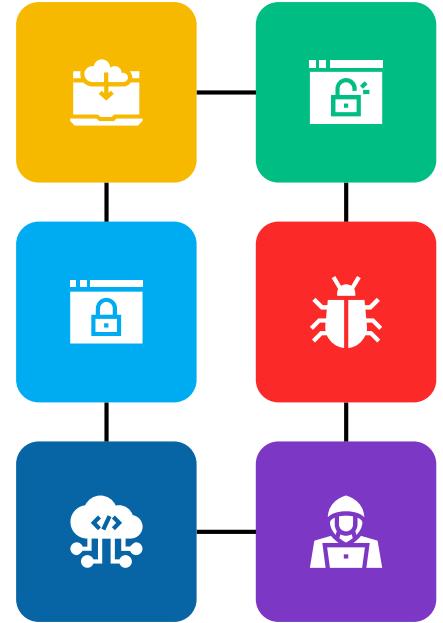


Implementing Secure Network Design

MNU-2025

Dr. Ahmed Samy

Lecture 03








Module Contents

In this module, we will cover the below topics:

| | | | |
|---|--------------------------------|-------------------------------|---|
|  | TCP/IP and OSI Protocol Suites | Layer3 Attacks and Mitigation |  |
|  | Network Devices | Layer4 Attacks and Mitigation |  |
|  | Layer2 Attacks and Mitigation | Virtual Private Network (VPN) |  |

Module Contents

In this module, we will cover the below topics:

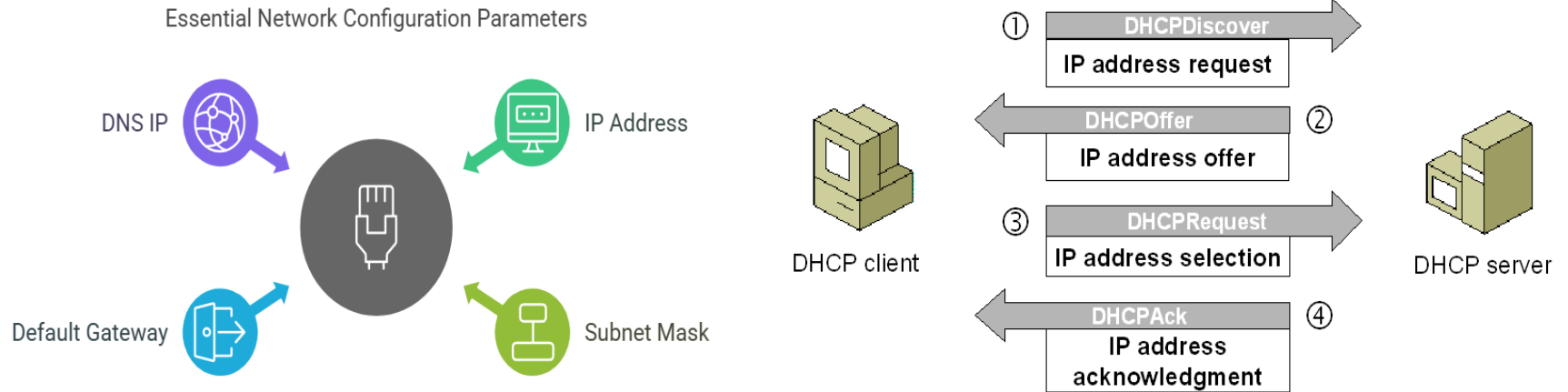
| | | | |
|---|--------------------------------|-------------------------------|---|
|  | TCP/IP and OSI Protocol Suites | Layer3 Attacks and Mitigation |  |
|  | Network Devices | Layer4 Attacks and Mitigation |  |
|  | Layer2 Attacks and Mitigation | Virtual Private Network (VPN) |  |

Layer 2 Attacks ...



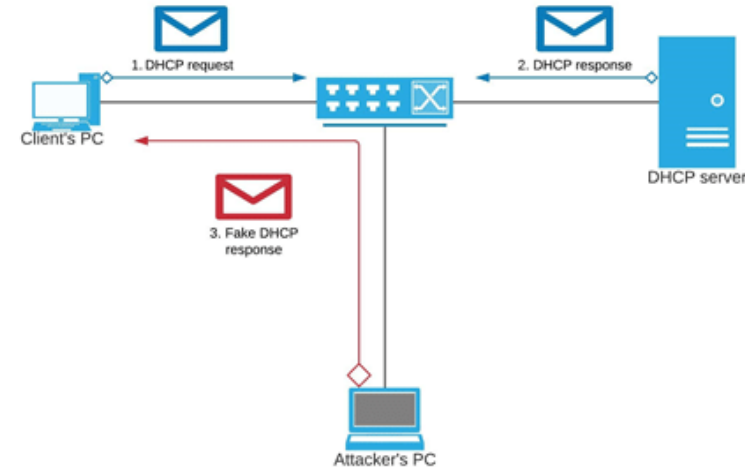
DHCP Spoofing Attack

- DHCP is a network management protocol used to automatically assign IP addresses and other network configuration parameters to devices on a network.



