that is requesting initialization parameters from a DHCP server) must be configured manually and IP addresses for computers that are removed from the network must be manually reclaimed.
- With DHCP, the IP address allocation process is automated and managed centrally.
- The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network.
- Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses that are no longer in use are automatically returned to the pool for reallocation.

# DHCP Attacks

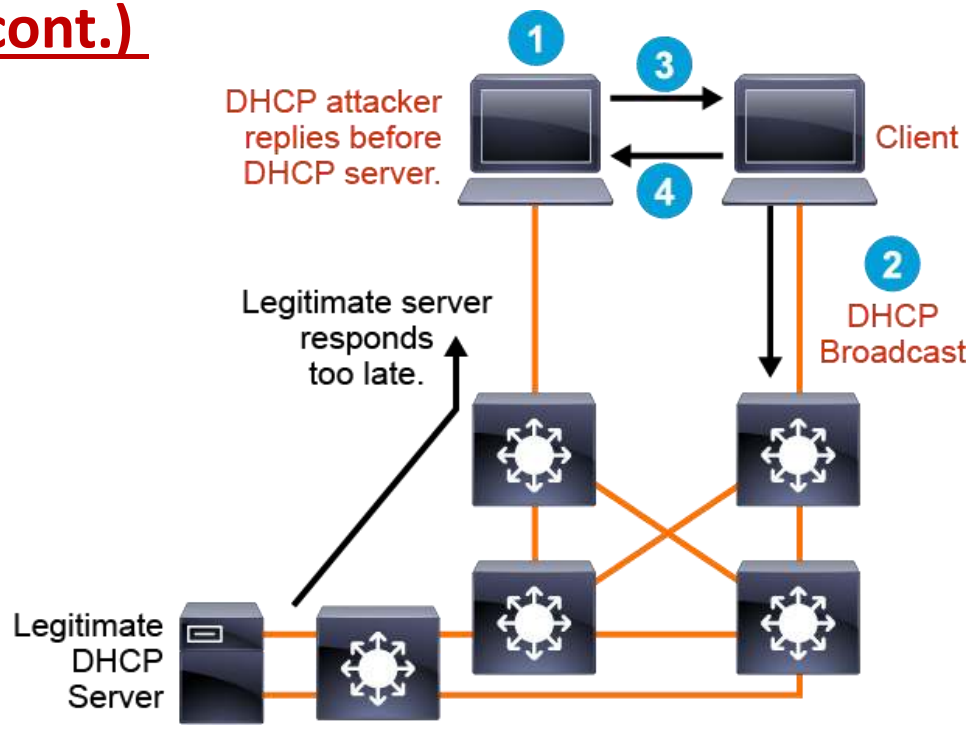
**Two classes of potential security problems are related to DHCP:**

- **DHCP server spoofing:**
  - The attacker runs DHCP server software and replies to DHCP requests from legitimate clients.
  - As a rogue DHCP server, the attacker can cause a DoS by providing invalid IP information.
  - The attacker can also perform confidentiality or integrity breaches via a man-in-the-middle attack.
  - The attacker can assign itself as the default gateway or DNS server in the DHCP replies, later intercepting IP communications from the configured hosts to the rest of the network.

# DHCP Attacks

## Two classes of potential security problems are related to DHCP (cont.)

- **DHCP server spoofing (cont.)**



# DHCP Attacks

## Two classes of potential security problems are related to DHCP (cont.)

- **DHCP server spoofing (cont.)**
  1. An attacker activates a malicious DHCP server on the attacker port.
  2. The client broadcasts a DHCP configuration request.
  3. The DHCP server of the attacker responds before the legitimate DHCP server can respond, assigning attacker-defined IP configuration information.
  4. Host packets are redirected to the attacker address because it emulates the default gateway that it provided to the client.

# DHCP Attacks

## Two classes of potential security problems are related to DHCP (cont.)

- **DHCP starvation:**
  - A DHCP starvation attack works by the broadcasting of DHCP requests with spoofed MAC addresses.
  - If enough requests are sent, the network attacker can exhaust the address space available to the DHCP servers in a time period.