DHCP Spoofing Attack

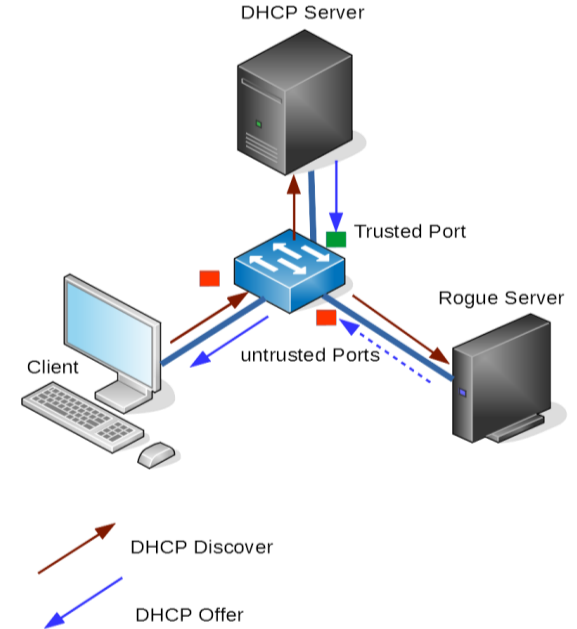
- An attacker sets up a **rogue DHCP server** (Physical server or Software running on a compromised machine) on the network to distribute false IP configuration information to clients.
- When a legitimate client broadcasts a DHCP Discover message to obtain an IP address, the rogue DHCP server responds with a DHCP Offer before the legitimate DHCP server can respond.
- The client accepts the offered IP configuration. The attacker can set the default gateway to their own machine, enabling them to intercept traffic (MITM attack).
- Alternatively, they can provide a non-existent gateway, causing a denial of service.
- **Impact of DHCP Spoofing**
 1. Man-in-the-Middle Attacks
 2. Denial of Service
 3. Data Theft
 4. Network Disruption



DHCP Spoofing Attack Mitigation

- **CISCO DHCP Snooping:** allows for the configuration of trusted ports, which establishes **which devices on the network are allowed to send DHCP Offer and DHCPACK** messages, and all other ports are considered untrusted, and cannot transmit DHCP Offer and DHCPACK messages.
- **DHCP Discover** and **Request** messages are allowed from **untrusted** ports while **DHCP Offer** and **ACK** are only allowed from **trusted** ports messages.
- **Using Dynamic ARP Inspection (DAI)**
- **Applying Port Security.**

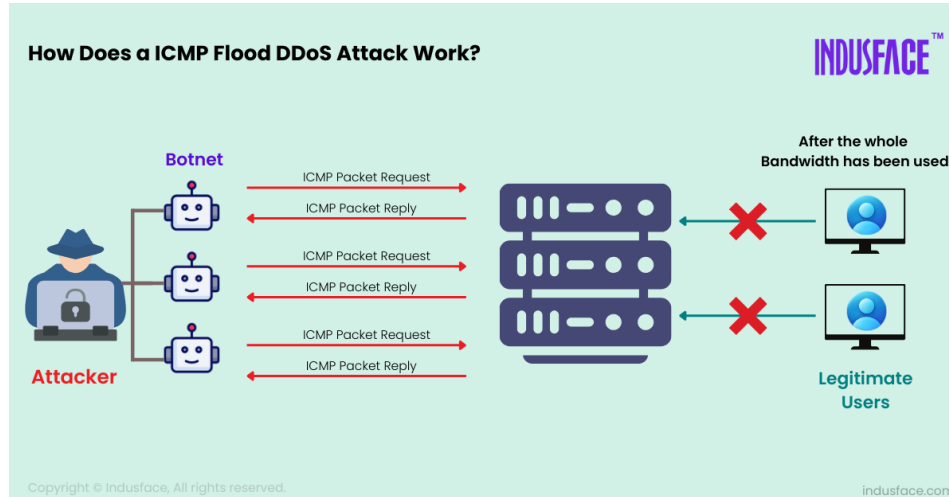
```
switch#conf t
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snoop vlan 1
switch(config)# int g0/24
switch(config-if)# ip dhcp snooping trust
switch(config-if)# exit
switch(config)# exit
switch# show ip dhcp snooping
```



Layer3 Attacks

ICMP Attacks

- Attackers exploit ICMP (Internet Control Message Protocol) to disrupt network services or gather information. Example [ping flood](#).
- A ping flood**, also known as an **ICMP flood**, is a type of distributed denial-of-service (DDoS) attack in which an attacker overwhelms the targeted device or network with continuous request packets (pings) preventing it from managing legitimate traffic and rendering the system unresponsive.

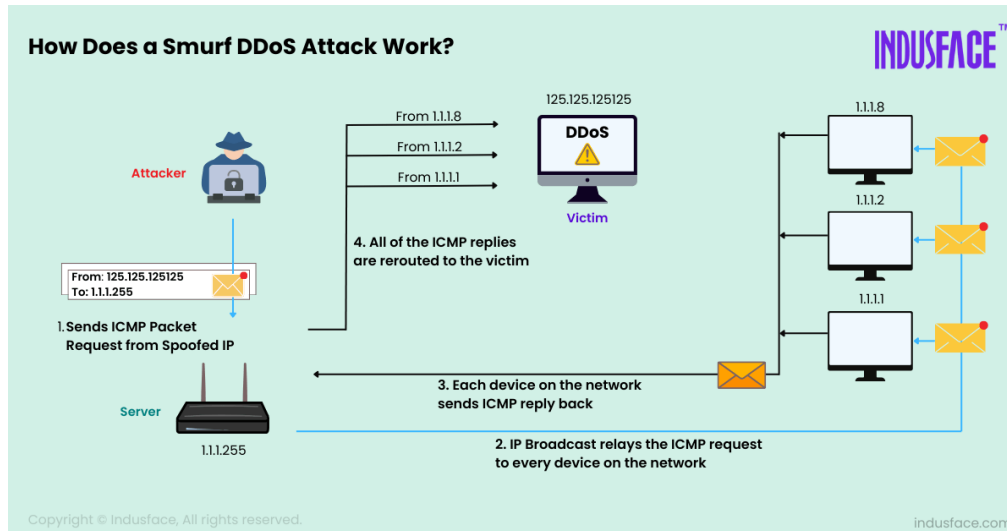


```
ping -t <target IP> -l 65500
```

This command will send a continuous stream of ping packets to the target IP address, with a packet size of 65,500 bytes.

ICMP Flood Attack Vs SMURF Attack

- While an ICMP flood attack directly targets a system with a high volume of ICMP echo requests, a **Smurf attack** amplifies the impact by exploiting IP broadcast addresses.
- In a Smurf attack, the attacker sends ICMP echo requests to the broadcast address of a network with the spoofed IP address of the target. This causes all devices on the network to respond to the target IP, overwhelming it with the responses.



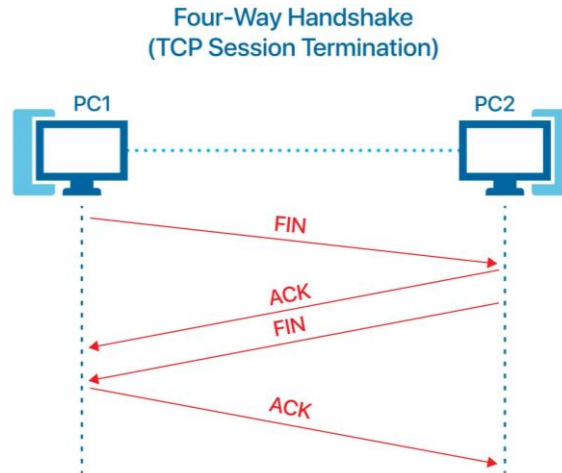
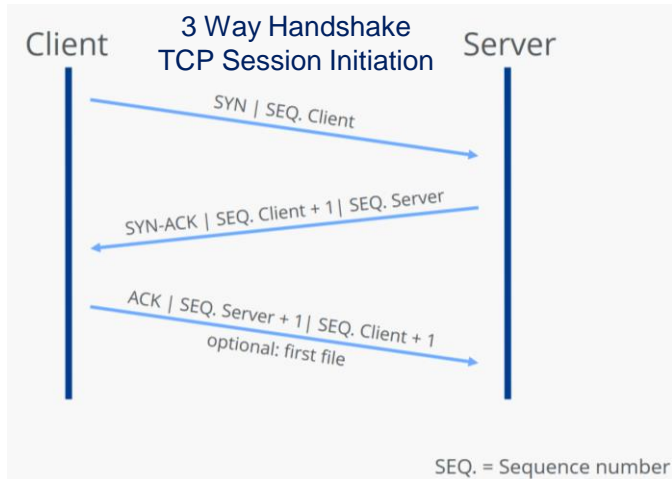
ICMP Attacks Mitigation

- Rate-limit ICMP traffic to prevent flooding.
- Disable unnecessary ICMP messages (e.g., ICMP redirects) on routers and firewalls.
- Use firewalls to filter and monitor ICMP traffic.
- Implementing a DDoS protection solution.
- Network Traffic Monitoring.

Layer4 Attacks

Transport Layer

- **Transport Layer:** Ensures reliable, end-to-end communication between devices, including error recovery and flow control.
- **Protocols:** TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and SCTP (Stream Control Transmission Protocol).
- Flow control, Reliability, Segmentation and Reassembly.



OSI Model

Application

Presenation

Session

Transport

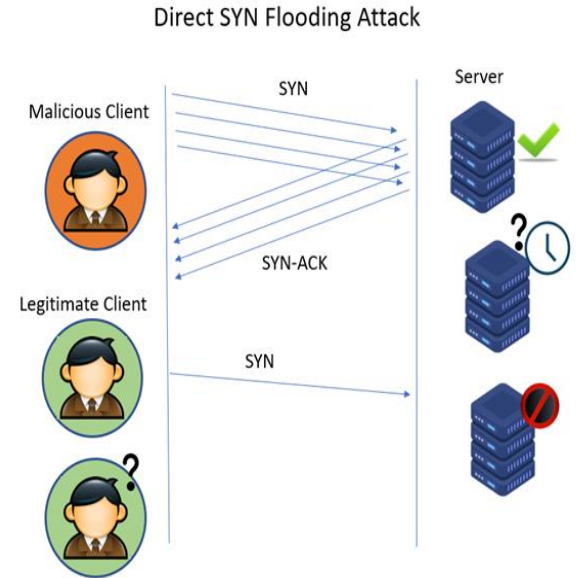
Network

Data-Link

Physical

TCP SYN Flood Attack

- The attacker sends a large number of SYN packets to the target server, often with spoofed source IP addresses.
- The server responds to each SYN packet with a SYN-ACK and waits for the corresponding ACK to complete the handshake.
- Since the source IP addresses are spoofed, the ACK packets never arrive, leaving the server with a **backlog of half-open connections**.
- This exhausts the server's resources (e.g., memory and connection queues), preventing it from accepting legitimate connection requests.
- **Impact of a SYN Flood Attack:**
 - Resource Exhaustion
 - Service Disruption
 - Potential Crashes



TCP SYN Flood Attack Mitigation

1. SYN Cookies:

- The server does not allocate resources until the three-way handshake is complete. Instead, it encodes connection information in the SYN-ACK response and validates it when the ACK is received.

2. Rate Limiting:

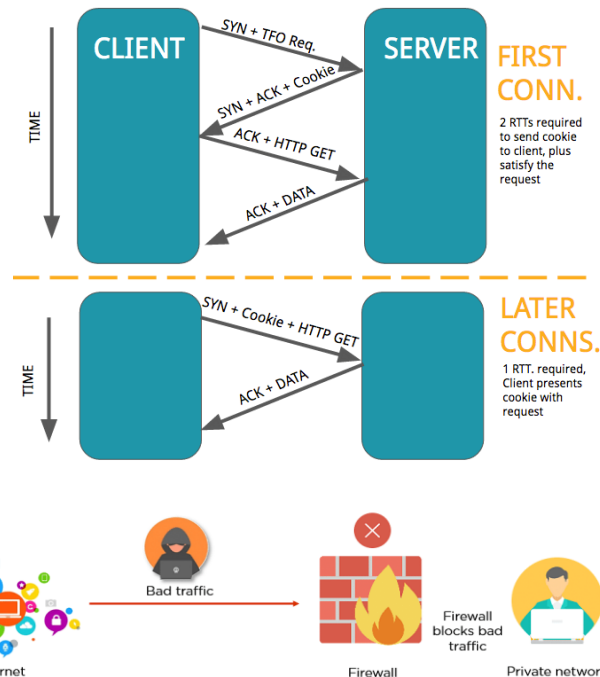
- Limit the number of SYN packets allowed per second from a single IP address or across the network.

3. Firewalls and Intrusion Prevention Systems (IPS):

- Use firewalls or IPS to detect and block suspicious traffic patterns associated with SYN floods.

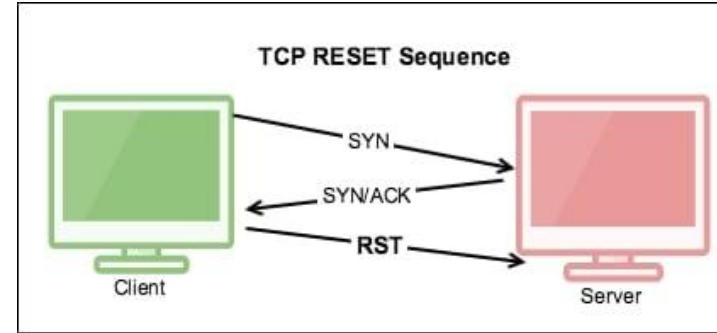
4. Load Balancers and DDoS Protection Services:

- Deploy load balancers or use cloud-based DDoS protection services to absorb and mitigate large-scale attacks.



TCP Reset Attack

- A **TCP reset (RST)** is a signal sent in the TCP to immediately terminate a connection between two devices.
- It is used to indicate that something went wrong with the communication such as connection refusal, port unavailability, protocol mismatch, and timeouts or errors.
- In a **TCP RST attack**, the attacker forges a TCP RST packet and sends it to one or both parties in an established TCP connection.
- The forged RST packet contains:
 - The **correct source and destination IP addresses and ports**.
 - A **valid sequence number** (or one within the acceptable window) to make the packet appear legitimate.
- When the victim receives the forged RST packet, it believes the connection has been terminated by the other party and closes the connection.



TCP Reset Attack Mitigation

1. Encryption and Authentication:

- Use encrypted protocols like TLS/SSL or IPSec to protect TCP traffic. This makes it harder for attackers to forge packets or predict sequence numbers.

2. Sequence Number Randomization:

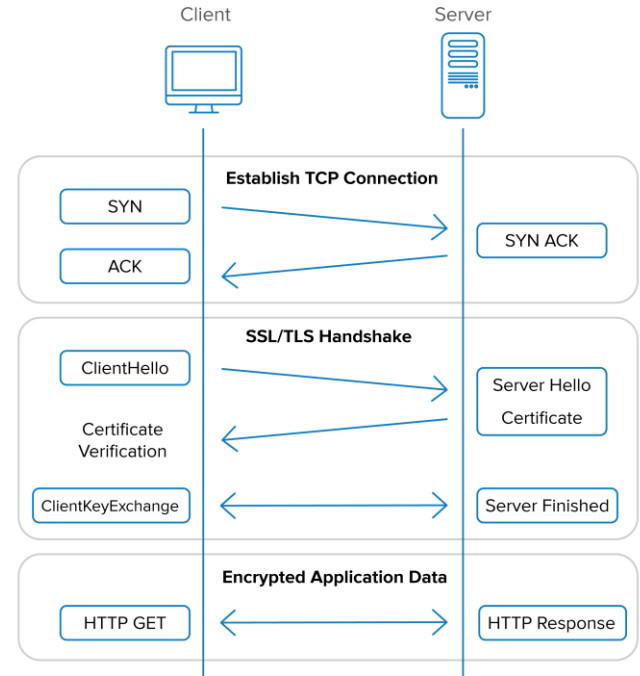
- use randomized initial sequence numbers (ISNs) to make sequence number prediction more difficult.

3. Firewalls rules:

- Configure firewalls to filter out unexpected RST packets or limit the rate at which RST packets are accepted.

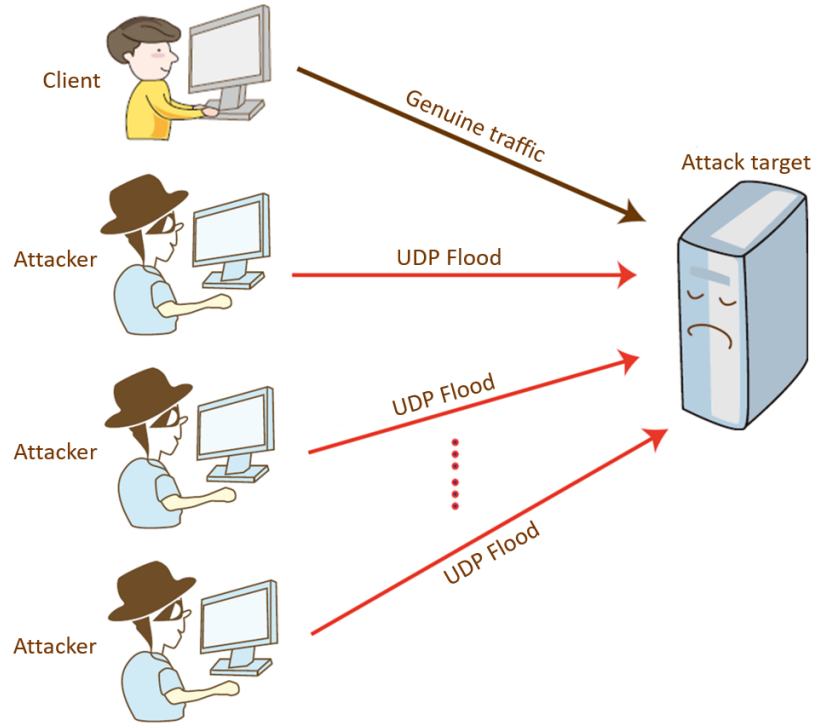
4. Network Monitoring and Intrusion Detection:

- Deploy intrusion detection systems (IDS) or intrusion prevention systems (IPS) to detect and block suspicious RST packets.



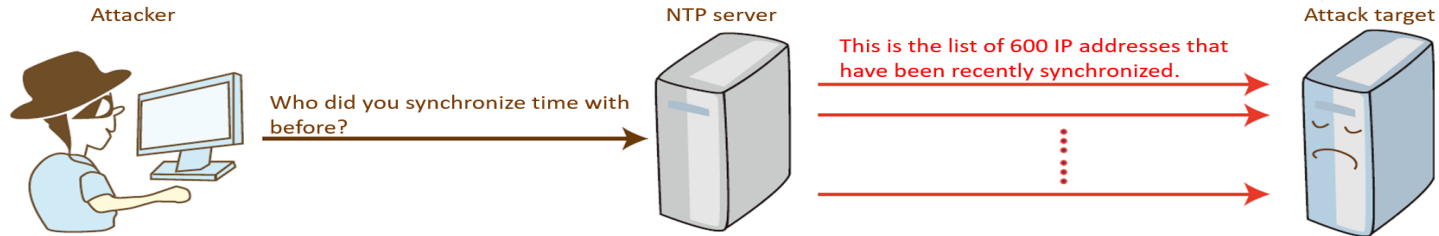
UDP Flooding Attack

- UDP flood is one of the most classic Distributed Denial of Service (DDoS) attacks on the Internet.
- The attacker sends a large number of UDP packets to the targeted device within a short period of time, causing network congestion and failures.
- These packets are usually large in **size** and are transmitted at a **high rate**, causing link congestion or even network breakdown.
- This traditional type of attack mode is rarely used due to its low technological requirements.



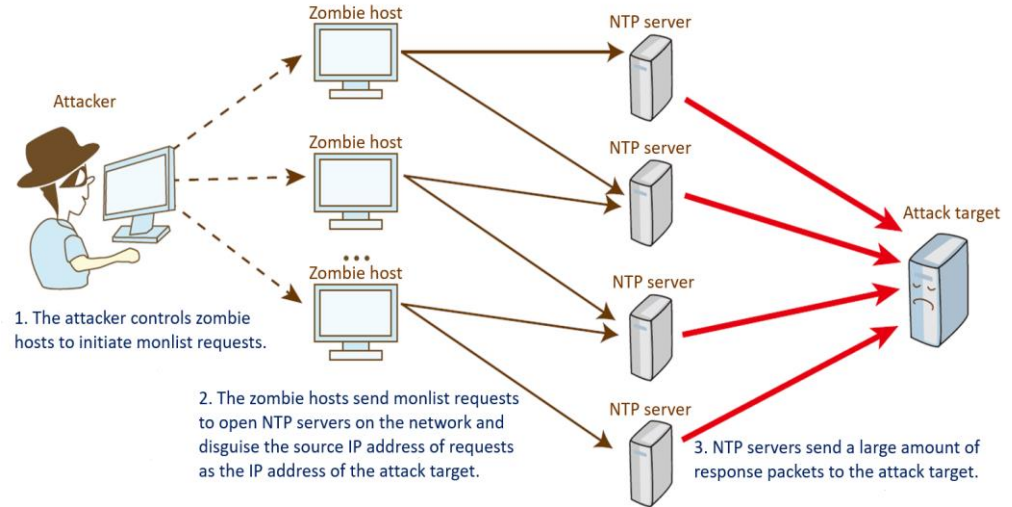
UDP Reflection Attack

- No verification is needed throughout the UDP communication. UDP is a connectionless and lacks a source authentication mechanism.
- These features are exploited by attackers to launch reflection attacks.
- The source IP address of the request packet from a client is changed to the IP address of the **attack target**, and the response packet returned by the server is sent to the attack target.



UDP Amplification Attack

- Attackers may use zombie hosts to send a large number of monlist requests to NTP servers at the same time. **One monlist request packet can trigger 100 response packets.**
- Generally, the size of an NTP request packet (one monlist request) is **~60 bytes**, and the size of a response packet is **~400–1400 bytes (or more)**.
- Therefore, the amplification Factor: **~10:1** to **20:1** (or higher).
- This attack causing link congestion or even network breakdown.



NTP monlist command was historically used for monitoring and debugging purposes. It allows an NTP server to return a list of the last **600 clients** that have interacted with it.

UDP Attacks Mitigation

- **Patch and Harden Servers:**

Ensure that servers running UDP-based services are patched and configured securely. For example:

- Disable the monlist command in NTP servers.

- **DDoS Protection Services:**

- Use cloud-based DDoS protection services (e.g., Cloudflare, Akamai, AWS Shield) to absorb and mitigate large-scale attacks.

- **Firewalls and Access Control Lists (ACLs):**

- Configure firewalls and ACLs to block unnecessary UDP traffic or restrict access to vulnerable services.

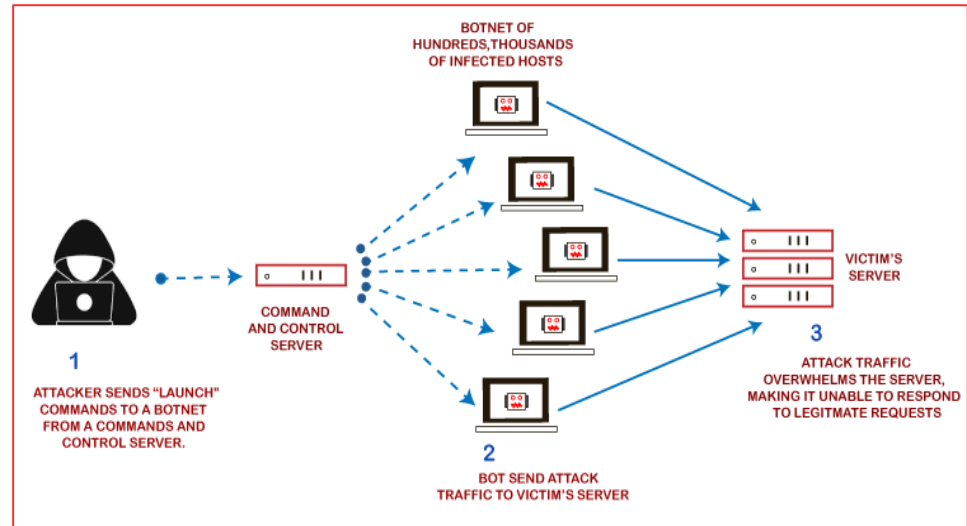
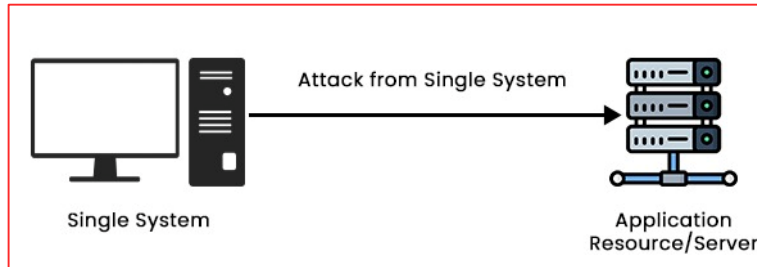
- **Rate Limiting:**

- Limit the rate of UDP traffic from a single source or to a specific service.

DoS vs DDoS Attack

DoS vs DDoS Attack

- A **Denial of Service (DoS) attack** is an attempt to make a service, system, or network unavailable to its intended users by overwhelming it with traffic or exploiting vulnerabilities.
- A **Distributed Denial of Service (DDoS) attack** is a more advanced form of DoS attack where multiple compromised systems (often part of a botnet) are used to overwhelm a target.



TYPES OF DDoS ATTACKS



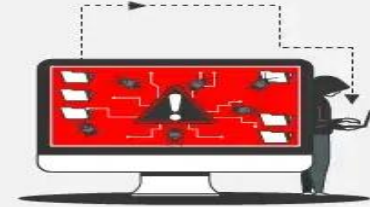
Volume-Based Attacks

Floods network with too much data



Protocol Attacks

Exploit weaknesses in network protocols



Application Layer Attacks

Make target applications crash or sluggish.



Distributed Denial-of-Service (DDoS) Attacks

Uses multiple systems to attack a single target.



Resource Exhaustion

Repeatedly request access to overload application.



Reflective Attacks

Sending requests to 3rd-party servers from victim's IP address.

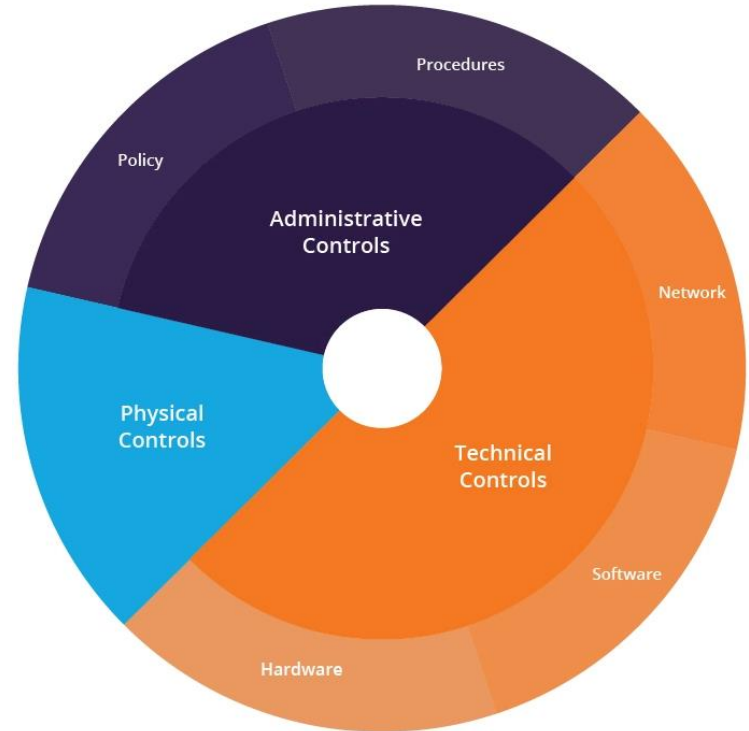
DoS vs DDoS Attack

| Aspect | DoS Attack | DDoS Attack |
|--------------------------|-----------------------------------|--|
| Source of Attack | Single machine or a few machines. | Multiple machines (often a botnet). |
| Scale | Smaller scale, limited resources | Larger scale, massive resources. |
| Complexity | Simpler to execute | More complex, requires coordination |
| Traffic Volume | Lower Volume | Extremely high volume |
| Detection and Mitigation | Easier to detect and block. | Harder to detect and mitigate. |
| Examples | UDP, ICMP, SYN floods | UDP amplification and reflection attacks |

Security Defense In Depth

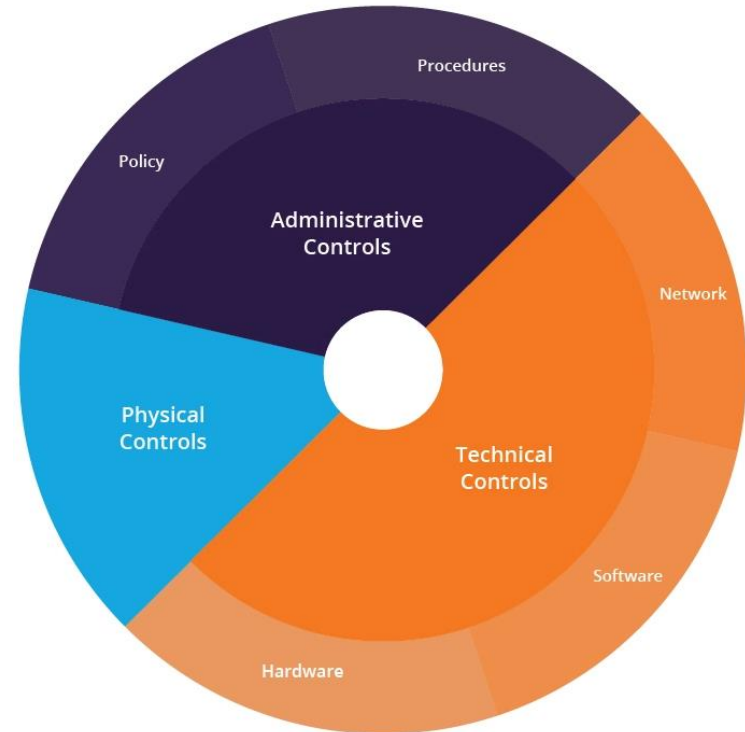
Security Defense In Depth

- Defense in depth is a strategy that leverages multiple security measures to protect an organization's assets.
- The thinking is that if one line of defense is compromised, additional layers exist as a backup to ensure that threats are stopped along the way.
- No one thing can completely secure a system.
- Defense-in-depth security architecture is based on controls that are designed to protect the physical, technical and administrative aspects of your network.



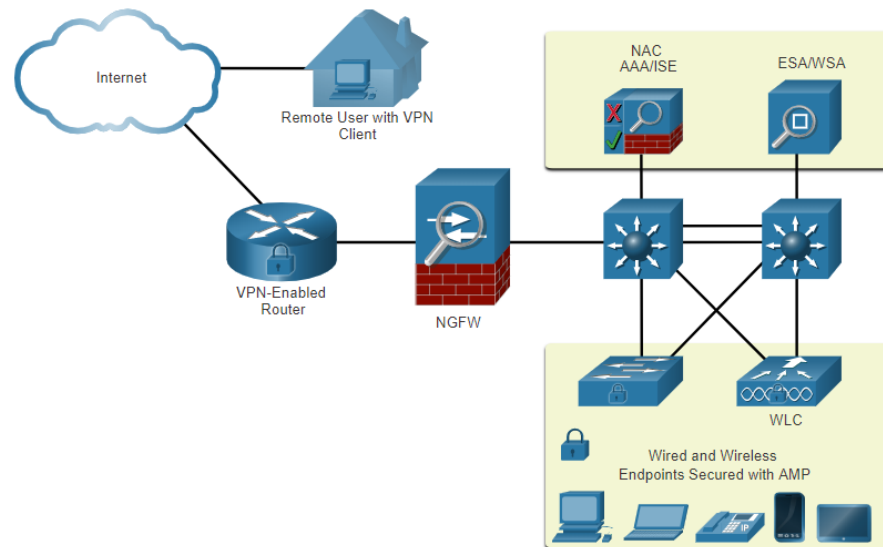
Defense In Depth layered Security Architecture

- **Physical controls** – These controls include security measures that prevent physical access to IT systems, such as security guards or locked doors.
- **Technical controls** – Technical controls include security measures that protect network systems or resources using specialized hardware or software, such as a firewall appliance or antivirus program.
- **Administrative controls** – Administrative controls are security measures consisting of policies or procedures directed at an organization's employees, e.g., instructing users to label sensitive information as "confidential".



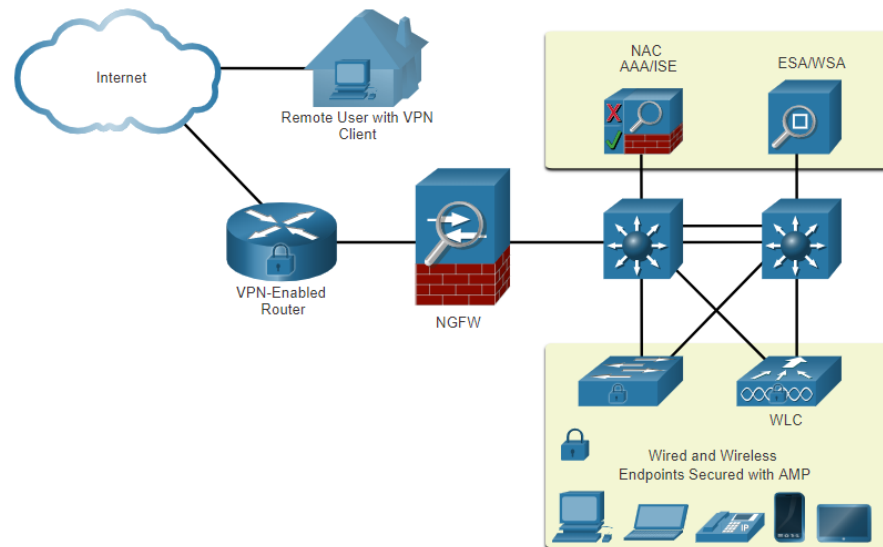
Defense In depth Mechanisms

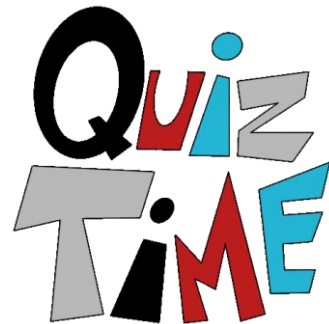
- Strong, complex passwords
- Antivirus software
- Secure gateway
- Firewall
- Patch management
- Backup and recovery
- The principle of least privilege, or giving a user the minimum access level or permissions needed to do his or her job



Defense In depth Mechanisms

- As companies grow and the number of devices, applications, and services used across the organization increases, these serve as important security layers in a defense-in-depth strategy:
- Two-factor authentication (2FA) or multi-factor authentication (MFA)
- Intrusion detection and prevention systems
- Endpoint detection and response (EDR)
- Network segmentation
- Encryption
- Data loss prevention
- VPNs





What is the primary goal of an ICMP flood attack?

- a) To encrypt network traffic
- b) To overwhelm a target with ICMP echo requests
- c) To steal sensitive data
- d) To block DHCP requests

Which of the following is a mitigation technique for ICMP attacks?

- a) Disabling DHCP
- b) Rate-limiting ICMP traffic
- c) Enabling UDP reflection
- d) Using SYN cookies

What is the main impact of a SYN flood attack?

- a) Data theft
- b) Resource exhaustion on the server
- c) Network speed increase
- d) Encryption of traffic

What is the main difference between a DoS and a DDoS attack?

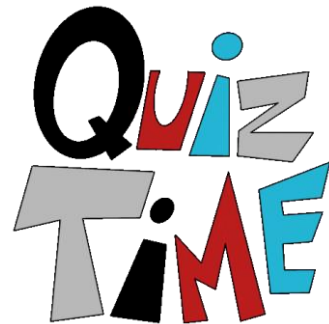
- a) DoS uses a single source, while DDoS uses multiple sources
- b) DoS uses multiple sources, while DDoS uses a single source
- c) DoS targets UDP, while DDoS targets TCP
- d) DoS is faster than DDoS

Which of the following is a mitigation technique for TCP SYN flood attacks?

- a) Disabling ICMP
- b) Using SYN cookies
- c) Enabling UDP reflection
- d) Disabling DHCP

True or False

1. DHCP spoofing can lead to Man-in-the-Middle (MITM) attacks
2. UDP is a connection-oriented protocol
3. A Smurf attack amplifies its impact by exploiting IP broadcast addresses.
4. NTP monlist command is used to increase network speed.



What is the primary goal of an ICMP flood attack?

- a) To encrypt network traffic
- b) To overwhelm a target with ICMP echo requests
- c) To steal sensitive data
- d) To block DHCP requests

Which of the following is a mitigation technique for ICMP attacks?

- a) Disabling DHCP
- b) Rate-limiting ICMP traffic
- c) Enabling UDP reflection
- d) Using SYN cookies

What is the main impact of a SYN flood attack?

- a) Data theft
- b) Resource exhaustion on the server
- c) Network speed increase
- d) Encryption of traffic

What is the main difference between a DoS and a DDoS attack?

- a) DoS uses a single source, while DDoS uses multiple sources
- b) DoS uses multiple sources, while DDoS uses a single source
- c) DoS targets UDP, while DDoS targets TCP
- d) DoS is faster than DDoS

Which of the following is a mitigation technique for TCP SYN flood attacks?

- a) Disabling ICMP
- b) Using SYN cookies
- c) Enabling UDP reflection
- d) Disabling DHCP

True or False

1. DHCP spoofing can lead to Man-in-the-Middle (MITM) attacks
True
2. UDP is a connection-oriented protocol False
3. A Smurf attack amplifies its impact by exploiting IP broadcast addresses. True
4. NTP monlist command is used to increase network speed.
False

Thanks!

Do you have any questions?

